LIVRE BLANC

DÉCEMBRE 2000

INTERNET,

quelles conséquences prudentielles ?

COMMISSION BANCAIRE
SECRÉTARIAT GÉNÉRAL

BANQUE DE FRANCE

INTERNET

QUELLES CONSÉQUENCES PRUDENTIELLES ?

La Banque de France et le Secrétariat général de la Commission bancaire expriment leurs remerciements à l'ensemble des membres des différents groupes de travail, représentants d'établissements de crédit et d'entreprises d'investissement de la place, ainsi qu'au Forum des compétences, qui ont participé à cette réflexion sur les conséquences prudentielles d'Internet.

SOMMAIRE

SOMMAIRE DES ENCADRÉS

ANNEXES

AVANT-PROPOS

En quelques années, Internet a connu un développement très rapide dans le domaine bancaire et financier. Ce phénomène s'est largement diffusé dans les pays développés. En France, le nombre d'internautes représente environ 15% de la population et devrait connaître une forte croissance dans les prochaines années grâce aux multiples modalités d'accès proposées (ordinateurs, téléphones mobiles, agendas électroniques, télévisions…). Le développement en France des services bancaires et financiers sur Internet a été très dynamique : 86 banques françaises proposaient un site Internet en 1999, et plus de 130 en 2000[1].

Les banques françaises ont privilégié le plus souvent une stratégie de type « multicanal ». Internet est alors un moyen parmi d'autres de relation avec la clientèle (agences, minitel, centre d'appels téléphoniques…). Les services rendus –initialement limités à la consultation du solde des comptes et au courtage en ligne[2]– s'élargissent progressivement à l'ensemble des transactions bancaires et financières.

De façon beaucoup plus minoritaire, Internet peut être le canal principal de la relation avec la clientèle. Ces « banques virtuelles » sont établies par des établissements bancaires désireux de pénétrer sur le marché français sans avoir à constituer un réseau d'agences ou par des entreprises d'assurance soucieuses de diversifier leur offre de services financiers.

Les services bancaires et financiers en ligne devraient connaître une progression importante dans les prochaines années, tant en raison de l'élargissement du nombre d'internautes que de leur usage croissant de ces services[3]. La baisse des coûts de télécommunication et le renforcement de la sécurité des transactions, tant d'un point de vue technique que juridique, devraient jouer un rôle essentiel dans cette évolution. A cet égard, l'évolution du droit et de la technique devrait permettre, le cas échéant, dans la plupart des pays développés de conclure prochainement des opérations en ligne pour lesquelles le formalisme de l'écrit-papier est encore aujourd'hui indispensable.

❖

Le développement de l'Internet est porteur de nombreuses opportunités pour les établissements financiers comme pour leur clientèle.

Pour les établissements, Internet diminue le coût de traitement de certaines opérations en impliquant davantage les clients dans les processus opérationnels. En facilitant un traitement des opérations de plus en plus automatisé, Internet permet de redéployer les effectifs vers des services à plus forte valeur ajoutée au bénéfice des clients.

---

[1] Selon l'Association française des banques/IDC

[2] L'Association des courtiers en ligne « Brokers on line » a évalué à près d'1 million le nombre d'ordres de bourse transmis en ligne à la bourse de Paris en novembre 2000 contre 600.000 en décembre 1999.

[3] Une enquête récente (Association française des banques/IREQ) indique que trois internautes sur cinq n'utilisent pas encore de services financiers sur Internet.

Internet permet également d'offrir une palette plus large de produits financiers à destination des particuliers ou des entreprises et d'améliorer la qualité des services. En outre, de nouveaux services se développent, notamment en matière de sécurité. Ainsi, les établissements bancaires, forts de leur capital de confiance, souhaitent développer des services de certification.

Par ailleurs, Internet conduit les établissements financiers à affiner l'analyse des coûts et des revenus associés à chacun de leurs produits en raison de la concurrence des offres en ligne, ce qui leur permet de répondre de la meilleure façon aux besoins de la clientèle. Les établissements agissent sur plusieurs paramètres : le contenu de l'offre, la tarification des services et l'élargissement des plages horaires en dehors des heures d'ouverture des agences.

Dans ce contexte, les moteurs de recherches, les portails et les sites de comparaison des offres de produits bancaires et financiers contribuent à une meilleure diffusion de l'information au profit de la clientèle.

❖

Face au développement de ce nouveau canal de distribution, le Livre blanc a une triple vocation.

- D'une part, ces évolutions, porteuses d'opportunités, tant pour la clientèle que pour les établissements, sont également sources d'incertitudes pour ces derniers. **Le Livre blanc est un recueil des bonnes pratiques en matière de contrôle interne, de lutte contre le blanchiment et de sécurité à destination de la profession.**

- D'autre part, **des propositions sont formulées pour augmenter encore la sécurité des opérations bancaires et financières en ligne**. Ces propositions sont de nature à renforcer la confiance de la clientèle dans ces nouvelles technologies.

- Enfin, **ce Livre blanc s'efforce d'apporter des solutions aux problèmes prudentiels liés à la nature transfrontalière de l'offre** et s'inscrit, à ce titre, dans le cadre de la réflexion internationale menée au sein du Comité de Bâle pour le contrôle bancaire et entre les superviseurs bancaires européens.

❖

En premier lieu, Internet, comme canal de distribution des services bancaires et financiers, fait courir un ensemble de risques essentiellement opérationnels, dont la nature n'est pas nouvelle, mais dont la portée est modifiée ou accentuée.

Ces risques, encourus pour certains d'entre eux par les établissements, pour d'autres par la communauté bancaire dans son ensemble, doivent être à la fois repérés, analysés, maîtrisés et contrôlés. Telle est la vocation première de ce Livre blanc, qui formule des recommandations en matière de contrôle interne et de lutte contre le blanchiment ainsi qu'en matière de sécurité des systèmes d'information et des transactions.

Le Livre blanc se veut pédagogique. Il rappelle avec précision l'état du droit et de la réglementation bancaire et financière ainsi que ses modalités d'application à l'Internet bancaire et financier. Les conditions d'accès à la profession sont également précisées pour les nouveaux entrants ou les prestations transfrontalières que favorise Internet. La maîtrise du **risque juridique** suppose que le droit soit connu de tous et soit précisé sur un certain nombre de points.

Le Livre blanc sur Internet, qui met en avant des bonnes pratiques en matière de services bancaires et financiers en ligne, ne doit pas faire oublier l'ampleur des risques traditionnels, notamment en matière de sécurité des systèmes de l'information. Le risque opérationnel forme un tout, qui ne doit pas être réduit à Internet. La sécurité des systèmes d'information s'inscrit dans une préoccupation globale, que le réseau interne de l'établissement soit connecté à l'Internet ou non, qu'il soit en totalité ou en partie externalisé.

Internet modifie considérablement l'environnement bancaire auquel les établissements de crédit et les entreprises d'investissement doivent s'adapter. L'ampleur et le rythme des investissements pour réussir cette adaptation sont incertains, dans un contexte de mutations technologiques et d'évolution des comportements de la clientèle. Des investissements hasardeux peuvent affecter la solidité d'un établissement. A ce titre, le Comité de Bâle sur le contrôle bancaire souligne[4] l'importance du **risque stratégique**, que fait courir Internet aux établissements.

Ensuite, le risque d'un **manque de maîtrise par les dirigeants des situations nouvelles** qu'introduit le recours à Internet, comme canal de distribution des services bancaires et financiers doit être plus particulièrement souligné. D'une part, Internet favorise le recours de plus en plus poussé à l'**externalisation**. Les établissements doivent être en mesure de contrôler ce type de situation, en prévoyant notamment des clauses d'audit précises dans les contrats de sous-traitance. D'autre part, les dirigeants peuvent être conduits, en raison de la complexité tant juridique que technique de l'Internet de déléguer ces questions à des spécialistes. Dans ce cas de figure, il est souhaitable que ces derniers décrivent de façon précise et exhaustive, dans un document approuvé par les dirigeants, leurs politiques de maîtrise de risques, qu'il s'agisse du risque de contrepartie, du risque juridique et du risque technique.

Sur ce dernier point, s'agissant de la **sécurité des systèmes d'information**, l'annexe au Livre blanc préparée par le Forum des compétences[5] présente un Guide d'élaboration d'une politique de sécurité Internet, dont il conviendrait de s'inspirer pour que soit améliorée la maîtrise de la sécurité des systèmes d'information, que ces derniers soient externalisés ou non.

En particulier, les évolutions tant juridiques que techniques relatives à la signature électronique et au formalisme des contrats électroniques[6], qui devrait être prochainement précisées, supposent plus que jamais que juristes et techniciens des systèmes d'information travaillent de concert pour définir les infrastructures de sécurité nécessaires au bon fonctionnement des services bancaires et financiers en ligne.

---

[4] Rapport du groupe Banque électronique du Comité de Bâle d'octobre 2000.

[5] Le Forum des compétences est une association de spécialistes de la sécurité des systèmes d'information du secteur bancaire et financier.

[6] La transposition de la directive « commerce électronique » devrait permettre, le cas échéant, d'adapter le formalisme de certains contrats à l'électronique, pour permettre la conclusion de contrats pour lesquels le formalisme écrit-papier est encore indispensable à la validité même de l'acte.

Outre des risques essentiellement opérationnels, Internet introduit une **incertitude en matière de rentabilité.**

Tout d'abord, Internet est le vecteur d'une accentuation de la concurrence, par l'arrivée de nouveaux entrants dispensés d'établir un réseau d'agences.

Internet favorise également de nouveaux modes de distribution des produits bancaires et financiers. Les portails mettent plus directement en concurrence les différentes offres. Ce mode de distribution des produits bancaires et financiers a des analogies avec le marché de la grande distribution, qui met en concurrence les producteurs. Certaines analyses envisagent que les établissements de crédit, dont la fonction principale est de créer des produits et de gérer les risques qui y sont attachés, confient ensuite aux portails la distribution de leurs produits. Une érosion des marges des producteurs au profit des distributeurs serait alors à craindre. D'où les initiatives récentes de certaines banques françaises pour créer leur propre portail ou leur place de marché pour leurs relations en ligne avec les entreprises.

En outre, une surenchère en matière de rémunération des dépôts de la part des banques électroniques, qui ont des coûts d'infrastructure moindres que les banques traditionnelles à réseau, est un phénomène dont les prémisses se manifestent en France et plus encore au Royaume-Uni. Cependant, l'expérience des banques électroniques, notamment aux Etats-Unis, a montré que leur développement passe par la constitution d'un réseau d'agences.

Enfin, dans ce contexte très concurrentiel, les frais de publicité et les coûts technologiques sont susceptibles d'obérer la solidité financière de certains établissements.

Ces éléments qui laissent présager une érosion des marges sont contrebalancés par d'autres processus, comme la plus grande productivité des services bancaires et financiers attendue d'Internet.

En outre, les établissements français s'organisent pour occuper le terrain des offres bancaires et financières en ligne, en développant notamment des partenariats entre eux. En ce sens, un renforcement des synergies bancaires est susceptible de conduire à des économies d'échelle et à la préservation des marges ou commissions.

Au-delà de ces incertitudes en matière de rentabilité, Internet appelle la communauté bancaire et financière à se préoccuper du **risque de réputation.** La détérioration de la réputation d'un établissement suite à une défaillance de ses services en ligne est, en effet, susceptible d'affecter l'image des autres établissements par un mécanisme de contagion. Pour sécuriser l'environnement dans lequel sont offerts les services bancaires et financiers, le Livre blanc avance deux propositions : la définition d'un référentiel de sécurité et la mise en place de politiques de labellisation.

❖

Telle est la seconde vocation de ce Livre blanc : proposer des solutions pour que le développement de l'Internet bancaire et financier se fasse en toute sécurité et gagne la confiance des consommateurs.

De graves dysfonctionnements rencontrés par un service bancaire ou financier en ligne peuvent susciter une perte de confiance et porter préjudice à l'ensemble de la communauté financière. Pour offrir de meilleures garanties, la définition d'un profil de protection, qui serait un référentiel de place en matière de sécurité, est préconisée.

Ce référentiel sur lequel travaille maintenant le Comité français d'organisation et de normalisation bancaire (CFONB) devrait servir de fondement à une certification, voire à une labellisation des sites financiers transactionnels. Le profil de protection et la labellisation des sites en matière de sécurité, selon un référentiel commun, devraient être repris par la profession et notamment par les grands acteurs de la place.

Par ailleurs, le développement d'activités bancaires et financières illégales est susceptible de porter préjudice à l'ensemble des établissements et à la clientèle. Aussi est-il proposé de relier dans des conditions de sécurité adéquates le site des établissements au site de la Banque de France-Comité des établissements de crédit et des entreprises d'investissement (CECEI) qui comporte la liste des établissements régulièrement agréés, sur laquelle il pourrait être fait mention, grâce à une procédure de déclaration, de l'activité opérationnelle des établissements sur Internet.

❖

Enfin, le Livre blanc est une source de propositions pour les travaux internationaux, que mènent les superviseurs bancaires et les autorités d'agrément, tant au Comité de Bâle sur le contrôle bancaire qu'au sein de l'espace économique européen.

Ainsi, sur la question de l'agrément en France d'une entreprise fournissant des produits bancaires ou financiers en ligne, un faisceau d'indices a été élaboré. Cette proposition sera faite aux autres pays membres du Comité de Bâle sur le contrôle bancaire pour qu'ils adoptent une approche similaire afin de diminuer l'insécurité juridique qui entoure la prestation transfrontalière de services sur Internet.

Le « profil de protection », sur lequel travaille le CFONB, s'inscrit également dans une perspective internationale. Les autorités prudentielles étrangères, tout comme les autorités françaises, s'intéressent de plus en plus à cette question essentielle de la sécurité des « banques électroniques » . Dans ce contexte, la certification par rapport à ce référentiel, selon une procédure permettant une reconnaissance mutuelle, devrait faciliter l'octroi d'agrément dans les pays vers lesquels les établissements entendent fournir leurs services.

❖

Internet est porteur d'opportunités mais également d'incertitudes pour les établissements bancaires et financiers. Les bonnes pratiques que met en avant ce Livre blanc et les propositions qu'il formule en direction de la profession et des autorités prudentielles étrangères s'efforcent d'offrir des conditions adéquates de sécurité tant technique que juridique ainsi qu'un cadre pour la maîtrise des risques associés à ces activités.

❖

RECOMMANDATIONS DU LIVRE BLANC

Les recommandations, qui figurent dans le Livre blanc, revêtent un caractère de bonnes pratiques, destinées à maîtriser les risques encourus par le recours à Internet, comme canal de distribution des services bancaires et financiers. La plupart des établissements de crédit et des entreprises d'investissement ont inscrit Internet dans le cadre d'une stratégie « multicanal ». Les services qu'ils rendent par voie électronique sont appelés à se développer. L'évolution du droit et des techniques devraient permettre, le cas échéant, de fournir à l'avenir certains services en ligne pour lesquels le formalisme de l'écrit-papier est encore aujourd'hui indispensable. L'essor de ce nouveau média appelle les recommandations suivantes :

1. Recommandations aux dirigeants des établissements de crédit et des entreprises d'investissement

- **en matière de contrôle interne**

- formaliser dans un document validé par les organes exécutifs la stratégie commerciale Internet de l'établissement en précisant en particulier les risques encourus (page 90)
- élaborer un document relatif à la maîtrise des risques, déclinés en risques de contrepartie, en risques juridiques et techniques, qui fournit à la direction générale une vision globale des risques encourus (point 8.1.1, page 96) ;
- fournir au responsable du contrôle interne une compétence explicite et exhaustive sur toutes les questions relatives à la sécurité (point 8.1.2, page 97) ;
- évaluer les moyens nécessaires pour assurer la continuité de l'entreprise et sa crédibilité vis à vis de ses clients et partenaires, tout particulièrement en situation de crise (point 7.2.2, page 94) ;
- maîtriser les prestations externalisées par l'établissement, en prévoyant des clauses d'audit dans ses contrats (point 8.3.1.1, page 102 et 8.3.2.1, page 108) ;

- **en matière de lutte contre le blanchiment**

- s'assurer du respect des règles d'identification satisfaisant le degré d'exigence de la loi du 12 juillet 1990, lorsque la relation de « face à face » est impossible (point 8.4.1.3., page 126) ;
- s'assurer que les renseignements qui sont exigés lors des ordres de transferts émis par le client sont complets et conservés afin de détecter les opérations douteuses et de s'assurer de la traçabilité des opérations (point 8.4.2.2.2, page 131) ;
- pouvoir bloquer, le cas échéant, la réalisation automatique de certaines opérations afin de se donner le temps d'examiner leurs caractéristiques ou d'obtenir un complément d'information (point 8.4.2.2.3, page 131) ;

- **en matière de sécurité**

- élaborer dans chaque établissement une politique de sécurité Internet, dont un Guide préparé par le Forum des compétences figure en annexe (point 8.1.1, page 96) ;
- utiliser des techniques permettant la non-répudiation pour les transactions jugées sensibles

par l'établissement (points 5.3, page 76 et 8.3.3., page 113) ;
- suivre attentivement l'évolution des textes juridiques relatifs à la signature électronique (point 3.2.1, page 62) et au formalisme des contrats électroniques (point 3.2.2, page 67) ainsi que la mise en place des prestataires de services de certification, qui apportera une réponse au besoin de sécurité des transactions (point 8.2.2, page 99) ;

• **en matière de risque juridique**

- établir une étude juridique destinée à mesurer précisément les risques encourus s'agissant des prestations transfrontalières (point 8.2.1, page 98) ;
- associer les directions juridiques et les directions techniques et informatiques pour renforcer le besoin de sécurité des transactions (point 8.2.3, page 101) ;

2. Recommandations à la place

• **la définition d'une référentiel de sécurité de place et la mise en place d'une labellisation ;**

- participer au sein du Comité français d'organisation et de normalisation bancaire (CFONB) au projet de référentiel de sécurité de place, destiné à maîtriser le risque de réputation et à élever le niveau de sécurité de l'ensemble de la place (point 8.3.4, page 117);
- accompagner ce référentiel de sécurité, qui s'inscrit dans une perspective internationale, d'une labellisation permettant de garantir non seulement la sécurité mais aussi la qualité (point 8.3.4.2, page 119) ;

• **la mise en place d'un lien hypertexte entre le site des établissements et celui de la Banque de France-CECEI, autorité d'agrément (point 2.2.1, page 50) ;**

• **la mise en place d'infrastructures de sécurité.**

- rechercher l'interopérabilité des autorités de certification ; la cryptographie à clef publique, qui suppose des infrastructures particulières, apportant des solutions aux besoins de sécurité des transactions bancaires et financières (point 5.3.3, page 78) ;
- définir des « certificats bancaires » et des politiques de certifications ad hoc pour l'identification des clients (point 8.2.2, page 99).

3. Recommandations dans le cadre des travaux internationaux menés par les superviseurs bancaires

- développer la notion de sites actifs et de sites passifs en la définissant précisément afin de diminuer l'insécurité juridique qui entoure actuelle les prestations transfrontalières (point 2.1.3, page 47) ;
- favoriser la certification selon des standards reconnus en matière de sécurité, garantie, tant pour les autorités du pays d'origine que pour les autorités du pays d'accueil de la maîtrise des risques par les établissements (point 8.3.4.1.4, page 118).

RÉSUMÉ

1. L'accès à l'exercice d'activités bancaires et financières sur Internet

La prestation de services bancaires et financiers par Internet modifie les conditions traditionnelles d'exercice de ces activités. L'essor de ce nouveau mode de relation d'affaires facilite l'établissement de contrats transfrontaliers et modifie la relation avec la clientèle tout en suscitant l'apparition de nouveaux acteurs. Par là-même, les autorités sont amenées à clarifier un certain nombre de situations et à préciser certaines exigences liées à l'agrément, relatives notamment à la solidité de la structure financière et à la maîtrise des sites web.

1.1. La caractérisation de l'exercice d'une prestation en France

En règle générale, les éléments caractéristiques des prestations bancaires ou financières sont réalisés par le prestataire au sein de son système de gestion relié au site web. Il faudra alors considérer que les opérations doivent être soumises à agrément au lieu d'établissement du prestataire. Le CECEI est amené en conséquence à examiner si ces opérations sont exercées en France et si elles sont entreprises par un établissement régulièrement agréé.

- **La notification de libre prestation de services pour les établissements de l'espace économique européen**

Un prestataire de l'espace économique européen peut exercer son activité sur la base de l'agrément dont il dispose dans son pays d'origine, en bénéficiant soit de la liberté d'établissement, soit de la liberté de prestation de services. Celles-ci supposent une information préalable des autorités. Il est proposé que la prestation par Internet s'apparente à une libre prestation de services dès lors que l'intention du prestataire est caractérisée. Cette intention serait appréciée sur la base d'un faisceau d'indices (possibilité d'entrer en relation d'affaires à distance, présentation du site dans la langue nationale, référencement du site dans des portails nationaux et dans des moteurs de recherche nationaux…).

- **Le cas d'un établissement d'un pays tiers à l'espace économique européen**

Le même faisceau d'indices serait utilisé pour déterminer si un établissement d'un pays tiers à l'espace économique européen doit être agréé pour offrir des services bancaires et financiers en France ou pour exercer une activité bancaire auprès de résidents français.

1.2. Le cadre juridique relatif à la sollicitation de la clientèle (publicité et démarchage) s'agissant des activités en ligne

A défaut de présence permanente, un établissement peut "solliciter" la clientèle française à des fins commerciales. Il est alors soumis aux lois de 1966, 1985 et de 1972 relatives au démarchage et au décret de 1968 relatif à la publicité. Les autorités françaises peuvent, le cas échéant, faire application de dispositions pénales pour empêcher le prestataire étranger de

mettre en œuvre des pratiques répréhensibles en France. Il est important, en l'état de la législation, d'apprécier dans quelle mesure les dispositions relatives à la publicité et au démarchage s'appliquent aux pratiques actuelles de l'Internet. A ce titre, une grille de lecture est proposée.

1.3. L'identification des services offerts sur Internet

La Direction des établissements de crédit et des entreprises d'investissement de la Banque de France, qui assure le secrétariat du CECEI, est fréquemment interrogée par le public sur l'existence de tel ou tel site offrant des services bancaires et financiers. Ses moyens traditionnels de renseignement sont cependant réduits : elle ne dispose pas à ce jour d'une information exhaustive des prestataires opérant en ligne.

Aussi est-il proposé de considérer que la prestation en ligne constitue un élément notable du mode de fourniture des services, modifiant les conditions d'exercice de l'activité bancaire ou financière et devant faire l'objet d'une déclaration auprès de l'autorité d'agrément.

Cette procédure de déclaration auprès de l'autorité d'agrément de l'intention de fournir des services en ligne permettrait également d'examiner, pour les établissement déjà constitués, si l'ouverture de services en ligne reste compatible avec les éléments de bon fonctionnement de l'établissement appréciés lors de son agrément.

Par ailleurs, il est proposé, conformément au droit communautaire, de rendre obligatoire sur la page d'accueil du site ou sur une page d'accès facile, direct et permanent, l'affichage d'un certain nombre de mentions : l'agrément du CECEI, l'adhésion à un système de garantie des dépôts et/ou des titres, l'adhésion à une association professionnelle.

En outre, dans un souci d'information et de protection des consommateurs contre les activités susceptibles d'être illégales, la mention de l'agrément du CECEI devrait être assortie d'un renvoi au site de la Banque de France-CECEI - dans des conditions de sécurité adéquates- afin de permettre au client de consulter la liste des prestataires agréés.

2. La sécurité

Le Livre blanc sur la sécurité des systèmes d'information des établissements de crédit de la Commission bancaire, publié en 1996, soulignait l'importance des risques liés aux systèmes d'information, dont la maîtrise devait devenir, si elle ne l'était déjà, l'un des objectifs de chaque direction générale. Cet avertissement a été renforcé, par la suite, par les prescriptions de l'article 14 du règlement n° 97-02 du Comité de la réglementation bancaire et financière, celui-ci rendant explicitement les dirigeants des établissements responsables de l'évaluation et de la maîtrise des risques liés à la sécurité des systèmes d'information.

Si les menaces auxquelles doivent faire face les établissements restent, sur le plan des principes, de nature traditionnelle et sont couverts par les objectifs de sécurité DICP[1], l'accélération des processus techniques et du risque de propagation, qui découle du recours à l'Internet, implique une réactivité immédiate et proportionnée à tout incident (menace révélée), destinée à en entraver aussi bien l'extension que l'accumulation des conséquences.

Le développement de l'Internet comme support d'un certain nombre d'activités bancaires et financières, exige donc dorénavant une vigilance accrue de la part des directions générales en matière de sécurité. Leur attention est attirée plus particulièrement sur le besoin de recourir à des évaluations périodiques de la vulnérabilité des systèmes face aux attaques internes et externes. Par ailleurs, la rapidité de propagation des incidents, en cas de mise en défaut des défenses devrait inciter les établissements à accroître l'efficacité des systèmes et des personnels en charge de la détection et des corrections.

C'est ainsi que des mesures particulières devraient être mises en place, afin de créer un environnement de confiance et de sécurité des transactions, de même niveau que celui qui prévaut lorsque ces transactions sont réalisées avec la présence physique des parties, ou au moins à l'aide d'un support matériel (en général papier). Liées à une accélération des transmissions et des processus techniques et face à l'extension de l'origine des menaces, les menaces inhérentes à l'émergence des nouvelles technologies de l'information et des télécommunications (NTIC) peuvent se décliner sous plusieurs angles :

- les dysfonctionnements rencontrés par un établissement peuvent non seulement induire un risque d'image pour celui-ci, mais peuvent aussi engendrer une perte de confiance de la clientèle dont la propagation à l'ensemble de la place est porteuse de risques systémiques ;

- la vitesse de propagation des menaces ne peut être prise en compte par les dispositifs de prévention et de protection traditionnels, une forte réactivité pour la détection et la neutralisation de la menace étant impérative ;

- le développement de la banque électronique s'accompagne d'un recours de plus en plus poussé à l'externalisation, ce qui engendre des risques additionnels dont l'établissement n'a pas, a priori, la maîtrise directe, mais dont la couverture doit être garantie ;

- la relation avec les tiers s'effectue dans un cadre dématérialisé susceptible d'introduire pour chacune des parties une insécurité juridique spécifique.

---

1) Disponibilité, Intégrité, Confidentialité et Preuve, comme exposés dans le Livre blanc sur la sécurité des systèmes d'information.

Au premier degré, les risques opérationnels doivent être maîtrisés par l'établissement dans le cadre de la définition et de la mise en œuvre d'une politique de sécurité Internet et de son contrôle **(1).** L'existence d'un risque de réputation, qui peut se diffuser à l'ensemble de la place, impliquerait qu'y soit ajouté un référentiel de sécurité de place **(2)**.

2.1. Les risques opérationnels liés à la sécurité des systèmes d'information doivent être évalués et maîtrisés par les établissements de crédit et les prestataires de services d'investissement

Si les dirigeants doivent s'impliquer dans l'élaboration et l'application de la politique de sécurité visant à répondre à ces menaces, c'est aux responsables de la sécurité des systèmes d'information (RSSI) qu'il appartiendra, le plus souvent, de prescrire les règles de sécurité propres à l'Internet, d'en déduire les procédures appropriées de mise en œuvre, et de s'attacher à rendre contrôlable l'ensemble du dispositif mis en place. Ceux-ci pourront utilement se reporter au " guide d'élaboration d'une politique de sécurité Internet " du Forum des compétences, figurant en annexe. Ce guide pourra également être utile aux personnes chargées d'élaborer le cadre de contrôle interne et aux personnes chargées de l'appliquer au titre des contrôles de premier niveau et de second niveau.

- **Des réponses aux menaces susceptibles de porter préjudice aux utilisateurs**

La perte d'intégrité des flux d'information, l'atteinte à la vie privée (écoute, conservation illicite d'informations personnelles), l'usurpation d'identité d'un utilisateur autorisé, sont autant de menaces auxquelles les établissements doivent s'efforcer de répondre afin d'assurer la sécurité des transactions.

Cela requiert en général la mise en oeuvre de techniques cryptographiques adaptées aux exigences des métiers bancaires. C'est ainsi que si toutes les informations transmises ne demandent pas à être protégées, les établissements auront soin de définir les transactions qui nécessitent des dispositifs ou des infrastructures de sécurité ad hoc : **cryptographie asymétrique**, chiffrement des données, etc.

Il peut être également nécessaire, dans le cadre des transactions sur Internet, de faire usage de fonctions d'authentification forte pour s'assurer de l'identité des différentes parties. Ceci peut être réalisé en utilisant une variété de méthodes (mots de passe chiffrés, cartes à puces[2], signatures électroniques, voire biométrie), qui ne sont pas exclusives les unes des autres, mais qui doivent s'adapter aux exigences des métiers bancaires. Les infrastructures à clef publique, dans lesquelles intervient un tiers pour certifier les échanges, restent cependant indispensables, dans l'état actuel des techniques, pour couvrir l'ensemble des besoins de sécurité : authentification, **confidentialité**, intégrité et **non-répudiation**.

2) Les conditions de sécurité fixées par le décret " signature électronique " étant a priori difficilement remplies par des dispositifs de création de signature sous environnement PC, l'utilisation de la carte à puce sera probablement incontournable.

- **Des réponses aux menaces pesant sur le fonctionnement du service**

La disponibilité des services offerts sur Internet et la maîtrise des risques d'intrusion dans les systèmes d'information de l'établissement doivent être au coeur des préoccupations des responsables. Sous la pression de la concurrence et des attentes des clients, une indisponibilité prolongée, outre le risque financier immédiat qu'elle peut comporter, peut être fortement dommageable pour les établissements en termes d'image et de crédibilité. C'est ainsi qu'en raison des menaces spécifiques de l'Internet, notamment en matière de déni de service[3], la conception et la fiabilité des systèmes de secours (*back-up*) doivent être particulièrement renforcées.

Les menaces d'intrusion que représentent des accès illicites, le contournement du contrôle d'accès, la modification des règles et l'usurpation de l'identité des exploitants du système sont sérieuses et peuvent porter préjudice tant au service sur Internet qu'aux systèmes d'information internes auxquels ce service Internet est raccordé. La conception et la fiabilité des systèmes de contrôle d'accès et de cloisonnement entre les sous-systèmes doivent être particulièrement bien étudiées. Les conditions de surveillance et de maintenance de ces systèmes doivent en particulier être très sérieusement détaillées, appliquées et pourvues en personnel compétent et disponible.

Il faut rappeler que les fraudes et malversations internes représentent toujours une grande part des actes de malveillance en matière d'atteinte à la sécurité des systèmes d'information. La mise en place conjointe de mesures assurant un contrôle efficace des accès et de modalités d'attribution des autorisations réellement discriminantes est seule de nature à juguler ce risque.

- **Des réponses aux menaces susceptibles de porter atteinte à la fois au service et aux clients**

Le risque de détournement de sites (*web spoofing*) apporte incontestablement une dimension particulière aux menaces induites par l'usage d'Internet. Il consiste à substituer à des sites " officiels ", et parfaitement honorables, des services dont la moindre conséquence est de nuire à l'image des premiers, et, à l'extrême, de fonder un système de fraude engageant leur responsabilité, faute de preuves contraires suffisantes.

Par ailleurs**,** la transposition des directives " commerce électronique " et " signature électronique " consacrera la possibilité juridique de conclure dorénavant des transactions pour lesquelles une preuve pré-constituée et matérialisée (un écrit) était jusque-là indispensable. Il sera nécessaire, en conséquence, que les établissements de crédit, comme les prestataires de services d'investissement, se dotent des infrastructures de sécurité permettant de remplir les exigences de forme attachées à certaines opérations bancaires et financières, sous peine de nullité des contrats. Ces risques doivent être particulièrement analysés sous un angle à la fois juridique et technique.

---

3) Attaques qui visent à paralyser un système sous un flot de requêtes saturant les serveurs.

2.2. La maîtrise du risque de réputation, qui peut se propager à l'ensemble de la communauté financière, plaiderait en faveur de la mise en place d'un référentiel de sécurité qui serve de fondement à une certification, voire à une labellisation des sites web financiers

De graves dysfonctionnement rencontrés par un service bancaire ou financier en ligne peuvent susciter de la part de la clientèle une perte de confiance et, par propagation, porter préjudice à l'ensemble de la communauté financière. Un établissement n'offrant pas de bonnes garanties de sécurité ferait ainsi courir un risque d'image et financier pour la place toute entière. La vocation première d'un référentiel de sécurité applicable à ce niveau serait donc de garantir, de façon publique, la conformité du dispositif de sécurité adopté par un établissement, en regard d'un ensemble de critères constituant une " cible de sécurité " communautaire.

La définition d'un tel référentiel de sécurité a motivé la saisine du Comité français d'organisation et de normalisation bancaire (CFONB) par le Secrétariat général de la Commission bancaire, afin que soit élaboré un " **profil de protection** " (PP) adapté aux risques des sites web financiers transactionnels, susceptible de déboucher, à terme, sur un processus de certification.

- **La dimension internationale du profil de protection**

La certification devrait ainsi avoir pour objet de garantir le niveau de sécurité offert par tout site soumis à l'obligation d'agrément, non seulement aux yeux des autorités françaises de contrôle, mais aussi étrangères, en raison de la vocation internationale croissante des services bancaires en ligne. En tant que standard international, les **Critères communs** s'imposeront alors immédiatement comme une référence obligée pour une recherche de reconnaissance mutuelle du (ou des) futur(s) PP susceptible(s) d'être défini(s).

- **La mise en place d'une labellisation**

Certains besoins sécuritaires, au-delà de la cible d'évaluation qui sera adoptée pour le PP, pourraient être jugés importants par les établissements. La réponse se situerait dans une labellisation complémentaire permettant de garantir la qualité du site concerné, notamment en regard des critères juridiques devant entourer la relation commerciale sur un plan bilatéral.

La création d'un label englobant tous ces aspects répondrait ainsi à l'objectif d'offrir une assurance supplémentaire de légitimité aux clients, tout en constituant un argument commercial pour les établissements qui l'adopteraient.

En tout état de cause, la certification et/ou la labellisation ne constitueraient que des éléments complémentaires intégrés au dispositif global de sécurité, lequel doit rester sous l'entière maîtrise de la direction générale des établissements.

3. Le contrôle interne et la lutte contre le blanchiment

Internet ne change pas la nature des risques encourus par les établissements. En revanche, la nature à la fois dématérialisée, automatisée et transfrontalière de ce canal de distribution rend plus difficile et sensible l'application des obligations légales et réglementaires en matière de lutte contre le blanchiment et de maîtrise des risques opérationnels ou financiers.

3.1. Les risques soulevés par l'Internet…

- Le **blanchiment peut être facilité par la nature dématérialisée** de la relation qui s'établit *via* Internet entre le banquier ou le prestataire de services d'investissement et son client, qui rend plus difficile la vérification de l'identité et de la capacité financière de ce dernier. Les possibilités de traitement, largement automatisés, des opérations des clients sont également un facteur de risque en permettant aux clients de dissimuler des opérations douteuses ou frauduleuses dans une masse d'opérations traitées sans contrôle humain.

- La possibilité d'ouvrir des comptes avec des clients non-résidents pose la **question de la maîtrise des risques juridiques**.

- Le **caractère hautement technologique de ces activités crée un risque de perte de maîtrise de l'outil informatique** par les dirigeants et les services utilisateurs, qui ne seraient plus en mesure de s'assurer que les systèmes offrent le niveau de service garanti aux clients et que les dispositifs de maîtrise du risque de contrepartie (contrôles de provision) répondent à leurs exigences.

- Il apparaît enfin que l'importance des investissements nécessaires impose aux établissements de porter une **attention particulière à la rentabilité des fonds investis**.

3.2. … appellent les recommandations suivantes

- **en matière de contrôle interne**

Le Livre blanc conclut qu'en matière de contrôle interne, les risques peuvent être maîtrisés dans le cadre de la réglementation actuelle. Les recommandations suivantes constituent à cet égard autant de principes de base du contrôle interne qui peuvent utilement être rappelés à tous :

- les organes dirigeants doivent être impliqués à toutes les étapes d'un projet Internet. Une coordination des projets existant au sein de l'établissement est nécessaire à la maîtrise des risques, dans le cadre de la politique de sécurité approuvée par les dirigeants ;

- lorsque les services sont rendus à des non-résidents, le cadre juridique de la relation doit être connu et l'ensemble de la documentation juridique doit y être adapté ;

- il est nécessaire de se doter de dispositifs de limitation permanente des risques sur les clients et contreparties, et notamment de filtres exhaustifs et automatiques, dont l'existence

et l'efficacité a été vérifiée par les utilisateurs ;

- le système d'information doit être maîtrisé, qu'il soit interne ou externalisé, afin d'offrir des performances et une sécurité conforme aux engagements pris par l'établissement. Dans ce dernier cas, celui-ci doit disposer de toute facilité pour contrôler les installations de son prestataire externe ;

- la rentabilité des opérations doit être connue et faire l'objet, pour l'avenir, de prévisions réalistes, qui doivent tenir compte des importants investissements nécessaires et de l'incertitude sur la stabilité de la clientèle.

• **en matière de lutte contre le blanchiment**

Le Livre blanc souligne les risques importants en matière de blanchiment induits par l'offre de services financiers sur Internet et la vigilance toute particulière qui est requise des établissements intervenant par ce canal. Il soulève également les difficultés d'application des dispositions de la loi du 12 juillet 1990 en matière d'identification lors de l'entrée en relation d'affaires avec un client qui n'est pas physiquement présent.

- Des préconisations sont faites en matière d'entrée en relation avec la clientèle, pour éviter que des comptes soient ouverts sous de fausses identités ou par des prête-noms en profitant des difficultés d'identification dues à une relation dématérialisée. Il est recommandé en particulier que des mesures spécifiques permettant d'établir l'identité du client soient mises en place telles que notamment, l'obtention de pièces justificatives supplémentaires ou des mesures additionnelles de vérification. Par exemple, le dossier d'ouverture de compte, comprenant notamment l'identifiant et le mot de passe du client (ou son équivalent) peut être envoyé par la poste, si possible avec accusé réception. Enfin, il est apparu nécessaire de souligner que le fonctionnement d'un compte - y compris la réception de fonds et d'instruments financiers - ne peut être autorisé qu'une fois que la procédure d'identification a été achevée.

- Sur le contrôle des opérations douteuses, a été identifiée, comme protection de base, la nécessité du contrôle exercé sur le fonctionnement des comptes par les responsables clientèle, qui doivent recevoir une responsabilité claire à ce titre et les moyens de la mettre en œuvre. Il est à souligner qu'en l'état de la technique, il est difficile, voire impossible, de savoir si la personne faisant fonctionner le compte est réellement celle qui l'a ouvert.

INTRODUCTION

Ce Livre blanc est issu d'une collaboration entre des représentants d'établissements de crédit et d'entreprises d'investissement et des agents de la Banque de France et du Secrétariat général de la Commission bancaire, au sein de groupes de travail dont la composition figure en annexe. La réflexion, qui s'est appuyée sur un document de discussion et d'études disponible sur le site de la Banque de France, s'est concentrée sur trois domaines :

- **conditions d'accès à l'exercice de la profession** ;

- **sécurité ;**

- **contrôle interne et lutte contre le blanchiment**.

Le cadre d'exercice des activités bancaires et financières sur Internet est analysé et précisé en **première partie**. En préalable, il convient de noter qu'Internet présente une nouvelle donne pour l'offre de services bancaires et financiers tant en raison de la nouvelle relation de clientèle qui prévaut sur ce canal de distribution, des nouveaux opérateurs et des nouvelles pratiques qui se développent, que de la nature transfrontalière de l'offre (point 1). Il découle de cette analyse les conditions d'accès à l'activité bancaire et financière sur Internet (point 2), qu'il s'agisse des opérateurs d'un pays tiers à l'espace économique européen (EEE) ou des pays de l'EEE. L'examen des conditions d'accès à l'activité bancaire et financière sur Internet ne peut pas faire l'économie d'une analyse supplémentaire concernant le droit applicable à l'exercice de cette activité (point 3.). Le cadre d'exercice de l'activité bancaire et financière sur Internet est présenté sous forme de grille d'analyse des différentes relations prestataires/ clients. Ces développements sont destinés à faciliter la maîtrise du risque juridique afférent à une relation transfrontalière, sans pour autant présenter une analyse exhaustive des règles de droit. Enfin, le droit de la preuve dans le contexte d'Internet est présenté.

Outre ces risques juridiques liés à une prestation transfrontalière, sont exposés dans une **seconde partie** les risques, d'un point de vue prudentiel, de l'usage de ce canal de distribution. Si les risques financiers sont de même nature (point 4.), l'Internet accentue la portée des risques opérationnels, qui restent de nature traditionnelle (point 5.) :

- risques juridiques ;

- risques liés à la sécurité des systèmes d'information et des transactions en ligne ;

- risques en matière de blanchiment présentés par l'usage d'Internet.

Enfin, tant l' « anonymat relatif » du client, l'accentuation de la concurrence que la faible culture de risque de certains prestataires de services sur Internet appellent à la prudence s'agissant de la maîtrise des risques sur les clients et les contreparties (point 6.).

Les recommandations relatives à la maîtrise des risques, tant au niveau de l'agrément qu'en matière de contrôle permanent figurent dans la **troisième partie.** Elles revêtent un caractère de bonnes pratiques et portent :

- sur l'assise financière et le suivi de la rentabilité (point 7.) ;
- sur la maîtrise des risques opérationnels (point 8.) ;
- sur la maîtrise du risque sur les clients (point 9.).

A ce titre, les établissements de crédit et les entreprises d'investissement sont invités à prendre connaissance des bonnes pratiques qu'exposent ce Livre blanc et son annexe technique, qui présente un guide d'élaboration d'une politique de sécurité Internet rédigé par le Forum des compétences.

PREMIÈRE PARTIE

L'ACCÈS A L'EXERCICE D'ACTIVITÉS BANCAIRES ET FINANCIÈRES SUR INTERNET

L'ACCÈS A L'EXERCICE D'ACTIVITÉS BANCAIRES ET FINANCIÈRES SUR INTERNET

1. L'exercice d'activités bancaires et financières sur Internet introduit-il une nouvelle problématique en matière d'agrément des opérateurs ?

Apparue il y a quelques années, l'offre de services bancaires et financiers sur Internet continue aujourd'hui à se développer et à conquérir de nouveaux publics. La France et l'ensemble des pays européens connaissent ainsi un mouvement comparable à celui déjà constaté aux États-Unis.

Ce développement est bien évidemment lié au formidable essor de la " nouvelle économie " qui se met en place sur le réseau mondial. Au cœur des nouveaux services, dits de la " société de l'information " - il s'agit de l'expression choisie par la directive « commerce électronique » pour désigner les services offerts sur Internet - les services bancaires et financiers sont en effet particulièrement recherchés par l'ensemble des acteurs du commerce électronique en ce qu'ils permettent la réalisation des opérations de paiement qui sont essentielles à la conclusion en ligne de relations commerciales.

Mais leur développement tient également dans la demande grandissante de la clientèle bancaire et financière d'accéder sur le réseau à une offre équivalente à celle dont elle peut déjà disposer dans les agences des établissements. Ce sont ces spécificités, notamment la facilité d'utilisation, qui favorisent ainsi l'émergence de l'offre de services bancaires sur Internet.

Les autorités d'agrément françaises ont suivi ces évolutions, notamment au travers des différents projets de création d'établissements se destinant à une offre de services par Internet. Elles ont également eu à répondre aux nombreuses questions juridiques posées par les professionnels ou leurs conseils concernant l'exercice de telles activités. Elles ont pu à cette occasion porter une appréciation sur l'impact de l'Internet dans les modes de réalisation des opérations de banque ou des services d'investissement.

1.1. Internet et l'exigence d'une autorisation pour exercer des activités bancaires et financières

Réaliser des opérations bancaires ou financières par Internet ne constitue pas un type nouveau d'activité. Le réseau joue simplement le rôle d'un nouveau média permettant l'exercice de ces opérations à distance, sans considération de frontières géographiques.

Internet offre de fait à chaque site web la possibilité d'accès à un marché mondial. C'est même ce sentiment d'ubiquité qui a pu amener certains acteurs du réseau à défendre l'idée d'un espace nouveau parce que délocalisé et constitué uniquement de rapports entre ordinateurs, échappant aux droits nationaux des États. Cette idée originelle est bien entendu contestable et il est largement reconnu désormais, tant en France qu'à l'étranger, que chaque acteur du monde Internet, consommateur, fournisseur d'accès, hébergeur et offreur, reste soumis

aux dispositions des droits nationaux applicables aux opérations qu'il exerce, comme le rappelle le Conseil d'Etat dans son rapport *" Internet et les réseaux numériques "* de 1998.

Ainsi, les opérations de banque ou les services d'investissement effectués sur Internet sont couverts par les réglementations générales et sectorielles applicables à ces activités.

À ce titre, comme dans la plupart des États, l'exercice de ces opérations est réservé, en France, à des entreprises ayant obtenu un agrément en qualité d'établissement de crédit ou d'entreprise d'investissement de la part des autorités compétentes. Pour l'ensemble des opérations bancaires et financières, à l'exception du service d'investissement de la gestion de portefeuille pour le compte de tiers, pour lequel la Commission des opérations de bourse est seule compétente, c'est le Comité des établissements de crédit et des entreprises d'investissement (CECEI) qui est chargé, par la loi bancaire du 24 janvier 1984 et la loi de modernisation des activités financières du 2 juillet 1996, de délivrer ces agréments.

L'exercice d'opérations bancaires ou financières sur le réseau requiert donc que son promoteur dispose d'un agrément en qualité d'établissement de crédit ou d'entreprise d'investissement, si cela n'est pas déjà le cas. De même, si son activité sur Internet s'élargit à de nouveaux services non couverts par le champ de l'agrément qui lui a été accordé précédemment, il devra veiller à demander l'élargissement de celui-ci.

L'agrément ne se réduit pas à la délivrance d'une autorisation d'exercer. La procédure prévue par la législation et la réglementation est destinée à garantir l'aptitude des opérateurs à exercer en toute sécurité des activités liées à la manipulation d'avoirs monétaires ou de titres pour le compte de leur clientèle. Les autorités doivent donc veiller au respect par les prestataires d'un certain nombre d'exigences portant sur le montant de leurs ressources et la solidité de leur actionnariat, sur l'honorabilité et l'expérience de leurs dirigeants, ainsi que sur les moyens techniques de leur organisation. Dans le cadre des missions qui lui sont dévolues par la loi bancaire, le Comité des établissements de crédit et des entreprises d'investissement procède à un examen approfondi tant du programme d'activités et des moyens techniques et financiers appelés à être mis en œuvre que de l'aptitude des candidats à réaliser des objectifs de développement dans des conditions compatibles avec le bon fonctionnement du système bancaire. Parallèlement, et conformément à la loi de modernisation des activités financières, le CECEI réalise un examen similaire lors de l'agrément relatif à la prestation de services d'investissement, sur la base d'une approbation des programmes d'activités par le Conseil des marchés financiers et, le cas échéant, par la Commission des opérations de bourse.

Est-il possible sur ces bases de conclure que l'exercice d'activités bancaires et financières par Internet n'emporte aucune conséquence en matière d'agrément ?

Le fait même que les opérations effectuées par Internet continuent à relever du droit bancaire et financier existant pose nécessairement la question de savoir si les exigences qui fondent aujourd'hui la délivrance de l'agrément demeurent adaptées. Les réflexions qui suivent permettent de tracer les changements qu'introduit l'usage d'Internet dans l'exercice d'opérations bancaires et financières. Elles font apparaître des questions tenant à l'aptitude des acteurs à effectuer ces services, à la licéité de pratiques nouvelles, à la modification de la relation entre le prestataire et son client, ainsi qu'au caractère transfrontalier de l'offre.

1.2. Une nouvelle donne pour l'offre de services bancaires et financiers

Internet transforme profondément la relation entre l'opérateur et ses clients en permettant à ceux-ci de s'informer et de décider à distance, éventuellement par delà les frontières des États, tout en bénéficiant d'une plus grande diversité de propositions de services et d'une plus grande concurrence des offres.

1.2.1. Une nouvelle relation clientèle

Originellement réduits à de simples sites " vitrine " présentant l'entreprise, les sites web bancaires français ont maintenant évolué vers de véritables sites transactionnels où la clientèle de l'établissement peut obtenir des informations sur les produits bancaires proposés, suivre ses comptes, effectuer des opérations liées à la gestion de ceux-ci (virements, commandes de chéquiers), voire contracter des prêts ou réaliser des opérations d'investissement.

L'ouverture d'un site web modifie dès lors le rapport que le prestataire entretient avec sa clientèle. La relation en agence est réduite et le client dispose désormais d'un service convivial et complet de banque à domicile. Le déplacement au guichet peut même être potentiellement supprimé si l'établissement fait ce choix et trouve une clientèle acquise au confort d'une relation totalement dépersonnalisée.

Deux types de sites doivent ainsi être différenciés. À l'image des services **audiotel** et minitel plus anciens, certains ne sont pour le client que de simples outils d'information et de réalisation d'opérations qui constituent le prolongement d'une relation établie au préalable en agence. D'autres, au contraire, se conçoivent totalement comme un service en ligne (*on line banking* ou *on line brokerage*), et acceptent que la relation contractuelle initiale (par exemple l'ouverture d'un compte) soit conclue à distance de même que les opérations de gestion qui suivent. C'est ce second type de site web bancaire ou boursier qui devrait seul retenir la qualification de " banque/entreprise d'investissement sur Internet " ou de " banque/entreprise d'investissement virtuelle ", ce qui induit l'idée que ces établissements n'ont pas d'implantation physique destinée à l'accueil de la clientèle. Les premiers sites ne sont que des services d'accès à distance à l'établissement et sont complémentaires de la relation d'agence déjà établie.

Cette deuxième situation concerne encore peu d'établissements bancaires en France, comme dans les autres pays. Elle est cependant déjà choisie par la plupart des sites boursiers spécialisés pour attirer plus facilement une clientèle nouvelle. Ce mode de relation complètement " virtuel " va donc se développer. Il est en effet moins coûteux pour les nouveaux entrants sur ce marché qui peuvent ainsi se dispenser d'un réseau d'agences. En outre, un certain nombre de textes législatifs d'ordre communautaire ou national favorisant le commerce électronique viendra prochainement encadrer ce mode d'offre de services en élaborant un cadre juridique reconnaissant la validité de ces pratiques**.** C'est le cas de la directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur ("directive sur le commerce électronique"), de la directive 1999/93/CE du Parlement européen et du Conseil, du 13 décembre 1999, sur un cadre européen pour les signatures électroniques,

ainsi que de la proposition de directive concernant les services financiers à distance. C'est le cas également de la prochaine loi française relative à la société de l'information.

Enfin, la technologie de l'Internet continue, quant à elle, à se perfectionner pour faciliter cette progression en répondant aux réticences liées à une relation dépersonnalisée (incrustation de la voix et de l'image sur la page web par exemple). Bien entendu, le choix entre ces deux modes opératoires n'est pas antinomique et ceux-ci peuvent tout à fait coexister sur un même site de façon à satisfaire des clientèles de profils différents.

La création d'une banque ou d'une entreprise d'investissement virtuelle, même si elle peut déboucher sur une exploitation moins coûteuse compte tenu de la diminution des structures commerciales, doit cependant prévoir un investissement élevé pour l'achat du système d'information matériel et logiciel, son installation et la recherche de la clientèle. Ce dernier aspect acquiert même des proportions très importantes dans le plan de développement des sociétés qui ouvrent un site Internet, avec un retour sur investissement souvent très tardif. Les budgets publicitaires très importants qui y sont consacrés doivent ainsi être mis en perspective avec la grande fragilité de la relation clientèle qui s'instaure. En effet, pouvant en permanence comparer les offres et faire jouer la concurrence, l'adhésion commerciale à un site du client internaute est volatile.

La maîtrise de ces investissements et le bon équilibre financier de l'exploitation de tels systèmes sont donc particulièrement importants s'agissant d'activités relatives à la réception de fonds et à l'épargne publique.

La clientèle tire un avantage de l'utilisation de ce canal de distribution à la fois parce qu'elle peut légitimement en attendre une baisse des frais liés aux opérations qu'elle effectue et parce qu'elle peut plus aisément comparer les offres concurrentes avant de s'engager. Il est à noter cependant qu'elle se trouve soumise au dispositif technique mis en place par le prestataire, tel qu'il résulte notamment du mode d'enchaînement des écrans, du contenu informatif délivré et du système de validation des ordres. Bien souvent, le client sera alors en situation de devoir adhérer à telle ou telle proposition sans avoir pu en modifier ses caractéristiques et sans avoir pu en discuter avec un conseiller commercial de l'établissement. C'est pourquoi la capacité d'un consommateur à disposer d'une bonne connaissance des conditions de son engagement dans un environnement Internet est une préoccupation majeure des autorités.

Le développement de la banque et de la finance sur Internet suppose que la clientèle adhère à ce nouveau mode de relation. Or cela ne pourra se faire sur la base du seul avantage d'un confort d'utilisation de la part du client. Ce dernier attend légitimement un service assorti des meilleures conditions de sécurité en raison de la sensibilité du contenu des informations financières échangées *via* le réseau et traitées sur les ordinateurs du prestataire. Il attend également des assurances concernant l'identité de l'opérateur. Celles-ci sont essentielles compte tenu des nombreux risques de malveillance informatique existant sur ce réseau ouvert. Elles le sont également dans la mesure où l'émergence de l'exercice d'activités bancaires et financières sur Internet fait apparaître de nouveaux acteurs et de nouvelles pratiques.

1.2.2. De nouveaux opérateurs et de nouvelles pratiques

En se développant, l'offre de services bancaires et financiers sur **Internet** dépasse la sphère des seuls établissements de crédit et des prestataires de services d'investissement existants. Elle attire de nouveaux opérateurs, venant d'autres métiers, notamment l'informatique, et désireux d'exercer ces activités. **Il est aussi fréquent, dans ce domaine dominé par la maîtrise de technologies nouvelles, que les établissements de crédit et les entreprises d'investissement délèguent à des prestataires externes la conception, la mise en œuvre, voire l'exploitation de leur site Internet. Les autorités d'agrément doivent sur ce point veiller à ce que les opérateurs agréés gardent la responsabilité et la maîtrise des services bancaires et financiers effectués par ce moyen.**

En outre, comme pour d'autres services proposés sur la toile mondiale, apparaissent de nouveaux modes d'intermédiation pour la présentation des offres. C'est, par exemple, la création par des sociétés non-établissements de crédit ou non-prestataires de services d'investissement, de portails rassemblant, autour d'un contenu de nature informative, un ensemble de liens hypertextes vers les sites de prestataires partenaires dont l'offre est éventuellement décrite. **L'utilisation d'Internet renforce de ce fait la nécessité pour la clientèle de pouvoir disposer d'une information sûre concernant l'identité de l'opérateur et sa capacité juridique à offrir ses services. Les autorités devraient en conséquence veiller à adapter les procédures existantes dès lors que des services en ligne sont proposés.**

Par ailleurs, la sensibilité du réseau aux actes de malveillance informatique offre un terrain particulièrement propice à l'ouverture clandestine de sites proposant des services bancaires et financiers sans disposer d'un agrément à cet effet, voire à la contrefaçon de sites régulièrement constitués. Ce risque amène naturellement les autorités en charge du respect des obligations liées à l'agrément à renforcer leur vigilance concernant de tels prestataires.

Enfin, le sentiment de nouveauté et de liberté qu'inspire le réseau mondial a naturellement suscité l'apparition de pratiques douteuses en matière d'intermédiation bancaire et financière, comme l'usage de monnaies " privées ", plus ou moins liées à des systèmes de fidélisation, ou la mise en œuvre de systèmes de troc de biens et de services. **Certaines activités d'intermédiation, comme celles pouvant consister à gérer des moyens de paiement, qui peuvent se situer en dehors du périmètre des opérations réservées aux établissements de crédit à l'étranger, sont également susceptibles, lorsqu'elles sont exercées en France, d'entrer dans la définition des opérations de banque faite par la loi bancaire**. Elles peuvent alors comporter des risques sur le bien collectif que sont les moyens de paiement et nécessitent donc une veille particulière des autorités monétaires. Ainsi, sur cette question des activités exercées sur Internet également, la vérification de la licéité des opérations par les autorités en charge de l'agrément est essentielle pour protéger la clientèle et assurer à l'ensemble des prestataires de l'Internet des conditions égales d'exercice des activités.

1.2.3. La nature transfrontalière de l'offre

Plus que la dépersonnalisation et l'automatisation, Internet présente pour caractéristique essentielle la distance dans les rapports client-fournisseur. Cet éloignement ne contrarie pas

l'internaute puisqu'il peut " dialoguer " avec l'opérateur, c'est-à-dire obtenir les informations qu'il recherche et passer des ordres. Chacune des parties opère ainsi sur le réseau via un ordinateur dont l'éloignement géographique et l'implantation sont indifférents. La localisation de ces machines est constituée par leur adresse sur le réseau. Celle d'un site web est enregistrée auprès des instances chargées de l'administration des noms de domaine qui sont organisées sur des bases nationale et mondiale. Il est toutefois à noter que malgré le rattachement indicatif à un pays, la localisation d'un site reste incertaine compte tenu de la nature même du réseau ouvert qui est construit en maillage, de ses nombreuses possibilités de reroutage et de la liberté de l'enregistrement de sites auprès d'autres autorités nationales que celles du lieu d'implantation du prestataire (par exemple l'enregistrement d'un opérateur français en " .com ", auprès des instances américaines).

En matière bancaire et financière, où les opérations sont réservées à des établissements régulièrement agréés par les autorités du pays dans lequel ils exercent une activité, cette dimension transnationale présente un certain nombre de difficultés, essentiellement pour ce qui concerne les établissements autorisant la clientèle à traiter entièrement par le réseau.

Le service étant réalisé à distance, deux questions essentielles se posent. Il faut d'abord déterminer si l'opérateur dispose de la capacité juridique à exercer son activité sur un territoire donné, notamment si celle-ci est effectuée dans un autre État que celui de son lieu d'établissement. Il est ensuite important de connaître le droit applicable aux opérations qui vont être conclues avec une contrepartie non-résidente.

Bien sûr, l'exercice d'activités bancaires et financières transfrontalières n'est pas nouveau. Ces situations sont traitées par des dispositions adéquates des droits nationaux des États et du droit international. Fondé sur le principe de la reconnaissance mutuelle des agréments, le droit européen, qui concourt à la mise en œuvre d'un vaste marché unique, offre même un cadre élaboré et harmonisé. **Mais les spécificités de l'utilisation d'Internet, qui tiennent à l'abolition des distances et au caractère transactionnel des ordres, peuvent compliquer l'interprétation des textes existants. Ainsi, il peut être difficile d'apprécier la localisation des opérations et de déterminer si elles sont effectuées auprès du prestataire ou auprès du client.** De même, le caractère mondial du réseau oblige naturellement à favoriser l'émergence de standards internationaux quant à la stabilité des acteurs et à la sécurité des clients et des marchés.

L'approfondissement de la réflexion sur ces points est important pour permettre aux autorités en charge de l'agrément de mesurer la légalité et la sécurité des opérations effectuées sur Internet.

Il est ainsi constaté que l'offre de services bancaires et financiers par Internet modifie sensiblement les conditions traditionnelles d'exercice de ces activités. L'essor de ce nouveau mode de relation d'affaires, qui facilite l'établissement de contrats transfrontaliers et qui modifie la relation avec la clientèle tout en suscitant l'apparition de nouveaux acteurs, amène les autorités à clarifier un certain nombre de situations et à préciser certaines exigences liées à l'agrément concernant les conditions d'accès à une telle activité et au droit applicable aux opérations.

2. Les conditions d'accès à l'activité bancaire ou financière sur Internet

2.1. La capacité à agir du prestataire

Un prestataire bancaire ou financier peut exercer sur un territoire donné comme la France, seul ou avec l'aide d'intermédiaires, différents types d'activités allant de la simple offre de services à la réalisation de la prestation bancaire ou financière proprement dite. La limite entre ces deux types d'activité est parfois ténue, notamment lorsqu'ils s'exercent sur la " toile ", mais leur régime juridique doit être différencié. La fourniture du service bancaire ou financier relève des dispositions requérant l'agrément ou l'autorisation d'exercer. Ainsi, seuls les établissements de crédit régulièrement agréés en France ou pouvant se prévaloir d'un agrément du même type délivré par une autre autorité de l'Espace économique européen, peuvent réaliser des opérations bancaires en France. Il en va de même pour les entreprises d'investissement pour la fourniture de services d'investissement. Mais la réalisation sur notre territoire de simples offres de services, sans accomplissement des prestations correspondantes, relève seulement des dispositions relatives à la sollicitation de la clientèle et non directement du droit de l'agrément.

Chacun de ces régimes juridiques impose un certain nombre de conditions pour la reconnaissance de la capacité d'un acteur à réaliser ces activités sur le territoire français. On distinguera donc la question de la capacité à agir selon chacun de ces deux types d'opérations.

2.1.1. La capacité d'un prestataire à exercer des activités bancaires ou financières en France

S'agissant, en matière bancaire et financière, d'activités soumises à autorisation préalable, les autorités en charge de l'agrément détermineront si un prestataire intervenant par Internet exerce illégalement des activités sur leur territoire de compétence. Cela pose la question de savoir où est exercée la prestation pour laquelle un agrément est requis.

Par rapport aux relations d'affaires établies avec des pays tiers, celles conclues au sein de l'Europe s'inscrivent sur ce point dans un cadre juridique plus simple puisque le marché unique européen offre aux prestataires de l'Espace économique européen une liberté de prestation de services au sein de la zone toute entière sur le fondement de l'agrément reçu dans leur pays d'origine. On raisonnera donc d'abord sur la base de situations générales applicables aux prestations en provenance ou à destination de pays tiers à l'Espace économique européen puis on étudiera spécifiquement le cadre européen.

2.1.1.1. La détermination du lieu d'exercice des opérations

Les services bancaires et financiers réservés aux seules entreprises agréées en qualité d'établissement de crédit ou d'entreprise d'investissement en France sont définis par les articles 1 à 4 de la loi bancaire et 4 de la loi de modernisation des activités financières.

Lorsque le prestataire sur Internet offre de conclure immédiatement par voie électronique une opération de banque ou de fourniture de services d'investissement, il est essentiel, pour savoir si cette opération entre dans le champ d'application du monopole prévu par les lois françaises, de déterminer le lieu où cette opération est effectuée.

Comment déterminer dès lors si l'opération réservée est effectuée au lieu d'implantation du prestataire ou à celui du client ?

Il nous semble qu'il faut considérer que le réseau Internet n'est qu'un moyen technique de communication à distance permettant à un internaute quel qu'il soit d'entrer en relation avec un service prévu à cet effet par un opérateur déterminé. En matière informatique en effet, cette relation consiste simplement en un accès à distance à un serveur par un poste client.

Au plan des principes, il faudra donc rechercher le lieu d'accomplissement de la prestation caractéristique du contrat. Celle-ci est entendue comme la prestation pour laquelle le paiement est dû. Dans certaines situations, elle pourrait être difficile à identifier, comme dans le cas de la négociation pour compte propre, ou lorsque le service est exécuté dans un pays autre que celui du client ou celui du prestataire. Cela étant, il y aura généralement lieu de considérer que les opérations concrètes d'ouverture de compte et de gestion des opérations, qui caractérisent les services bancaires et financiers, même commandées par un client situé à l'étranger, s'effectuent sur les ordinateurs et au sein du système d'information et de gestion du prestataire, donc normalement au lieu de son implantation administrative ou opérationnelle (opérations sur les comptes tenus dans ses livres, octroi de crédit par inscription en compte ou virement, passation d'ordres sur le marché réglementé auquel il accède). S'il y a dissociation entre le lieu où est implanté le serveur hébergeant le site du prestataire et le lieu de son système de gestion, où sont tenus les comptes, il y aura lieu de considérer ce dernier comme pertinent.

Bien évidemment, la réalité des schémas de fonctionnement mis en œuvre par certains prestataires peut être plus compliquée et, par exemple, mobiliser en relais les services d'un correspondant dans le pays du client pour faciliter à ce dernier la réalisation de ses opérations transitant par les systèmes de paiement ou de règlement-livraison domestiques. Dans de tels cas, il appartient aux autorités d'apprécier s'il y a réalisation d'opérations bancaires ou financières en France.

De même, l'interprétation doit être différente de celle donnée pour le cas général exposé plus haut si Internet permet au prestataire de réaliser le service en " apportant " l'objet de celui-ci directement sur l'ordinateur du client. Cela pourrait par exemple être le cas dans l'hypothèse où un prestataire effectuerait une mise à disposition de monnaie électronique depuis son site directement sur le poste du client ou sur la carte dite " porte-monnaie électronique " insérée dans un lecteur attaché à ce poste. Néanmoins, ces cas restent pour l'instant marginaux. Il pourrait également en être autrement si les prestations caractérisant le contrat n'étaient effectuées ni au lieu d'établissement du prestataire, ni sur l'ordinateur du client, mais néanmoins dans le pays du client (octroi des fonds directement sur un compte localisé dans ce pays par exemple, mise à la disposition du public d'un moyen de paiement tel une carte de retrait ou une carte de paiement).

La seule ouverture d'un site web bancaire ou financier, par nature accessible à distance et donc de l'étranger, ne place donc pas son promoteur en situation d'exercice illégal de la profession sur d'autres territoires que celui de son lieu d'établissement. De même, la connexion d'un client originaire d'un État autre que celui du site bancaire ou financier, à l'image du déplacement physique à l'étranger de celui-ci dans une agence de l'établissement, ne doit pas *ipso facto* faire considérer que le prestataire exerce *via* son site une activité sur le territoire du client.

2.1.1.2. Les différents cas d'exercice par Internet d'opérations bancaires ou financières en France

Pour l'autorité d'agrément, différents cas de figure sont à analyser pour déterminer la réalisation en France d'opérations soumises à autorisation.

Le cas des entreprises de droit français qui exercent leur activité sur Internet avec la clientèle française ne pose évidemment pas de problème de localisation du service. Comme pour des services effectués en agence, une telle activité est soumise à l'agrément du CECEI.

Quelle est en revanche la situation des sociétés implantées à l'étranger qui exerceraient des opérations bancaires ou des services d'investissement en France ? Le CECEI doit apprécier si l'exercice de leur activité nécessite qu'elles se mettent en conformité avec les dispositions relatives à l'agrément en France. Or, certaines pourront avoir spontanément fait le choix d'ouvrir une structure agréée, alors que d'autres choisiront des modes d'établissement des relations d'affaires ne faisant pas appel à une entité régulièrement habilitée. L'attention de ces sociétés doit alors être portée sur le fait que certains de ces modes peuvent être considérés par le CECEI comme des cas de présence permanente en France, nécessitant un agrément.

Dans tous les cas, il doit bien entendu être rappelé que l'obligation d'agrément s'applique aux activités bancaires et financières telles que définies par la loi bancaire et la loi de modernisation des activités financières, et non telles que définies par la législation du pays d'origine desdites sociétés.

2.1.1.2.1. Le choix de l'ouverture d'une structure agréée

Il est possible que le prestataire d'un pays tiers à l'Espace économique européen, qui désire offrir ses services à la clientèle française, choisisse de lui-même de s'établir en France en ouvrant une filiale ou une succursale qui mettra en œuvre un service sur Internet à destination de cette clientèle. Cette démarche peut être motivée par des considérations commerciales en ce qu'elle permet au prestataire de mieux se faire connaître auprès du public et de rassurer sur la pérennité de son offre. Il est en effet fréquent que la prestation en ligne s'assortisse de la création d'un réseau minimal d'agences destinées au contact avec la clientèle et à la promotion de l'offre sur Internet.

Vis-à-vis des autorités françaises, l'entreprise aura alors à solliciter un agrément pour la création de la filiale ou de la succursale et sera par ailleurs soumise aux dispositions françaises de nature législative ou réglementaire relatives à l'exercice d'activités bancaires ou financières (sur les modalités précises d'ouverture de cette implantation et sur la doctrine du CECEI en la

matière, voir le *Rapport annuel pour 1999* du Comité des établissements de crédit et des entreprises d'investissement, points 8.2.1 et suivants).

La situation peut évidemment être moins simple. En effet, l'apport technologique d'Internet facilite la sollicitation sur le réseau, par des offreurs opérant depuis leur pays d'établissement, d'une clientèle résidant dans un autre État. Les autorités françaises doivent dès lors analyser au cas par cas si de telles activités, lorsqu'elles sont effectuées en France, ne doivent pas être considérées comme constituant une présence permanente de l'offreur en infraction avec le monopole bancaire et financier posé par la loi bancaire et la loi de modernisation des activités financières (voir point 2.1.3).

2.1.1.2.2. Cas s'apparentant à une présence permanente en France

Bien avant l'essor d'Internet, le CECEI a eu à examiner la question du champ d'application territorial des dispositions posées par la loi bancaire concernant le monopole des activités en France. Ce point est en effet essentiel au respect de conditions égales de concurrence pour l'ensemble des prestations exercées en France et pour la protection de l'épargne et la sécurité des paiements. **Le CECEI a ainsi pu considérer que les formes de présence entretenues de façon permanente par des établissements étrangers sur notre territoire pouvaient être assimilées à un exercice d'opérations bancaires en France, dès lors que les clients français étaient dispensés de s'adresser directement à l'opérateur étranger et qu'ils pouvaient conclure valablement en France.**

Ainsi, le fait pour un prestataire étranger de proposer ses services en France, en y ouvrant un simple bureau géré par le personnel de l'entreprise, ou en mandatant un intermédiaire qui y est établi durablement, peut constituer une présence permanente de cet établissement sur notre territoire dès lors que la clientèle française pourra se dispenser de s'adresser directement à lui et que l'opérateur étranger se reconnaîtra valablement engagé par les actes conclus par l'entremise du bureau ou de l'intermédiaire. Dès lors, ces activités devront être autorisées par l'autorité d'agrément française.

Bien entendu, dans l'appréciation de cette position, le CECEI a tenu compte dès 1993 de l'ouverture du marché unique des services bancaires et financiers pour les activités exercées de cette manière par les établissements installés dans l'Espace économique européen. Il est alors admis que le prestataire d'un autre État membre exerce ses activités en libre établissement. Cette position a été exposée à la Commission européenne et a encore été rappelée pour les services d'investissement dans le rapport au Comité *" La libre prestation de services en matière de services d'investissement "* (novembre 1998). Les raisonnements qui suivent traiteront donc du cas de prestataires installés dans des pays tiers à l'Espace économique européen. La situation des pays appartenant à l'Espace économique européen est analysée au point 2.1.1.2.3.

La technologie du réseau Internet aidant, il est probable que des prestataires étrangers ne disposant pas de structures agréées en France tentent de développer une présence sur Internet en France pour approcher avec la plus grande efficacité commerciale la clientèle française. Il convient alors de qualifier ces formes de présence pour considérer si elles constituent une présence permanente en France. Plusieurs cas sont envisageables :

a) Le prestataire ouvre en France un site web présenté en français, en y localisant un serveur et en affichant éventuellement à la clientèle française un nom de domaine en " .fr ". Il souhaite ainsi cibler la clientèle française en lui présentant une offre adaptée au marché français et en la rassurant sur l'origine géographique de son offre, alors que les opérations bancaires ou financières pourront continuer à être *in fine* réalisées au lieu où le prestataire a son administration et son système de gestion. Dès lors que la localisation géographique en France de l'installation serait certaine, et que l'on pourrait considérer que la clientèle française n'a dès lors qu'à s'adresser au serveur situé en France pour conclure valablement des opérations avec le prestataire, le serveur pourrait être assimilé à une présence permanente de l'opérateur en France. Un tel dispositif obligerait le prestataire, conformément aux critères posés par le CECEI, à requérir l'ouverture d'une filiale ou d'une succursale dûment agréée.

b) De la même façon qu'il est décrit ci-dessus, le prestataire peut ouvrir un site en France mais en destinant celui-ci à la simple information du public et non à la réalisation d'opérations de banque ou de services d'investissement. Il s'agira ainsi, par exemple, de diffuser des communications relatives à la société. Le site remplirait alors la fonction habituelle d'un bureau de représentation et devrait donc, conformément à la loi, notifier sa demande d'ouverture au CECEI (articles 9 de loi bancaire et 81-I de la loi de modernisation des activités financières).

c) L'inscription sur un site portail français d'un lien hypertexte renvoyant vers le site d'un prestataire étranger est plus difficile à caractériser. En effet, un tel lien n'est pas toujours établi sur demande ou même accord du site destinataire. De nombreux annuaires ou portails composent eux-mêmes de véritables " bouquets de services ", de sorte qu'il est difficile de déterminer si le prestataire a réellement souhaité être présent par ce moyen sur les sites du réseau localisables en France. Cela pourrait toutefois être le cas si le lien hypertexte était accompagné par exemple des signes commerciaux distinctifs de l'établissement étranger (logo, message commercial) car ce type d'affichage est le plus souvent caractéristique d'un véritable partenariat entre le portail et le prestataire. La question se pose alors de savoir si l'opérateur, dont le site lui-même reste localisé à l'étranger, remplit les critères posés par le CECEI pour déterminer une présence permanente en France. Même si une analyse des situations particulières est nécessaire, il semble que dans ce type de relation, le client ne peut conclure avec l'intermédiaire un contrat engageant valablement l'opérateur étranger. Il ne dispose de fait que d'un accès simplifié au site de celui-ci mais il doit prendre l'initiative de s'y connecter. Les critères posés par le CECEI ne seront donc vraisemblablement pas remplis. En revanche, à défaut de présence permanente il pourra quand même s'agir d'une sollicitation de la clientèle française exercée sur le territoire français. Celle-ci entrerait alors dans le champ des dispositions relatives à la publicité et au démarchage.

Il se peut également que, sur la base de partenariats avec des établissements de crédit ou des entreprises d'investissement français disposant de sites Internet, le prestataire soit accessible aux clients français de ces sites par un lien hypertexte. Dans cette hypothèse, le site du prestataire français proposerait la commercialisation de services réalisés par le prestataire étranger. Cette situation doit être distinguée de la simple relation de type " correspondent

banking " qui fait intervenir deux opérateurs pour exécution des ordres de l'un sur le marché de l'autre. En la matière, le CECEI a jusqu'à présent réservé sa position et n'a pas considéré que le recours à un partenariat avec un établissement dûment agréé devait requérir une habilitation quelconque en France du prestataire étranger.

Pour l'interprétation de l'ensemble de ces situations, qui peuvent présenter une grande variété dans les dispositifs techniques mis en œuvre, la Banque de France et la Commission bancaire adhèrent au principe d'utilisation d'un faisceau d'indices permettant de distinguer l'exercice d'activités réglementées en France.

2.1.1.2.3. Internet et le marché unique européen des services bancaires et financiers

Conformément aux directives bancaires et financières, les législations nationales des États membres soumettent l'exercice d'opérations de banque et de services d'investissement à la délivrance d'une autorisation préalable par les autorités compétentes.

Les prestataires ainsi agréés bénéficient, sur le fondement du Traité de Rome, de la deuxième directive de coordination bancaire et de la directive sur les services d'investissement qui prévoient la reconnaissance mutuelle des agréments, d'une liberté d'établissement et d'une liberté de prestation de services au sein de l'ensemble de la zone. Ces libertés sont destinées à faciliter et à favoriser l'exercice d'opérations transfrontalières.

S'agissant de la capacité juridique à exercer son activité, il ressort de ces textes qu'un prestataire de l'Espace économique européen peut agir sur la base de l'agrément dont il dispose dans son pays d'origine, soit en bénéficiant de la liberté d'établissement, soit de la liberté de prestation de services. Celles-ci supposent néanmoins une information préalable des autorités conformément aux articles 19 de la deuxième directive de coordination bancaire et 18 de la directive sur les services d'investissement. Bien entendu, la reconnaissance de ces libertés ne vaut qu'au sein de l'espace économique européen et ne saurait signifier qu'une succursale établie dans un pays tiers par un établissement de crédit communautaire peut offrir ses services au sein de l'Union européenne.

La question se pose donc de savoir si la réalisation d'opérations de banque ou de services d'investissement par Internet, entre des parties qui résident dans des États membres différents, entre dans l'une ou l'autre de ces modalités d'exercice et entraîne une telle obligation d'information. Celle-ci concourt, notamment, à la bonne information des clients sur la capacité du prestataire à exercer son activité sur leur territoire.

À moins que le prestataire n'installe un site web dans le pays du client (installation d'un serveur, choix d'un nom de domaine suffixé par le sigle du pays, etc.) ou ne recoure à des formes d'implantation telles que décrites précédemment (ouverture d'une filiale ou d'une succursale), la délivrance de services bancaires ou financiers sur son site ne peut manifestement pas s'apparenter à une présence permanente dans le pays du client, ni donc relever du droit d'établissement.

Quant à l'assimilation de la prestation par Internet à une libre prestation de services, la Commission européenne a pris position dans sa " communication interprétative relative à la libre prestation de services et à l'intérêt général dans la deuxième directive de coordination bancaire " (10/7/97). Elle a considéré que " la fourniture de services bancaires à distance, par exemple par Internet, ne devrait pas, selon [elle], nécessiter de notification préalable dans la mesure où le prestataire ne peut être considéré comme exerçant ses activités sur le territoire du client ". Elle ajoutait immédiatement être " consciente du fait que cette solution nécessitera une analyse au cas par cas, qui peut s'avérer difficile ".

La difficulté juridique est de savoir si un prestataire a **eu l'intention d'exercer son activité sur le territoire d'un autre État membre**. La Commission semble considérer que la prestation par Internet reste localisée sur les ordinateurs du prestataire, qui n'intervient donc pas sur le territoire du client.

Le CECEI et les autres autorités françaises compétentes ont réservé leur position sur ce point dans un rapport de novembre 1998 intitulé " *La libre prestation de services en matière de services d'investissement* ". Conformément aux principes posés par le Comité, il est en effet important d'apprécier la **réalité de la volonté** du prestataire d'entrer en relation d'affaires avec une clientèle non-résidente. La prestation par Internet peut donc s'apparenter à une libre prestation de services dès lors que l'intention du prestataire est caractérisée.

1. Faisceau d'indices pour caractériser les cas entrant dans le champ de la libre prestation de services

Afin de mieux caractériser les cas entrant dans le champ de la libre prestation de services au sein de l'Espace économique européen, nous proposons qu'à défaut de manifestation expresse de cette volonté par l'établissement lui-même, les autorités d'agrément et de contrôle considèrent que le prestataire " désire exercer pour la première fois " ses activités sur le territoire d'un autre État membre dès lors que sont réunis tout ou partie des indices suivants :

- **la conclusion d'opérations bancaires ou financières peut être réalisée à distance sur le site du prestataire par un client non résident, sans que celui-ci soit obligé d'établir au préalable en agence une première relation contractuelle comme l'ouverture d'un compte ;**

- **le prestataire propose des services via un correspondant dans le pays du client ;**

- **le site est présenté dans la langue du pays du client ;**

- **le site du prestataire est accessible via des portails localisés dans le pays du client ;**

- **le site du prestataire est référencé dans les moteurs de recherche du pays du client ;**

- **le prestataire a recours à des bandeaux publicitaires associés à un lien hypertexte sur des sites du pays du client ;**

- **le prestataire a recours à des envois de mailings auprès de clients résidant dans d'autres États membres ;**

- **le prestataire se fait connaître sur les forums de discussion spécialisés en matière bancaire et financière dans le pays du client ;**

- **le prestataire tend à introduire un doute quant à sa localisation géographique précise en utilisant un nom de domaine permettant de penser qu'il est installé dans le pays du client d'un autre État membre.**

Bien entendu, les éléments figurant ci-dessus ne sont pas tous de la même importance. C'est leur réunion qui permet la constitution d'un faisceau d'indices. Leur liste n'est pas limitative et peut être revue par les autorités compétentes en fonction de l'évolution des techniques et des pratiques utilisées sur le réseau.

Les autorités françaises rechercheront l'adhésion des autres autorités de l'Espace économique européen pour parvenir à une interprétation homogène des textes en vigueur.

Il peut exister des relations d'affaires transfrontalières sans que les indices énumérés ci-dessus soient réunis, de telle façon qu'il n'est pas possible de penser que le prestataire a souhaité exercer son activité sur le territoire du client. Il faudra alors considérer que le client est entré de lui-même en relation avec le prestataire et que ce dernier n'a pas à effectuer de démarche de déclaration de libre prestation de services auprès des autorités compétentes.

2.1.2. La capacité juridique d'un prestataire à solliciter la clientèle française

Parce qu'elle peut constituer la préfiguration de l'exécution d'une opération bancaire ou financière, l'offre de services faite à la clientèle par un prestataire, directement ou indirectement, est strictement encadrée par la législation française. Ainsi, le démarchage et la publicité relatifs à certains types d'offres sont soumis à conditions, le principe général étant que ces activités doivent être réservées à des entreprises habilitées à fournir les services correspondants sur le territoire français, ou à leurs intermédiaires.

Le prestataire peut ne pas se contenter d'offrir ses services aux seuls résidents de son État. Il peut entreprendre de diverses manières de faire des offres auprès de clientèles étrangères, soit en s'établissant dans leur État, soit en les sollicitant pour les attirer sur son site. **Les autorités françaises doivent ainsi, au cas par cas, examiner les conditions de la légalité des sollicitations effectuées sur le territoire français et vérifier si elles ne sont pas constitutives d'une forme d'implantation du prestataire en France.**

En effet, compte tenu du caractère ancien des textes relatifs à la sollicitation et de la variété des techniques d'offres employées sur Internet, cette analyse n'est pas toujours facile à mener. Plusieurs cas de figure sont détaillés ci-après.

2.1.2.1. La sollicitation de la clientèle

Hors les cas d'implantation dans un pays, il est très facile à un prestataire étranger de solliciter à distance la clientèle d'un autre État que le sien. En effet, les pratiques les plus fréquentes de recherche de la clientèle reposent classiquement sur la publicité ou le démarchage en direction des résidents d'un autre État.

Ces activités ne sont pas assimilables en elles-mêmes à la réalisation d'opérations de banque ou de services d'investissement. Elles n'emportent donc pas l'obligation d'un agrément au regard de la loi bancaire ou de la loi de modernisation des activités financières. Cependant, elles sont en France, lorsqu'elles ont pour objet une offre de certains services bancaires ou financiers, strictement réservées à des entités disposant d'un agrément et celles-ci font toujours l'objet d'un strict encadrement juridique. Ainsi, elles sont particulièrement encadrées lorsqu'elles sont initiées par des établissements de crédit ou des entreprises d'investissement étrangers.

2.1.2.1.1. La publicité

Aux termes du décret n°68-259 du 15 mars 1968, pris pour l'application de l'article 10 de la loi n° 66-1010 du 28 décembre 1966 relative à l'usure, aux prêts d'argent et à certaines opérations de démarchage et de publicité, " les personnes qui sont domiciliées ou qui ont leur

siège social hors du territoire de la République française doivent, préalablement à toute propagande ou publicité faite [sous quelque forme et par quelque moyen que ce soit, en vue de conseiller ou d'offrir des prêts d'argent ou de recueillir, sous forme de dépôts ou autrement, des fonds du public ou de proposer des placements de fonds], avoir désigné un mandataire domicilié ou ayant son siège social en France ".

De plus, " aucune propagande ou publicité en vue de recueillir auprès du public des dépôts à vue ou à moins de deux ans ne peut être faite par des établissements autres que les banques [établissements de crédit] inscrites et les organismes habilités à recevoir, sur le territoire de la République française, des dépôts de cette nature ". Il ne peut être fait de publicité offrant une rémunération des dépôts qui serait contraire à la réglementation en vigueur en France. Enfin, tant l'offreur que, le cas échéant, son intermédiaire, doivent clairement s'identifier auprès du public et lui indiquer leur localisation.

Le démarchage relatif à des opérations bancaires ou financières est également réservé à des établissements, ou à des personnes agissant sous leur responsabilité, autorisés à exercer en France.

2.1.2.1.2. Le démarchage

Aux termes de la loi n° 66-1010 du 28 décembre 1966 précitée, le démarchage " en vue de conseiller ou d'offrir des prêts d'argent, [ou] de recueillir sous forme de dépôts ou autrement des fonds du public, [ou] en vue de proposer tous autres placements de fonds " est réservé aux établissements de crédit. Sous réserve des conventions internationales, les démarcheurs agissant pour le compte de ces derniers doivent être de nationalité française ou ressortissants d'un État membre de la Communauté européenne et porteurs d'une carte de démarchage délivrée par l'établissement. Toutefois, cette carte n'est pas exigée dans le cas où le démarcheur propose des contrats de financements à crédit.

Pour être considérés comme du démarchage, les actes précités doivent être faits à titre habituel, " soit au domicile ou à la résidence des personnes, soit sur leur lieu de travail, soit dans des lieux ouverts au public et non réservés à de telles fins ", ou encore " par envoi de lettres ou circulaires ou par communications téléphoniques ".

La loi n° 72-6 du 3 janvier 1972 relative au démarchage financier et à des opérations de placement et d'assurance reprend les mêmes critères de définition et réserve le démarchage en vue d'opérations sur valeurs mobilières aux établissements de crédit et aux prestataires de services d'investissement. Ceux-ci peuvent recourir à des démarcheurs auxquels ils délivrent une carte d'emploi et qui agissent sous leur responsabilité. La carte d'emploi ne peut être délivrée, sous réserve des conventions internationales, qu'à des personnes majeures de nationalité française ou ressortissantes d'un État membre de la Communauté européenne, seulement après que l'établissement a déclaré au procureur de la République du lieu de son siège social ou de ses succursales son intention de recourir à ce démarchage ainsi que le nom, l'adresse et l'état civil de ses démarcheurs.

Ces dispositions sont relativement anciennes et peuvent paraître inadaptées aux pratiques aujourd'hui courantes sur Internet. Elles n'ont cependant pas ignoré la possibilité d'offres transfrontalières mais elles les ont, au contraire, réservées dans un but de protection de l'épargne aux seuls établissements habilités en France (ce qui inclut les prestataires de l'Espace économique européen) ou à leurs intermédiaires qui y sont localisés.

Cette position pourrait toutefois être modifiée par le législateur à l'occasion d'un projet de réforme de ces textes. Certaines dispositions sont en effet difficiles à appliquer au fonctionnement des services sur le réseau et mériteraient d'être adaptées. Mais au delà de ces aménagements d'ordre technique, l'enjeu d'un nouveau texte sera de poser les conditions de la légalité d'offres de services effectuées par Internet, auprès de la clientèle française, par des opérateurs situés hors de la Communauté européenne.

2.1.2.1.3. Pratiques en cours sur Internet

En l'état de la législation, la difficulté est d'apprécier dans quelle mesure les dispositions relatives à la publicité et au démarchage s'appliquent aux pratiques actuelles de l'Internet. En effet, les moyens utilisés par les offreurs sur le réseau pour se faire connaître du public ou pour lui formuler des offres diffèrent de ceux connus dans les décennies 1960 et 1970 et se renouvellent constamment grâce aux progrès de la technique.

Ils peuvent être aujourd'hui regroupés selon les modalités suivantes :

a) inscription, sur un site généraliste (**portail** ou annuaire par exemple) du pays du client, d'images et de messages publicitaires, généralement associés à un lien hypertexte réacheminant vers le site offreur (" bandeau publicitaire "). Cette pratique constitue une forme de publicité et doit en conséquence, dès lors qu'elle a pour objet de conseiller ou d'offrir des prêts d'argent ou de recueillir, sous forme de dépôts ou autrement, des fonds du public ou de proposer des placements de fonds, être effectuée en conformité avec les obligations posées au point 2.1.2.1.1. La qualification de démarchage doit en revanche être, selon nous, rejetée. En effet, si elle peut être habituelle, cette pratique ne peut à notre sens être considérée comme effectuée au lieu de résidence, au domicile ou au lieu de travail du client, ni être assimilée à un envoi de courrier ou de circulaire ou à une communication téléphonique. La question pourrait être posée de savoir si le site généraliste hébergeant le bandeau publicitaire, dans le cas d'opérations sur prêts d'argent, peut s'apparenter à un " lieu ouvert au public et non réservé à de telles [opérations] ". Notre sentiment est qu'une telle interprétation serait exagérée. En effet, le site généraliste reste avant tout un site commercial à la recherche de la plus grande fréquentation et son usage est par ailleurs toujours initié par le client qui prend l'initiative de s'y connecter ;

b) communication d'informations, de conseils ou d'offres du prestataire sur des sites ou des forums de discussion du pays du client. Comme dans le cas évoqué précédemment, la qualification de démarchage ne saurait selon nous être ici retenu. En effet, même si les sites français ne sont pas dans cette hypothèse des sites généralistes mais spécialisés, ils ne peuvent être comparés au domicile, à la résidence, au lieu de travail du client ou encore, le cas échéant, à un lieu public, ni être assimilés à un envoi de courier ou encore à une communication téléphonique. Seul le cas d'un forum de discussion est douteux et

pourrait éventuellement être assimilé à un «lieu ouvert au public». Lorsqu'ils ont pour objet de conseiller ou d'offrir des prêts d'argent ou de recueillir, sous forme de dépôts ou autrement, des fonds du public ou de proposer des placements de fonds, ces actes peuvent être assimilés à de la publicité. Ils doivent dans ce cas être effectués en conformité avec les obligations posées au point 2.1.2.1.1.

c) envoi de messages (" e-mails ") par un offreur sur les messageries électroniques de particuliers, éventuellement ciblés selon le " profil " commercial de l'internaute. Qualifiée par les anglo-saxons de " *spamming* ", cette technique, qui peut par ailleurs poser des problèmes d'atteinte à la vie privée doit être selon nous considérée comme un acte de démarchage. En effet, c'est ici à la boîte aux lettres identifiant un individu qu'est adressé le message, de la même façon qu'un courrier peut être envoyé à une adresse postale ou qu'une communication téléphonique peut être passée au numéro d'un particulier. Lorsque l'objet du message entre dans le champ du démarchage sur prêts d'argent ou du démarchage financier conformément aux lois de 1966 et de 1972, l'opérateur ou son intermédiaire doivent se mettre en conformité avec les dispositions de ces textes.

d) En revanche, comme il a déjà été précisé, l'accessibilité d'un site par un portail ou un moteur de recherche d'un autre pays ne permet pas dans tous les cas de déterminer une démarche active du prestataire pour offrir ses services à la clientèle de ce pays. Cela est possible à la condition que l'opérateur ait fait la démarche de référencement, mais il est courant que l'indexation par un moteur de recherche soit réalisée sans le consentement, ni même l'information du promoteur du site. Selon ces cas, on pourra donc conclure qu'il y a ou non en France sollicitation de la clientèle. Ainsi, l'inscription d'un signe commercial (logo), éventuellement accompagnée d'un message (slogan) pourra être assimilée à une publicité. Comme dans les cas a) et b), la qualification de démarchage nous semble en revanche devoir être exclue.

En conséquence, le prestataire étranger, gérant un site bancaire ou financier dans son pays d'établissement, qui présenterait des pages en français mais qui ne ferait en aucune manière des sollicitations réglementées en France (démarchage ou publicité), ne serait donc pas soumis à l'agrément des autorités françaises par le seul fait que des clients français peuvent s'y connecter sur leur propre initiative et grâce à leur connaissance personnelle de l'adresse du site.

Si le service soumis au monopole bancaire ou financier de par la loi est donc, dans la plupart des cas, exécuté au lieu d'établissement du fournisseur, les autorités françaises peuvent toutefois, le cas échéant, faire application de dispositions pénales pour empêcher le prestataire de mettre en œuvre des pratiques répréhensibles en France comme le démarchage (application des lois de police). De même, ces pratiques de sollicitation de la clientèle peuvent entraîner l'application de certaines règles du droit du pays du client au contrat (voir 3.1.2).

2.1.3. L'utilisation de faisceaux d'indices pour déterminer si un établissement d'un pays tiers à l'EEE doit être agréé pour offrir des services bancaires et financiers en France ou pour exercer une activité bancaire auprès de résidents français

Dans certains cas, le prestataire souhaitera réserver l'accès à son site à la seule clientèle résidente de son État d'implantation. Ce sera normalement le cas lorsque son site ne permet pas l'ouverture d'une relation en ligne et oblige le client à établir avec lui la " primo-relation " en face-à-face, par exemple en agence, ce qui facilite ainsi l'identification de son cocontractant. Ici, la prestation sur Internet s'apparente à un service mis à la disposition des clients du prestataire pour faciliter leurs démarches auprès de lui (services minitel ou **audiotel** existant). Les offres qui y sont faites sont clairement ciblées sur la clientèle résidente. L'accès à ce service pourra même faire l'objet d'une sécurisation par code d'accès délivré par l'établissement après la conclusion du contrat. Une autre possibilité serait que l'établissement indique clairement sur son site que ses prestations sont réservées aux seuls résidents de son État, voire qu'il effectue de surcroît (en ligne ou par courrier) une vérification de la localisation du client ou de son ordinateur. La localisation de l'ordinateur du client par vérification de son adresse électronique sur le réseau rencontre toutefois des limites techniques liées aux nombreuses possibilités de dissimulation de celle-ci, voire à sa contrefaçon (technique d'écran par l'emploi de machines esclaves, reroutages en boucle...).

À l'inverse, si le prestataire ne " cible " pas de façon restrictive sa clientèle résidente, il est permis de s'interroger sur son intention de proposer ses services à des non-résidents. Cette analyse peut être menée lorsqu'il existe des éléments permettant de caractériser l'intention manifeste de l'établissement d'agir activement de façon transfrontalière. À cet égard, la situation des prestataires établis dans des pays tiers à l'Espace économique européen doit trouver un cadre d'analyse spécifique, dans la mesure où l'exercice à distance de leur activité sur le territoire d'un État membre ne peut être couvert par un principe de reconnaissance mutuelle des agréments comme celui qui structure le marché unique européen.

2. Faisceau d'indices pour l'agrément d'un prestataire originaire d'un pays tiers

À cette fin, nous proposons de retenir, comme pour la mise en évidence d'une situation de libre prestation de services en Europe (voir 2.1.1.2.3), la définition d'un faisceau d'indices pour déterminer si une offre de services ou l'exécution d'activités bancaires à destination de la clientèle française nécessite l'agrément du prestataire originaire d'un pays tiers. Ce faisceau d'indices sera destiné à apprécier le comportement " actif " ou " passif " de l'offre ou de la fourniture de services.

A ce titre, il nous semble que l'appréciation des offres et des exécutions de services bancaires ou financiers transfrontaliers devrait s'inscrire, au niveau international, dans un cadre clair. Il s'agirait de distinguer les offres et les exécutions de services qui s'adressent directement aux résidents, en raison de l'implantation géographique de l'offre (succursale, filiale, serveur le cas échéant) ou du comportement actif du prestataire auprès des résidents, des services qui sont adressés aux résidents d'un pays donné depuis un pays tiers sans qu'ils ne soient orientés spécifiquement en direction des résidents de ce pays donné.

Dans le premier cas, il s'agira d'offres ou d'exécutions de services " dans un pays ". L'établissement doit être agréé par l'autorité du pays d'accueil. S'appliqueront alors les règles internationales de coopération entre pays d'accueil et pays d'origine, posées par le Comité de Bâle (Concordat de 1983 et Minimum Standard de 1992). Dans le second cas, il s'agit d'offres ou d'exécutions de services 'adressées au pays' sans que ses résidents ne soient spécifiquement ciblés. Ces offres ou ces prestations de services peuvent revêtir une grande variété de cas, selon le comportement actif ou passif du prestataire. Ce caractère actif peut placer le prestataire dans une situation très proche d'une offre ou d'une exécution " dans un pays ", lorsque ces dernières sont très ciblées sur un pays où il n'a pas la capacité à exercer son activité. Aussi est-il important de fixer des critères pour vérifier si le prestataire n'abuse pas de la situation tout en n'étant pas soumis à la législation du pays ciblé.

Cette analyse, qui propose la définition d'un faisceau d'indices, s'inscrit dans la logique des recommandations de l'Organisation internationale des commissions de valeurs (OICV). Dans le rapport du Comité technique de l'OICV, *«Internet et les services financiers»*, de septembre 1998, des recommandations sont en effet formulées quant au partage de compétences entre autorités pour les activités financières transfrontalières réalisées par le biais d'Internet. Le principe général est fondé sur la notion d' " impact significatif ". Si l'offre de produits ou de services effectuée sur Internet par un émetteur ou un prestataire de services financiers a lieu dans la juridiction du régulateur ou si les activités réalisées depuis l'étranger par l'émetteur ou le prestataire de services financiers ont un impact significatif sur les investisseurs ou les marchés situés dans la juridiction du régulateur, ce dernier peut s'estimer compétent et imposer à cet émetteur ou à ce prestataire le respect de ses règles, dont ces règles d'agrément.

L'OICV considère que les facteurs permettant à un régulateur de se considérer compétent sont les suivants :

- l'information diffusée est manifestement destinée aux investisseurs de la juridiction du régulateur ;

- l'émetteur ou le prestataire de services financiers concernés accepte des ordres en provenance des investisseurs de la juridiction du régulateur ou leur propose des services ;

- l'émetteur ou le prestataire de services financiers concerné utilise le courrier électronique ou d'autres moyens de communication pour " imposer " les informations les concernant aux investisseurs de la juridiction du régulateur.

De même, elle considère que les facteurs pouvant amener un régulateur à décliner sa compétence sont les suivants :

- l'émetteur ou le prestataire de services financiers désigne clairement à qui s'adresse son offre de produits ou de services financiers ;

- le site Internet contient la liste des juridictions dans lesquelles l'émetteur ou le prestataire de services financiers concerné a été ou n'a pas été autorisé à proposer ses produits ou ses services financiers ;

- l'émetteur ou le prestataire de services financiers prend les précautions nécessaires pour éviter d'offrir ses produits ou ses services financiers aux investisseurs de la juridiction du régulateur.

Sur la base notamment de ces principes, certains régulateurs ont précisé les conditions qui devraient présider au partage de compétence entre autorités. Ainsi la COB dans sa recommandation n° 99-02 relative à la promotion ou la vente de produits de placement collectif ou de services de gestion sous mandat via Internet précise dans sa recommandation n°1 le public visé. Elle rappelle que « la société qui choisit d'ouvrir un site Internet de promotion et/ou de commercialisation de produits de placement collectif ou de services de gestion sous mandat est tenue de veiller à ce que son offre respecte les règles en vigueur dans les territoires visés. […] Afin que les résidents des pays où il est possible de consulter le site ne soient pas induits en erreur, la société est invitée à préciser le champ géographique de son offre ». Cette recommandation répond à la position des autorités américaines. La SEC dans sa recommandation du 23 mars 1998, *" Use of* Internet Web *site to offer securities, solicit securities transactions or advertise investment services offshore "* prévoit en effet des procédures pour éviter que les offres ne soient considérées comme visant les résidents américains. Le site web doit comporter un avertissement clair mettant en évidence que l'offre est dirigée vers des pays tiers aux États-Unis. Il doit également mettre en place des procédures permettant au prestataire de services d'éviter de fournir des services à des personnes ayant des adresses ou des numéros de téléphone aux États-Unis.

Cette analyse ne devrait pas cependant conduire à priver un résident d'un pays donné de la possibilité d'ouvrir, par exemple, un compte en banque dans un établissement d'un pays tiers, qui ne dispose pas d'un agrément dans le pays du résident. Ce résident fait lui-même la démarche d'ouvrir ce compte à l'étranger, l'établissement ayant à l'égard des résidents un comportement passif. Aussi, il ne nous semble pas que cette analyse, et ce qu'elle implique en termes de partage de responsabilités entre les autorités du pays d'origine et d'accueil, soit transposable en matière prudentielle.

2.2. La vérification de la capacité d'exercice des opérateurs et la licéité des opérations effectuées sur Internet

Face au développement de la pratique d'opérations bancaires et financières sur Internet, le CECEI doit veiller, dans l'intérêt des consommateurs français et en tant qu'autorité en charge du contrôle des agréments au plan communautaire, à ce que l'exercice de telles activités soit effectué sur la base d'un agrément délivré par lui, ou par une autorité compétente d'un autre État partie à l'accord sur l'Espace économique européen où le prestataire serait implanté. Le Comité doit également apprécier si des prestations nouvelles offertes sur le réseau n'entrent pas dans le champ de la définition légale des opérations de banque et des services d'investissement. Les développements qui suivent font un certain nombre de propositions pour renforcer les moyens d'action des autorités.

2.2.1. L'information de la clientèle quant à la capacité d'exercice d'un prestataire

Compte tenu de la dépersonnalisation de la relation qui s'instaure sur Internet entre le client et le prestataire, il est important que le premier dispose d'une information fiable sur l'identité du second. Il s'agit là d'une condition essentielle au renforcement de la confiance du public et donc au développement de l'activité sur Internet. C'est cette fonction d'information que remplit la liste des établissements de crédit et des prestataires de services d'investissement agréés qu'établit le CECEI en application des articles 15 alinéa 8 de la loi bancaire et 18 du décret n° 96-880 du 8 octobre 1996. Cette liste est arrêtée au 31 décembre de chaque année pour parution au Journal officiel. Les modifications qui y sont apportées en cours d'année sont publiées au Bulletin officiel du CECEI, édité avec le Bulletin de la Banque de France. La liste annuelle et ses modifications trimestrielles sont consultables sur le site Internet de la Banque de France (www.banque-france.fr/informations bancaires et financières/agréments des établissements de crédit et des prestataires de services d'investissement par le CECEI).

Aujourd'hui cependant, cette liste n'indique pas les établissements proposant une prestation sur Internet. Seuls des annuaires ou des moteurs de recherche du réseau délivrent actuellement ce type d'information mais celle-ci est destinée précisément à orienter la clientèle vers ces sites, et non à attester que leur offre est régulière.

La Direction des établissements de crédit et des entreprises d'investissement de la Banque de France, qui assure le secrétariat du CECEI, est fréquemment interrogée par le public sur l'existence de tel ou tel site offrant des services bancaires et financiers. Ses moyens de renseignement traditionnels sont ici réduits puisqu'elle ne dispose pas à ce jour d'une information exhaustive des sites en fonctionnement. En effet, si l'autorité est bien saisie d'une demande d'autorisation par des entreprises qui souhaitent démarrer une prestation par Internet, la création d'un site web par un établissement déjà agréé ne fait actuellement pas l'objet d'une demande d'autorisation, ni même d'une simple déclaration auprès du Comité.

Il est important de compléter l'information des autorités sur ce point, afin que celles-ci puissent apprécier l'évolution de l'activité des établissements agréés en France et renseigner le public sur la capacité juridique d'exercer des offreurs.

En outre, compte tenu des risques inhérents à l'exercice de la prestation bancaire et financière sur Internet, notamment quant à la stabilité financière de l'établissement et à la maîtrise du système d'information, les autorités doivent pouvoir veiller à l'accomplissement d'un certain nombre de diligences lors de l'ouverture d'un site web bancaire ou financier (voir la troisième partie " maîtrise des risques "). L'utilisation du canal Internet modifie en effet largement les conditions de recherche de la clientèle et peut modifier le programme d'activité de l'entreprise, en facilitant notamment l'élargissement de sa clientèle. Conformément à l'article 15, alinéa 3, de la loi bancaire, le CECEI, qui doit apprécier l'aptitude de l'entreprise requérante à réaliser ses objectifs de développement dans des conditions compatibles avec le bon fonctionnement du système bancaire et en assurant à la clientèle une sécurité satisfaisante, doit pouvoir apprécier si l'ouverture d'un site Internet bancaire ou financier remplit ces conditions.

3. Proposition de déclaration auprès de l'autorité d'agrément de l'intention d'un prestataire de réaliser des opérations bancaires et financières sur Internet

Il est en conséquence proposé de considérer que la réalisation d'opérations bancaires ou de services d'investissement par Internet constitue un élément notable du mode de fourniture des services, modifiant les conditions d'exercice de l'activité bancaire ou financière et résultant d'un choix stratégique de l'établissement ; qu'en conséquence, l'intention d'un prestataire de réaliser des opérations bancaires ou des services d'investissement par Internet devrait faire l'objet d'une déclaration auprès de l'autorité d'agrément. A l'occasion d'une telle déclaration, le CECEI examinerait pour les établissements déjà constitués si l'ouverture du nouveau canal de distribution reste compatible avec les éléments de bon fonctionnement de l'établissement appréciés lors de son agrément. Le règlement n° 96-16 du Comité de la réglementation bancaire et financière pourrait être modifié en ce sens.

4. Création d'une base de recherche des activités sur Internet des établissements de crédit et des prestataires de services d'investissement

Le CECEI, disposant alors de la connaissance de l'ensemble des établissements offrant des services en ligne, fera mention sur la liste des établissements de crédit et des prestataires de services d'investissement de leur activité sur Internet. Ces informations devraient être aisément consultables par le public sur le site Internet de la Banque de France-CECEI, ce qui amènerait à faire évoluer celui-ci de la simple mise à disposition actuelle de la liste annuelle et de ses modifications trimestrielles à une base de recherche.

Le site Internet de la Banque de France fera l'objet d'une nouvelle maquette donnant un accès plus facile aux informations de chaque autorité (Commission bancaire et Comité des établissements de crédit et des entreprises d'investissement). Il devrait également comporter un message de prudence invitant les internautes souhaitant contracter avec un établissement bancaire ou financier sur le réseau à vérifier que celui-ci est régulièrement agréé soit sur le site Banque de France soit auprès du secrétariat du CECEI pour toute information complémentaire.

Cette proposition s'inscrit dans la ligne de l'article 4 de la directive 2000/31 du Parlement européen et du Conseil dite " commerce électronique ". Cet article pose un large principe de non-autorisation préalable à l'exercice de l'activité d'un prestataire de service de la société de l'information (" Les États membres veillent à ce que l'accès à l'activité d'un prestataire de services de la société de l'information et l'exercice de celle-ci ne puissent pas être soumis à un régime d'autorisation préalable ou à toute autre exigence ayant un équivalent "). Ce texte ne remet pas en cause l'agrément requis pour l'activité bancaire ou financière elle-même qui reste exigible conformément à l'alinéa 2 de l'article précité.

L'article 5 de la directive 2000/31 prévoit par ailleurs que les États membres doivent obliger les prestataires sur Internet à développer les éléments permettant leur identification

claire par le public. Un certain nombre d'exigences d'information sont même prévues dans le cas des professions réglementées telles que la banque et la finance : la mention sur le site du titre professionnel et de l'État membre qui l'a octroyé, la référence aux règles professionnelles de l'État membre d'établissement du prestataire de services sur Internet et le moyen d'y avoir accès.

Les autorités françaises sont également sensibles à la bonne information des clients concernant la garantie accordée aux fonds ou aux titres gérés par l'intermédiaire d'un prestataire sur Internet. Cette position est conforme aux dispositions contenues dans la proposition de directive relative à la " vente à distance de services financiers " en cours de discussion devant le Conseil.

5. Identification du prestataire et renvoi par lien hypertexte au site de la Banque de France-CECEI

Conformément aux directives en cours d'examen, il est proposé de rendre obligatoire l'affichage, sur la page d'accueil d'un site bancaire ou financier d'un prestataire agréé en France ou sur une page d'accès facile, direct et permanent, d'un certain nombre de mentions de façon à l'identifier clairement et à renseigner la clientèle sur sa capacité d'exercer :

- **nom du prestataire ;**
- **adresses de son siège social et de son lieu d'établissement ;**
- **association professionnelle à laquelle il adhère conformément à l'article 23 de la loi bancaire ou à l'article 24-I de la loi de modernisation des activités financières ;**
- **mention de l'agrément délivré par le CECEI, des services qu'il recouvre et renvoi par lien hypertexte (dans des conditions de sécurité adéquates) au site de la Banque de France-CECEI pour permettre au client de consulter la liste des prestataires agréés. Ce renvoi pourrait être matérialisé par l'affichage d'un sigle " CECEI " ;**
- **mention de l'adhésion à un mécanisme de garantie des déposants ou des investisseurs.**

2.2.2. Appréciation par les autorités du caractère bancaire ou financier de certaines opérations

Le commerce électronique peut favoriser l'émergence de nouvelles activités d'intermédiation financière susceptibles d'entrer dans le périmètre des opérations bancaires et financières telles qu'elles sont aujourd'hui définies par le législateur.

Il appartient aux autorités de veiller au respect du monopole d'exercice des opérations bancaires et financières en caractérisant ces pratiques nouvelles.

2.2.2.1. Le cas des portails et des sites agrégateurs

De nouveaux opérateurs spécialisés dans la fonction de distribution de services bancaires et financiers tendent à remettre en cause la fonction bancaire. D'une part, portails et sites agrégateurs risquent de réduire les établissements à une simple fonction de production et de gestion du risque. D'autre part, ils les mettent directement en compétition.

2.2.2.1.1. Les agrégateurs de données (" screen scrapers ")

Ces opérateurs, qui se développent aux États-Unis, consolident sur une même page web les données financières d'un client, trouvées auprès des banques et gestionnaires de comptes auxquels le client leur donne accès. L'intérêt du particulier est ainsi d'obtenir sur une même page, une concentration d'information sur ses comptes personnels recueillie auprès de plusieurs autres sites. Ce service peut être complété de diverses facilités d'e-mails, de paiements électroniques ou de réservations. Pour le bon fonctionnement d'un tel service, les établissements gestionnaires des comptes doivent donner leur accord, ce qui facilite la récupération des zones d'écran concernées.

Les prestataires bancaires et financiers risquent ainsi cependant de favoriser la dispersion des opérations de leur clientèle et d'y perdre une part de la connaissance qu'ils ont de leurs clients.

Le développement d'une telle activité présente ainsi des risques quant à la sécurité des sites agrégateurs, à la **confidentialité** des informations personnelles transmises entre le teneur de comptes et l'agrégateur (mots de passe, numéros de comptes, etc.), mais aussi quant à la responsabilité de ces sites dans les services qui sont proposés.

Certains d'entre eux tendent en effet à évoluer de façon à proposer au-delà du service de base de récupération de données, une véritable gamme de services de conseil ou de paiement à distance. Conformément à l'article 1er de loi bancaire, de tels opérateurs sont susceptibles d'être soumis à agrément en France dans la mesure où les opérations de banque comprennent la mise à disposition de la clientèle ou la gestion de moyens de paiement. Les autorités bancaires veilleront, en particulier, à ce que les établissements, par l'introduction de clauses contractuelles entre ces derniers et les agrégateurs de données, ne perdent pas la connaissance de leurs clients, exigence au titre du contrôle interne et de la lutte contre le blanchiment.

2.2.2.1.2. Les portails

Le développement des portails, portes d'accès au réseau offrant une gamme de services variés, pourra à terme représenter un point de passage plus ou moins obligé pour les établissements de crédit et les entreprises d'investissement. En effet, Internet modifie principalement les conditions d'établissement de la relation avec la clientèle. La force économique des portails tient à leur notoriété et à la concentration de services qu'ils fournissent. En matière bancaire ou financière aussi, leur notoriété sur la " toile " peut devenir supérieure à celle des établissements et fédérer une audience telle qu'il deviendra économiquement obligatoire aux prestataires de services financiers d'y être présents. Dès

lors, les établissements devront construire leur stratégie de fourniture de service en choisissant une offre en propre ou intégrée à un portail.

Aujourd'hui, le plus souvent encore locataires d'espaces publicitaires sur les portails existant, certaines banques, craignant d'être réduites au rôle de sous-traitant financier banalisé, cherchent à échapper aux sociétés qui développent ces sites en construisant leur propre système.

En règle générale, s'ils ne font que mettre en relation les clients et les prestataires en vue de la conclusion d'opérations bancaires sans se porter ducroire, les portails sont des intermédiaires en opérations de banque, tels que définis par les articles 65 et suivants de la loi bancaire. En tant que tels, ils ne seraient pas soumis à agrément. Cependant, certains **sites portails** sont susceptibles d' " effectuer à titre de profession habituelle des opérations de banque " et doivent dès lors disposer d'un agrément d'établissement de crédit.

2.2.2.2. Monnaie privée

Les autorités ont déjà pu constater l'existence de sites proposant l'usage de monnaie privée, parfois associée à des mécanismes de fidélisation de la clientèle. Elles ont été interrogées également sur la pratique du troc de biens et de services divers. Ces opérations entrant dans le champ des activités de mise à la disposition du public et de gestion de moyens de paiement, elles ne peuvent être légalement exercées que par des établissements de crédit.

Ainsi, même s'il est destiné à fidéliser la clientèle, un point délivré par une entreprise s'apparente clairement à un titre de créance, s'il est admis en paiement par une universalité de commerçants pour le règlement d'achats auprès d'eux d'un ensemble de biens ou de services variés. Il doit dès lors être considéré comme un moyen de paiement au sens de l'article 4 de la loi bancaire du 24 janvier 1984.

Les systèmes de fidélisation ne peuvent être mis en œuvre, en France, par des entreprises non agréées en qualité d'établissement de crédit, qu'à la condition de respecter les conditions posées par l'article 12.5 de la loi bancaire, qui permet " à une entreprise, quelle que soit sa nature, d'émettre des bons et cartes délivrés pour l'achat auprès d'elle d'un bien ou d'un service déterminé ". Dans un tel système, dit " monoprestataire ", l'émetteur du titre est en effet le seul à l'accepter en paiement pour les achats effectués auprès de lui.

2.2.2.3. Le mode de paiement dit du kiosque

De même, le mode de paiement dit du " **kiosque** ", apparu sur le minitel et repris maintenant par les fournisseurs d'accès à Internet, soulève certains problèmes. Dans ce mécanisme, le paiement de l'offreur de service n'est pas effectué directement par l'internaute. C'est l'opérateur de télécommunication, qui inclura, dans la facturation de la communication au client, le montant du paiement destiné au prestataire du service et le lui reversera. Les autorités bancaires se sont montrées pour l'instant réservées sur la question de la légalité de cette pratique.

2.2.3. La sanction de l'exercice illégal du métier de banquier

Le développement des services financiers accessibles par Internet est si rapide qu'il est impossible de connaître précisément l'ensemble des sites existants. Il en résulte qu'Internet pourrait faciliter l'exercice d'activités financières en dehors de tout cadre légal. Outre le risque de contrefaçon de sites de prestataires reconnus, il est ainsi possible que des entités ouvrent des sites Internet pour proposer des services bancaires ou d'investissement en laissant entendre qu'ils sont régulièrement agréés. Si des opérations bancaires sont effectivement réalisées sur le territoire français, ces personnes s'exposent alors aux sanctions pénales prévues par les articles 75 et suivants de la loi bancaire ou 82 et suivants de la loi de modernisation des activités financières. En application de l'article 85 de la loi bancaire, la Commission bancaire peut se constituer partie civile à tous les stades de la procédure pour les infractions à la loi bancaire. En outre, lorsqu'elle a connaissance de faits susceptibles de revêtir une qualification pénale, elle transmet ces derniers au Procureur.

Des réflexions sont en cours au niveau international pour organiser la coopération entre autorités afin de lutter contre l'exercice illégal du métier de banquier. L'information entre pays d'origine et pays d'accueil (de fait) sera renforcée selon des modalités qui restent à préciser.

3. Le cadre d'exercice de l'activité bancaire ou financière sur Internet

Compte tenu de la grande facilité de l'utilisation transfrontalière du réseau, il sera possible à un prestataire d'entrer en relation d'affaires avec des clientèles de différents pays sans forcément y réaliser des opérations bancaires ou financières soumises à agrément. Cette question n'est bien évidemment pas nouvelle mais prend une autre ampleur avec Internet compte tenu des facultés de " déplacement " de l'internaute.

En conséquence, dans une telle relation transfrontalière, la sécurité juridique des offreurs et des clients ne se réduit pas au seul contrôle des agréments. Elle est liée au bon équilibre des règles posées par le droit international privé pour déterminer le juge compétent et le droit applicable à un litige comportant un élément d'extranéité.

Aussi, l'examen des conditions d'accès à l'activité bancaire et financière sur Internet ne peut faire l'économie d'une analyse supplémentaire concernant le droit applicable à l'exercice de ladite activité. Cet examen est indispensable :

- pour le prestataire, qui doit connaître et encadrer juridiquement l'exercice de son service pour maîtriser le risque afférent à une relation transfrontalière ;

- pour les autorités, tant d'agrément que prudentielles, tenues de prendre en compte le risque ainsi créé pour les prestataires, et éventuellement de contrôler l'application des mesures impératives afférentes à son activité ;

- pour le consommateur qui, en contractant à l'étranger, peut se trouver privé des protections prévues dans son propre système juridique.

Il ne peut s'agir ici de présenter une analyse exhaustive des règles de droit international privé dont l'application relève des tribunaux. Il est en revanche nécessaire de déterminer à l'usage de l'ensemble des acteurs, d'une part, une typologie générale des situations à examiner, et, d'autre part, dans le cadre de cette typologie, une grille d'analyse des situations concourant à la résolution de chaque cas particulier.

3.1 Essai d'une typologie des relations prestataire/client

Pour les opérations effectuées dans un même État entre des opérateurs qui y résident, le cadre juridique applicable au contrat pourra être aisément déterminé en référence au droit de cet État. En revanche, il est plus difficile d'apprécier l'environnement juridique d'un contrat conclu entre des parties localisées dans des États différents à la fois quant au droit applicable et quant au règlement du litige y afférent. Il est donc important de différencier les types de relations contractuelles possibles selon la localisation des parties en examinant les principes de règlement des conflits de lois en la matière. Les développements qui suivent ne portent cependant que sur les cas mettant en jeu au moins un cocontractant français.

La détermination du droit applicable à un contrat est nécessaire dès lors qu'un litige surgit entre les cocontractants et que l'obligation comprend un élément d'extranéité.

La détermination du droit applicable s'effectue toujours en deux étapes :

- la détermination du juge compétent ;

- la qualification par le juge saisi du conflit de l'opération litigieuse puis l'application des règles de conflit de loi telles qu'elles sont inscrites dans son droit national. En un certain nombre de matières, les États auront pu harmoniser leurs règles au sein de conventions constituant le droit international privé. Ces règles de résolution des conflits de lois permettent d'arbitrer en faveur de l'application du droit d'un État ou d'un autre en fonction des caractéristiques de la relation contractuelle. Elles supposent de pouvoir déterminer la localisation du prestataire, du client, ainsi que de la prestation.

À cet égard, en matière bancaire et financière, si c'est un tribunal français ou plus généralement un tribunal d'un État membre de l'Union européenne qui est compétent, il appliquera les règles de conflit prévues dans la Convention de Rome du 19 juin 1980 sur la loi applicable aux obligations contractuelles. Cette dernière consacre la loi d'autonomie, c'est-à-dire la faculté pour les parties de désigner la loi applicable au contrat. Si c'est un tribunal d'un État qui n'est pas membre de l'Union européenne qui est saisi du litige, ce dernier appliquera la règle de conflit du for (c'est-à-dire du tribunal saisi).

Ainsi, un Français, client ou prestataire, qui noue une relation d'affaire sur Internet pourra se trouver dans trois cas possibles selon la localisation géographique de son cocontractant ou de la prestation délivrée.

Pour déterminer la loi applicable aux contrats conclus sur Internet, il faut donc distinguer le contrat conclu entre deux cocontractants situés en France (3.1.1), celui conclu entre deux ressortissants de l'Union européenne (3.1.2) et celui passé avec un cocontractant situé à l'extérieur de l'Union européenne (3.1.3).

3.1.1. Contrat conclu entre un client ayant sa résidence en France et un prestataire de droit français

En principe, le juge français sera compétent et appliquera le droit français. En effet, le principe de l'autonomie de la volonté qui laisse le choix aux contractants de déterminer le droit applicable à leur contrat est écarté en l'absence de tout élément d'extranéité.

Toutefois, la prestation peut être soumise à un droit étranger, à raison d'un élément d'extranéité, qu'il s'agisse de sa nature (par exemple négociation sur un marché réglementé étranger, qui entraîne l'application du droit applicable à ce marché pour la réalisation de l'opération), ou qu'il s'agisse d'un choix des parties.

On doit dès lors s'interroger sur la possibilité pour le juge français d'imposer malgré tout l'application de certains principes de droit français. Le code civil intègre à cet effet des

règles de conflit de lois issues du droit international privé, qui permettent de déterminer dans quelles conditions des dispositions du droit français s'imposent à un contrat soumis à un autre droit.

Ceci va notamment concerner les règles dites d'ordre public et de police, au nombre desquelles on trouvera sans aucun doute les règles applicables en matière de protection du consommateur. Ainsi, conformément au code civil, même si le contrat prévoit l'application d'un droit étranger, le juge français peut écarter des textes contraires aux dispositions impératives de protection du consommateur français.

A ce titre, il convient de souligner que, devant l'absence d'une définition de la notion de consommateur, tant le Code de la consommation que la jurisprudence française se concentrent sur une définition plutôt étroite (le particulier-client), qui diffère de la conception usitée en droit communautaire (conception large de la notion de consommateur qui inclut les professionnels qui agissent en dehors de leurs spécialités).

En outre, force est de constater qu'il n'y a pas un droit de la consommation spécifique aux opérations bancaires et financières, les différentes règles qui existent sont en partie réunies dans le Code de la consommation, et dans les règlements du Comité de la réglementation bancaire, alors que d'autres sont purement jurisprudentielles. Cependant, la disparité des sources n'enlève en rien à l'homogénéité des objectifs poursuivis par les différentes règles : information du consommateur, encadrement de l'offre, octroi de délais, lutte contre les taux abusifs. Particulièrement importantes pour le commerce électronique, on recense les dispositions suivantes :

- la loi de 1966 relative à l'usure ;

- la loi n° 78-23 du 10 janvier 1978 sur la protection et l'information des consommateurs de produits et de services et son décret d'application n° 78-464 du 24 mars 1978 ;

- la loi n° 92-60 du 18 janvier 1992 renforçant la protection des consommateurs ;

- la loi n° 72-1137 relative à la protection des consommateurs en matière de démarchage et de vente à domicile ;

- la loi n° 78-22 relative à l'information et à la protection des consommateurs dans le domaine de certaines opérations de crédit et ses décrets d'application du 17 mars 1978 et du 25 mars 1988 ;

- la loi n° 89-1010 relative à l'information et à la protection des consommateurs ainsi qu'à diverses pratiques commerciales.

Ces textes de référence concernant la protection et l'information des consommateurs de produits et services ont été réunis dans un code de la consommation promulgué par une loi du 27 juillet 1993.

3.1.2. Contrat conclu entre deux ressortissants de l'Union européenne

En raison d'une certaine harmonisation des règles de conflit, peu importe pour la détermination du droit applicable que ce soit le client ou le prestataire qui soit situé hors de France et à l'intérieur de l'Union.

La détermination du juge compétent sera effectuée selon les principes posés par la Convention de Bruxelles de 1968 " concernant la compétence judiciaire et l'exécution des décisions en matière civile et commerciale ". Sa section 4, " compétence en matière de contrats conclus par les consommateurs ", indique que le consommateur peut, à sa convenance, attraire l'autre partie soit devant le tribunal de son propre domicile, soit devant celui du domicile du défendeur.

En ce qui concerne le droit applicable pour les établissements de crédit qui relèvent de pays de l'Union européenne, les deux directives de coordination bancaire du 12 décembre 1977 et 15 décembre 1989 ont posé le principe que tout établissement de crédit agréé dans l'un quelconque des autres États membres pourra y exercer ses activités dans tous les autres soit par voie d'établissement (succursale), soit par voie de liberté de prestation de service et ce, normalement, dans le respect des seules règles d'origine. Cependant, le droit applicable aux relations contractuelles entre un client ressortissant européen et un établissement qui exercera en libre prestation de services ou par voie d'établissement sera déterminé par les règles de conflits prévues par les Conventions internationales.

Concernant l'offre de service et des produits bancaires et financiers sur Internet, et sauf lorsqu'il existe des règles du droit communautaire éventuellement applicables dans des cas particuliers, il faut se référer aux règles de conflits posées par la Convention de Rome du 19 juin 1980 sur la loi applicable aux obligations contractuelles.

La Convention de Rome prévoit l'application de la loi du pays avec lequel le contrat présente les liens les plus étroits (loi du pays où la partie fournit la prestation caractéristique, ou a sa résidence habituelle ou son établissement) à défaut de choix exprès de la loi du contrat. Sera donc privilégiée la loi du lieu d'exécution de la prestation, le plus souvent confondue avec la loi du lieu d'établissement du prestataire.

Toutefois, le prestataire, qui semble ainsi en tout état de cause maîtriser le choix de la loi applicable, qu'il l'insère expressément dans ses conditions générales, ou qu'il laisse s'appliquer les règles de droit international privé, doit tenir compte du fait que des règles exogènes peuvent venir inférer :

- *via* les règles d'intérêt général applicables dans le cadre de la libre prestation de services (voir la communication interprétative de la Commission européenne de juillet 1997) ;

- par le biais de l'article 5 de la Convention de Rome du 19 juin 1980 qui prévoit que le choix de la loi par les parties ne doit pas avoir pour conséquence de priver le consommateur de la protection que lui assurent les dispositions impératives de la loi du pays de sa résidence habituelle ;

- par le truchement de l'article 7 de la Convention qui reprend le principe selon lequel le juge peut ne pas tenir compte de la loi du contrat pour appliquer une loi de police. Celle-ci devra s'appliquer même si la règle de conflit ne l'a pas désignée. C'est le cas notamment en France de la loi du 28 décembre 1966 relative à l'usure, la loi du 10 janvier 1978 relative à la protection des emprunteurs en matière de crédit mobilier ainsi que la loi du 13 juillet 1979 relative à la protection des emprunteurs en matière de crédit immobilier ou plus généralement les lois françaises relatives aux opérations de crédit à la consommation, dites lois Scrivener ; de même que les dispositions qualifiées d'intérêt général. Il ne s'agit pas ici de la notion communautaire susvisée, mais d'une notion classique de droit international privé qui impose un " ordre public contractuel " auquel les parties ne sauraient déroger, quelle que soit la loi sous l'empire de laquelle elles souhaiteraient placer le contrat. En revanche, d'autres dispositions de protection du consommateur, telles que l'obligation d'information de la caution, ne doivent pas être considérées comme des lois de police applicables à des eurocrédits. On rappellera toutefois que le client ne peut prétendre à la protection relative aux lois de police dès lors qu'il a contracté à la suite d'une démarche active de sa part dans un autre Etat que celui de sa résidence principale.

3.1.3. Un des cocontractants est extérieur à l'Union Européenne

C'est la règle de conflit du juge saisi du litige qui désignera le droit applicable. Pour ce qui concerne la détermination du juge compétent, il convient de rappeler que l'article 14 du Code civil français permet toujours dans ce cas au plaignant résident français, qu'il soit prestataire ou client, de saisir un juge français d'une action en responsabilité contractuelle. En raison des difficultés à faire exécuter un jugement à l'étranger, cette procédure pourra être très aléatoire, surtout si le juge français se voit conduit à appliquer un droit étranger.

En revanche, il convient d'appeler l'attention du prestataire français sur l'application qui pourrait lui être faite de l'article 15 du Code civil, qui permet à un client, même ayant contracté à l'étranger, d'attraire ledit prestataire devant un tribunal français, dont les décisions pourront bien entendu faire l'objet de voies d'exécution en France.

Nonobstant les dispositions susvisées du Code civil, si le juge compétent est le juge du ressortissant ayant sa résidence à l'extérieur de l'Union européenne, il appliquera sa propre règle de conflit. Cette dernière peut désigner soit la loi du for, soit la loi désignée par le contrat, soit une loi de police considérée comme telle par le juge. Bien que chaque État ait ses règles de conflit propres, la tendance dominante est généralement de privilégier la loi de l'exécution du contrat donc la loi du prestataire.

En revanche, si c'est le juge français qui est saisi d'un litige opposant un ressortissant français à un prestataire étranger à l'Union européenne, il se réfèrera aux règles de conflits de la Convention de Rome pour déterminer le droit applicable.

Les professionnels comme les consommateurs s'exposent dans ce type de relation contractuelle à se voir opposer des règles moins protectrices que celles prévues dans l'Union européenne. Ils doivent être vigilants et s'informer sur le système juridique de l'État de leurs cocontractants.

3.2. Le droit de la preuve

Il semble tout à fait opportun de rappeler aux prestataires la nécessité de maîtriser le droit applicable en matière de preuve.

Par-delà la question juridique, il doit être également souligné que, dans tous les cas, la preuve vise la sécurité de la transaction et s'inscrit dans le cadre des principes généraux de sécurité DICP (Disponibilité, Intégrité, Confidentialité et Preuve) sur lesquels a insisté le Livre blanc de 1996 de la Commission bancaire sur la sécurité des systèmes d'information. Il est recommandé à ce titre d'adopter des techniques permettant la **non-répudiation** pour les transactions jugées sensibles par l'établissement de crédit ou le prestataire de services d'investissement. Les points 5.3 (Intégrité, authentification, non répudiation et **confidentialité** des transactions), de la deuxième partie " analyse des risques " et 8.3.3. de la troisième partie relative à la maîtrise de risques (exemples de mise en place d'infrastructures de sécurité) traitent plus particulièrement de cette question.

Les questions relatives à la preuve sur l'Internet recouvrent deux types de problématiques, l'une relative aux aspects techniques de la question (génération de signature numérique, utilisation de moyens de cryptographie, techniques de conservation des documents électroniques…), l'autre aux questions juridiques. Si ces dernières vont constituer la substance des quelques rappels auxquels se limite cette première approche, il convient de noter que leur champ d'action est de facto cantonné à la reconnaissance ou non d'effets de droit aux techniques mises en œuvre, ces dernières conditionnant l'efficacité de la règle de droit qui est censée les encadrer. Par ailleurs, si elles trouvent une acuité particulière en matière d'Internet, ces questions concernent les messages numériques en général.

Comme le souligne le Conseil d'État " prouver, au sens courant du terme, est ce qui sert à établir qu'une chose est vraie. Il n'en va pas autrement en matière juridique, à cette précision près que c'est le juge qu'il s'agit de convaincre de la vérité d'une allégation : la preuve juridique est une preuve judiciaire ". Dans ce but, la " preuve " doit permettre la vérification de deux éléments :

- d'une part, de l'identification des parties concernées, et de façon concomitante, la qualité de leur consentement (avec parfois l'imposition d'un formalisme non seulement *ad probationem*, mais également *ad validitatem*) ;

- d'autre part, sur le contenu de leur engagement qui doit pouvoir être connu et accepté à un instant donné par l'ensemble des acteurs (à ce stade, aucune distinction n'est faite entre acte et fait juridique, engagements unilatéraux ou synallagmatiques…).

Dès lors, une bonne connaissance non seulement du juge compétent mais également du système de preuve qu'il est susceptible d'accepter est essentiel.

Jusqu'à présent, pour les opérations conclues en matière civile et supérieures à un certain montant (5000 FF), l'acceptation de la preuve électronique nécessitait la définition d'un cadre contractuel entre les acteurs concernés (convention de preuve), sans que ceux-ci aient l'absolue certitude que les moyens mis en œuvre soient reçus par le juge. Désormais la

directive " signature électronique " et ses textes de transposition clarifient cette situation en accordant un statut juridique défini à ce mode de preuve. Le point se limite aux règles de preuve (formalisme ***ad probationem***) des contrats et formule en la matière des recommandations de bonne pratique.

Par delà l'utilisation *ad probationem* de la " signature électronique ", la transposition de la directive " commerce électronique " consacrera la possibilité juridique de conclure par voie électronique des transactions pour lesquelles un écrit-papier obéissant à un certain formalisme est nécessaire, et constitue –au-delà d'un moyen de preuve- la condition même de la validité de l'acte en question. Le formalisme est alors ***ad validitatem.***

3.2.1. La reconnaissance de l'écrit électronique comme formalisme *ad probationem*

Sont présentées ci-dessous la directive signature électronique, la loi du 13 mars 2000 ainsi que les grandes lignes du décret " signature électronique ", sachant que des textes importants n'ont pas encore été adoptés : transposition des dispositions de la directive " signature électronique " concernant la responsabilité des **prestataires de services de certification (PSC)**, décrets et arrêtés relatifs à la signature électronique.

3.2.1.1. La directive signature électronique

La directive signature électronique pose le principe de la non discrimination et de l'équivalence, sous certaines conditions, de la " signature électronique "[4] avec la signature manuscrite. Une signature électronique ne peut être écartée juridiquement pour la seule raison de sa forme électronique.

La directive permet la reconnaissance juridique d'une signature électronique à deux niveaux : elle confère à la signature électronique, sous certaines conditions, une force probante équivalente à celle de la signature manuscrite (article 5.1) ; elle affirme ensuite le principe de non discrimination (article 5.2) de la signature électronique par rapport à la signature manuscrite. Ces conditions visent à la fois :

- les signatures elles-mêmes (notion de signature électronique " avancée "[5]) ;
- les certificats de clés publiques (notion de certificats " qualifiés ") ;
- les prestataires de services de certification (**PSC**)[6] ;
- et les dispositifs de création de signature.

Si le **certificat** et le fournisseur de services, de même que la signature utilisée, satisfont à un ensemble de spécifications, la signature sera réputée de même valeur qu'une signature

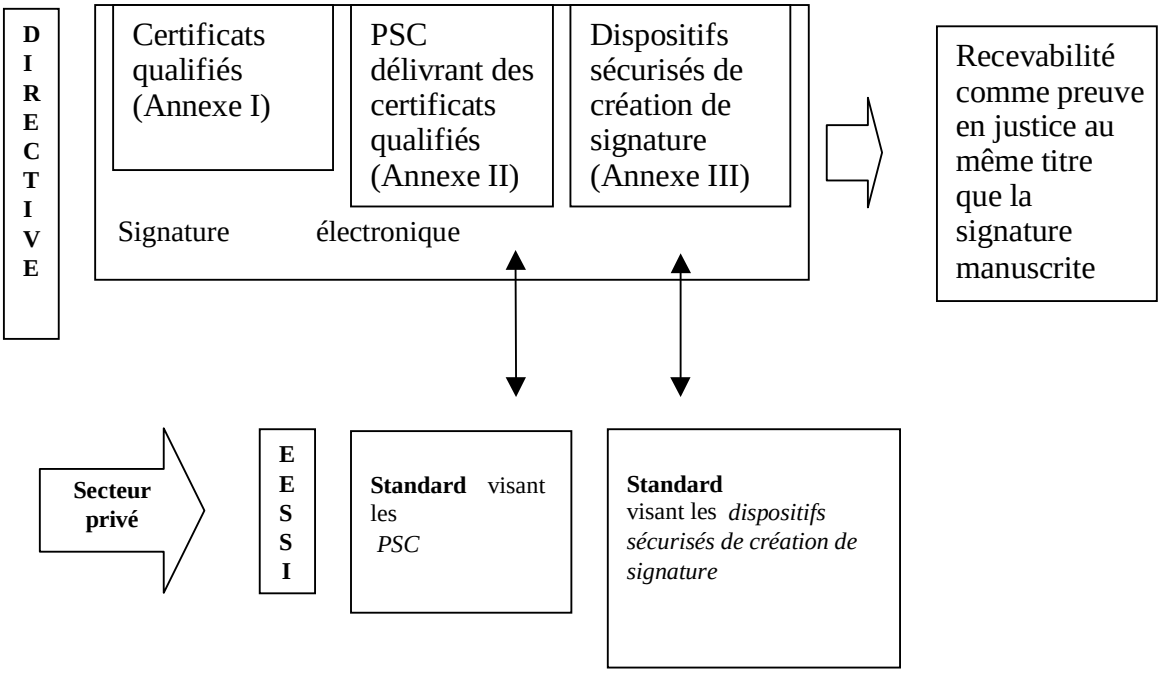
4) La «signature électronique» est un terme générique, qui se veut «neutre technologiquement». Dans l'état actuel de la technique, il renvoie aux techniques de la cryptographie asymétrique.

5) Permettant d'identifier de façon univoque le signataire, de détecter une perte d'intégrité au niveau des données auxquelles elle s'attache, et enfin créée par des moyens que le signataire puisse garder sous son contrôle exclusif.

manuscrite. Ces spécifications sont reprises dans les annexes I (exigences concernant les certificats qualifiés) et II (exigences concernant des prestataires de services de certification[7] délivrant des certificats qualifiés) de la directive. L'annexe III, quant à elle, traite des dispositifs de création de signature.

La directive définit deux niveaux de signature : la signature " simple " et la signature " avancée ". La signature simple n'est pas dénuée d'efficacité juridique mais elle ne bénéficie pas de la présomption de fiabilité contrairement à la signature avancée. La preuve de cette fiabilité doit être apportée devant le juge en cas de litige.

Exigences générales de la directive signature électronique



Les travaux de normalisation sont engagés au niveau européen -European Electronic Signature Standardisation Initiative (EESSI)- et au niveau national au sein de la Direction centrale de la sécurité des systèmes d'information (**DCSSI**) et d'un groupe d'experts du monde industriel réunis autour du Secrétariat d'Etat à l'Industrie (groupe GFTA).

Trois organismes de normalisation européens compétents en matière de technologies de l'information -le Comité Européen de Normalisation (CEN), sa déclinaison dans le domaine de l'électronique (CENELEC) et dans les télécommunications (ETSI)- ont fondé l'Information and Communication Technology Steering Board (ICTSB), une structure de coordination spécifique aux technologies de l'information et de la communication, à laquelle participe notamment le Comité européen de normalisation bancaire (CENB).

---

6) Parmi lesquels les autorités de certification et leurs sous-traitants : autorités d'enregistrement, d'horodatage, de révocation, opérateurs de certification, etc.

7) Les différents métiers de la certification : autorité de certification, autorité d'enregistrement et opérateur de certification sont exposés en annexe.

L'ICTSB a été mandaté par la Commission Européenne ainsi que par les États Membres à travers leur groupe d'experts en sécurité des systèmes d'information (SOGITS), pour faire l'inventaire des travaux de normalisation à réaliser pour accélérer le développement des solutions de signature électronique (EESSI phase 1), et pour organiser les tâches de normalisation jugées prioritaires (EESSI phase 2). Cette initiative s'articule autour de trois axes :

- la **DCSSI** travaille actuellement dans plusieurs directions avec les industriels en vue d'alimenter les réflexions européennes ;

- l'évolution des politiques de certification actuelles destinées aux **PSC** émettant des **certificats** pour le compte des administrations (dites PC2), pour tenir compte du retour d'expérience obtenu dans le secteur de la santé et des télédéclarations ;

- la rédaction d'exigences sécuritaires (par exemple sous forme de **profils de protection,** visant les systèmes des **opérateurs de certification** et des **autorités d'enregistrement**, ainsi que leurs ressources cryptographiques.

3.2.1.2. La loi du 13 mars 2000

3.2.1.2.1. Définition légale de la présomption de fiabilité des signatures électroniques

La loi du 13 mars 2000, portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique, reconnaît l'écrit électronique comme mode de preuve, sous réserve que l'on puisse identifier la personne dont elle émane, et précise à ce titre que « *lorsqu'elle est électronique, [la signature] consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d'État* ».

Ces conditions portent notamment sur les prestataires de services de certification –exigences de l'annexe II de la directive- qui devront pouvoir démontrer leur conformité à ces conditions.

3.2.1.2.2. Les conventions de preuve

La loi du 13 mars 2000 consacre la possibilité pour deux parties de conclure des conventions sur la preuve. L'article 1316-2 du code civil dispose à ce titre que « *[l]orsque la loi n'a pas fixé d'autres principes, **et** à défaut de convention valable entre les parties, le juge règle les conflits de preuve littérale en déterminant par tous les moyens le titre le plus vraisemblable, quel qu'en soit le support* ».

En vertu de l'article 1316-1, une convention de preuve n'est plus indispensable pour que la preuve électronique soit recevable en matière civile.

Les conventions de preuve demeurent cependant utiles :

- pour régler les conflits de preuve (article 1316-2), notamment pour permettre aux parties

de marquer leur préférence pour un mode de preuve particulier ;

- pour que soient recevables des procédés de preuve ne bénéficiant pas de la présomption de fiabilité de l'article 1316-4.

Il faut noter que les conventions de preuve peuvent parfois aboutir à la constitution unilatérale de la preuve par le professionnel exploitant le système informatique :

- mettant en situation d'infériorité le client qui n'est pas toujours à même de vérifier l'engagement qu'il a pris lorsque le système ne délivre pas de trace ;

- transférant sur le client les risques nés des éventuelles faiblesses existant dans la sécurité du système informatique.

La loi n°95-96 du 1er février 1995 concernant les clauses abusives et la présentation des contrats prend en compte ce problème en définissant les clauses abusives comme des " *clauses qui ont pour objet ou pour effet de créer au détriment du non-professionnel ou du consommateur, un déséquilibre significatif entre les droits et les obligations des parties au contrat* ". La sanction civile pour de telles clauses est alors la nullité. En annexe à cette loi figure une liste indicative de ces clauses. Sont notamment visées celles qui ont pour effet de supprimer ou d'entraver l'exercice d'actions en justice ou des voies de recours par le consommateur, notamment en limitant indûment les moyens de preuve à la disposition du consommateur ou en imposant à celui-ci une charge de preuve qui, en vertu du droit applicable, devrait normalement revenir à une autre partie au contrat.

3.2.1.2.3. Le projet de décret d'application transposant la directive signature électronique

Le décret fixe les conditions dans lesquelles la fiabilité d'un procédé de signature électronique est présumée (jusqu'à preuve contraire). Il revient ainsi à celui qui conteste la validité d'une signature réalisée selon un procédé respectant les conditions fixées dans le décret de faire la preuve de son manque de fiabilité. Inversement, une signature électronique est recevable dès lors qu'elle est réalisée suivant *un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache.* Il revient à celui qui revendique des droits découlant de cet acte de le démontrer lorsque le procédé de signature utilisé ne remplit pas les conditions fixées par le décret (il n'y a pas de présomption favorable dans ce cas).

La fiabilité d'un procédé sera présumée lorsque deux conditions sont remplies :

- ce procédé met en œuvre un dispositif de création de signature électronique qui répond aux critères définis à l'article 3 du décret. Cet article s'inspire des conditions fixées aux signatures électroniques avancées dans la directive, ainsi qu'aux dispositifs sécurisés de création de signature, visés à l'Annexe III de la directive ;

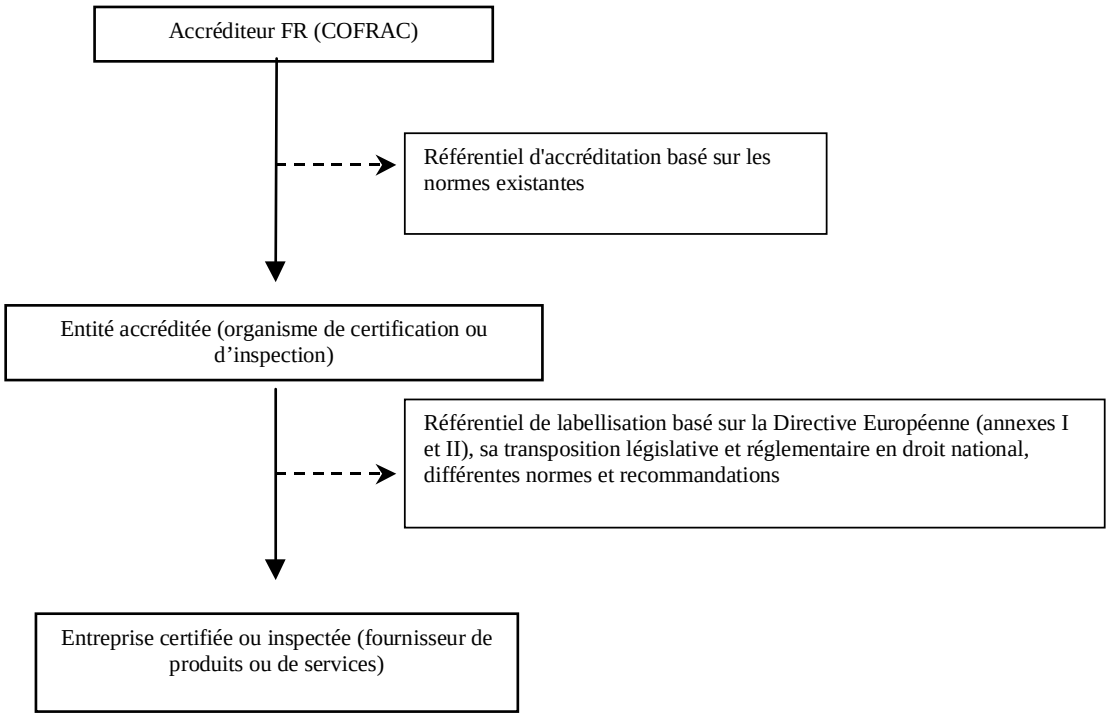
- ce procédé utilise un **certificat** électronique répondant aux critères définis à l'article 6, qui reprend les conditions figurant aux Annexes I et II de la directive visant respectivement les certificats et les prestataires qui les fournissent.

D'après la directive " signature électronique ", ni autorisation ni accréditation obligatoire ne peut intervenir préalablement à l'activité de prestataire de services de certification. Seuls sont possibles des contrôles *a posteriori*. En revanche, les Etats membres peuvent mettre en place un schéma d'accréditation volontaire, visant à élever le niveau de service.

Afin de faciliter le choix des utilisateurs et les travaux des tribunaux, la définition de critères et de pratiques de labellisation des prestataires de services de certification, impartiaux et objectifs, harmonisés au niveau international et permettant de qualifier *a priori* les niveaux de services offerts, s'est avérée nécessaire. Dans ce cadre sera mis en place un schéma d'accréditation volontaire des prestataires de services de certification. Le référentiel est fondé sur la directive européenne et notamment ses annexes I et II.

Ce schéma répond aux recommandations du Conseil d'État, qui, dans son rapport de septembre 1998, *«Internet et les réseaux numériques»*, soulignait qu'il paraissait " légitime de réserver certains effets juridiques à la production d'un certificat délivré par un certificateur accrédité garantissant le respect des exigences légales ". L'accréditation sera délivrée par le COFRAC à des organismes de certification ou d'inspection, qui évalueront, inspecteront puis certifieront les entreprises, qui utiliseront le certificat ou le label fourni. Le graphique ci-après décrit le dispositif d'accréditation voulu par le Secrétariat d'État à l'industrie.

Le schéma d'accréditation des prestataires de services de certification (PSC)



Les arrêtés pris en application du projet de décret " signature électronique " préciseront ce mécanisme d'accréditation.

3.2.2. La reconnaissance de l'écrit éléctronique comme formalisme *ad validitatem*

S'il convient bien entendu d'attendre l'adoption des textes réglementaires de transposition de l'article 9 de la directive « commerce électronique » visant à adapter le formalisme des textes actuels à l'électronique pour pouvoir se prononcer sur les modalités pratiques de leur mise en œuvre, les établissements sont invités à réfléchir sur ces points (voir notamment 8.2.3). Ils devront en effet, le cas échéant, se doter des infrastructures de sécurité permettant de remplir les exigences de forme de certaines opérations bancaires et financières.

3.3. Un cadre juridique européen en construction

3.3.1. L'impact de la directive " commerce électronique " en matière bancaire et financière

La directive " commerce électronique " consacre le principe de la liberté d'exercice d'une activité bancaire en ligne. Tout régime d'autorisation préalable est exclu, s'il vise exclusivement et spécifiquement le service en ligne.

En outre, l'article 3 de la directive " commerce électronique " pose le principe selon lequel « chaque État membre veille à ce que les services de la société de l'information fournis par un prestataire établi sur son territoire respectent les dispositions nationales applicables dans cet Etat membre relevant du domaine coordonné » et que les « Etats membres ne peuvent, pour des raisons relevant du domaine coordonné, restreindre la libre circulation des services de la société de l'information en provenance d'un autre Etat membre ». Il en résulte que le droit applicable aux services fournis en ligne est donc en principe celui du pays où le prestataire de ces services est établi et qu'il appartient aux autorités de ce pays de contrôler les conditions d'exercice de l'activité des services en ligne.

Selon l'article 3, troisième paragraphe, les Etats membres peuvent cependant, dans certains aspects du domaine coordonné et sous certaines conditions, déroger à la règle du pays d'établissement du prestataire en ligne, par exemple pour la protection des consommateurs et des investisseurs. Dans ce cas, les mesures doivent être justifiées et notifiées à la Commission européenne. Elles doivent être motivées par des risques sérieux et graves et doivent être proportionnées.

En matière de surveillance prudentielle du prestataire de service en ligne, la directive «commerce électronique» ne modifie pas le partage de responsabilité actuel entre pays d'origine et pays d'accueil, issu du Traité et de la seconde directive bancaire, ni le principe de la notification de libre prestation de services.

En revanche, la directive " commerce électronique " introduit une distinction entre le pays d'origine du prestataire et le pays d'établissement du prestataire du service de la société de l'information. Ainsi, par exemple, dans le domaine coordonné par la directive, le site d'une succursale implantée en Allemagne par un établissement bancaire de droit français, qui offrirait des services de la société de l'information à partir de l'Allemagne, sera soumis au droit allemand

(pays d'établissement du prestataire de services en ligne) mais non au droit français, qui demeurera applicable à la surveillance prudentielle du prestataire.

Par ailleurs, le principe de l'application du droit coordonné du pays d'établissement du prestataire de service en ligne ne s'applique pas pour toute une série de domaines, explicitement énumérés dans l'annexe de la directive. Ainsi des obligations contractuelles concernant les contrats conclus par les consommateurs.

3.3.2. La directive " commerce électronique " ne remet pas en cause les règles traditionnelles de droit international privé

La détermination de la juridiction compétente et de la loi applicable est actuellement régie pour les contrats par deux conventions, auxquelles sont parties tous les États membres, les Conventions de Rome et de Bruxelles, la première permettant de déterminer la loi applicable, la seconde la juridiction compétente. La directive " commerce électronique " n'établit pas de règle additionnelle de droit international privé. La Convention de Rome est d'application intégrale. Il en va de même pour les dispositions nationales de droit international privé, qui régissent les cas de relations transfrontalières non traités par les Conventions de Rome et de Bruxelles, à savoir tout le domaine extracontractuel. La Convention de Bruxelles est également d'application intégrale.

3.3.3. Le Livre vert de la Commission européenne sur le commerce électronique et les services financiers

Le Livre vert de la Commission sur le commerce électronique et les services financiers, qui sera publié courant 2001, devrait préparer une nouvelle étape d'approfondissement du marché intérieur. Est visée une harmonisation maximale des règles de protection des consommateurs, que doivent respecter les établissements dans le pays d'accueil. Les dérogations à l'approche par le pays d'origine (protection des consommateurs, des investisseurs, obligations contractuelles…) prévues par l'article 3 de la directive " commerce électronique " seront également réexaminées. Par ailleurs, les contradictions entre la directive " commerce électronique " et les directives sectorielles seront analysées.

La proposition de directive relative aux **services financiers à distance,** adoptée par la Commission fin 1998, s'inscrit dans cette logique. Les négociations ayant achoppé sur un désaccord politique entre les tenants de l'harmonisation minimale et les tenants d'une harmonisation totale, elles se poursuivent sur la base d'un inventaire effectué par la Commission portant sur les obligations d'information actuelles dans les quinze États membres. Ce «tronc commun» rassemblerait des informations générales sur la commercialisation du service (identité du fournisseur, durée de l'offre, conditions et modalités de rétractation, langue du contrat, etc.) voire sur le contenu même du service financier (prix et conditions de paiement et d'exécution du contrat).

DEUXIÈME PARTIE

L’ANALYSE DES RISQUES

L'ANALYSE DES RISQUES

Si Internet ne change pas la nature des risques financiers pris par un établissement sur son client ou sa contrepartie, les risques opérationnels (risques juridiques, dont certains ont été exposés précédemment, risque de blanchiment, risques de sécurité des systèmes d'information…) sont accentués.

En particulier, s'agissant de la sécurité des systèmes d'information, l'utilisation d'Internet, comme canal de distribution des services bancaires et financiers, implique un risque de " perméabilité " des systèmes de traitement de l'information des établissements avec les plates-formes web qu'ils ont mises en place et, par conséquent, avec les utilisateurs extérieurs. Cette ouverture ne constitue pas une totale nouveauté. De longue date, les établissements ont organisé des communications entre leurs systèmes et l'extérieur : échanges de fichiers et de messages, transmissions d'ordres, etc. Pour autant, jusqu'à présent, les échanges ont été réalisés soit au sein de la communauté financière (**SWIFT** par exemple) soit au moyen de réseaux publics maîtrisés par des opérateurs reconnus (norme de transfert **X25** gérée par **Transpac** notamment). L'Internet, en revanche, obéit à des **protocoles** de communication banalisés et accessibles à tous. En outre, sa maîtrise n'est pas confiée à un opérateur unique.

Les risques opérationnels liés à la sécurité des systèmes d'information, bien qu'accentués, revêtent un caractère traditionnel. A ce titre, les principes généraux exposés par le Livre blanc sur la sécurité des systèmes d'information de la Commission bancaire en 1996 sont toujours d'actualité. Le risque spécifique est celui d'une crise de confiance, liée à la perte de crédibilité du public et des clients, qui deviennent de plus en plus volatiles.

4. Les risques financiers

4.1. Les services classiquement rendus dans une relation physique sont ou seront en ligne

La communication par télétransmission entre le client et son banquier ou son prestataire de services d'investissement permet en effet l'échange de toutes les informations nécessaires à l'engagement des deux parties. On retrouve donc sur Internet l'ensemble des services classiquement rendus dans une relation physique ou, plus récemment, par téléphone :

- ouverture et fonctionnement d'un compte de dépôt, avec consultation du compte et opérations de paiements (par virement, prélèvements automatiques, TIP, émission de chèques, délivrance d'une carte de paiement voire d'une carte de crédit) ;

- octroi de crédits et de garanties : sous réserve des formalités légales imposées sur certains types d'opérations (notamment les crédits immobiliers) ;

- ouverture et fonctionnement d'un compte d'instrument financier : achat et vente de tous types d'instruments financiers, notamment lors des émissions de titres ;

- délivrance de conseils commerciaux.

Ces services pourraient d'ailleurs être étendus à d'autres types de services bancaires et financiers, par exemple :

- le recouvrement d'effets de commerce ;

- les introductions en bourse et placements d'émissions obligataires. Ces activités sont en plein développement aux États-Unis.

Les services existants ou en projet sur Internet ne font en revanche apparaître aucun service ou opération ayant une nature particulière. Tout au contraire, les prestataires engagés sur ce moyen d'échange mettent plutôt en avant la possibilité de réaliser par Internet toutes les opérations traditionnellement effectuées au guichet, voire par courrier, en bénéficiant des avantages d'un échange automatique : rapidité, faibles coûts, et même sécurité.

4.2. Les risques financiers sont de même nature

Ce caractère traditionnel des opérations bancaires et financières sur Internet a pour conséquence évidente que les risques de nature financière de l'établissement sur son client restent ceux existant dans le cadre d'une relation traditionnelle :

- **risque de crédit** pour les concours octroyés sous quelque forme que ce soit (prêts, avances, découverts autorisés en comptes, crédits revolving, facilités de trésorerie, voire garanties) ;

- **risque d'illiquidité** (inadéquation emplois/ressources) ;

- **risque d'intermédiation** sur les opérations d'investissement exécutées pour le compte du client.

En matière de contrôle interne du risque financier, les dispositifs classiques de maîtrise des risques, prévus par les prescriptions réglementaires en vigueur ou à venir (pour les prestataires de services d'investissement) sont suffisants.

Par ailleurs, sur le plan juridique, le maintien de la forme écrite a pour conséquence qu'Internet ne peut servir que de canal d'échange d'informations, tant qu'un contrat écrit n'est pas signé. A défaut de possibilité d'engagement par ce moyen, il ne peut y avoir de risques financiers.

Cette conclusion est naturellement remise en cause par les évolutions en cours du droit positif : projet de loi sur la société de l'information, transposition totale de la directive sur le commerce électronique, qui prévoit une adaptation des exigences juridiques de l'écrit-papier à l'électronique. Ces questions sont traitées au point 3.2 relatif au droit de la preuve. Une réflexion particulière devra, à ce titre, être menée en fonction des principes et règles retenus par le législateur.

5. Les risques opérationnels

Les risques opérationnels sont ici déclinés en plusieurs risques : risque juridique, risques liés à la sécurité des systèmes d'information, risques liés à la sécurité des transactions, risques en matière de blanchiment.

5.1. La sécurité juridique

Le caractère transfrontalier de l'offre " Internet " fait courir aux établissements de crédit et aux entreprises d'investissement des risques juridiques. Ils doivent se conformer, pays par pays, aux règles relatives à l'exercice de l'activité envisagée - notamment l'obtention d'un agrément -, aux règles relatives à la capacité des clients à effectuer des opérations bancaires et financières (conditions de majorité ou de capacité juridique, conditions d'accès au type de service proposé), aux conditions de forme de la prestation de services envisagée, notamment les conditions déclaratives ou les obligations de vérification (consultation de fichiers d'incidents par exemple) à l'ouverture d'un compte, aux régimes spécifiques de protection des clients (droit de la consommation, règles applicables à l'information des investisseurs,…), et notamment aux règles d'ordre public qui s'imposent aux parties, au régime fiscal, aux règles de preuve, etc.

Par ailleurs, au-delà du respect des règles relatives à la lutte contre le blanchiment, la connaissance du statut juridique du client est indispensable pour la maîtrise du risque juridique, compte tenu du caractère international de l'activité. Aussi l'établissement doit-il veiller à la sécurité juridique de toutes les opérations engagées avec ou pour le compte de son client. Il doit s'assurer en particulier du caractère certain de son consentement à l'opération, même transmis de manière dématérialisée.

Enfin, la transposition de l'article 9 de la directive «commerce électronique», qui prévoit l'adaptation du formalisme de l'écrit-papier à l'électronique (voir point 3.2. sur le droit de la preuve), fixera des règles de forme pour les contrats conclus électroniquement. La technique devra accompagner ces exigences juridiques, sous peine de nullité du contrat.

5.2. L'Internet bancaire et financier accentue la portée du risque opérationnel lié à la sécurité des systèmes d'information

5.2.1. La perméabilité entre systèmes d'information internes et Internet

Internet décloisonne les moyens d'échange et de traitement des données. Les réseaux internes et externes reposent en effet désormais avec Internet sur la même technologie **TCP/IP**. Les techniques utilisées sur ces terminaux à l'extérieur de l'établissement et le réseau public et les techniques utilisées en interne au sein de l'établissement sont identiques. En outre, les équipements terminaux ne sont plus spécifiques : ordinateurs personnels banalisés, téléphones portables, connectables depuis n'importe quelle localisation.

Internet rend possible le traitement entièrement automatisé d'un nombre très élevé d'échanges par unité de temps et rend enfin beaucoup plus probables (en fréquence et en amplitude) les attaques. Décloisonnement et nombre considérable d'internautes appelé à se développer à la faveur de l'accès au réseau par les téléphones ou autres appareils domestiques et mobiles se conjuguent pour rendre les systèmes d'information plus vulnérables.

En outre, l'opportunité ou même la nécessité d'externaliser l'informatique, de délocaliser ou d'éclater le système d'information sont désormais plus grandes qu'auparavant. Or, dans de telles situations, il peut s'avérer plus difficile de surveiller, de contrôler et de réagir directement à des attaques ou à des dysfonctionnements. La gestion du système d'information peut être même complètement externalisée. Le contrôle interne se doit, dans cette perspective, d'étendre son champ d'action.

Un site peut être dans l'incapacité de répondre aux appels des clients. Les attaques de déni de service, qui visent à saturer le serveur sous un flot de requêtes, se sont récemment développées. Tout site web a en effet une capacité maximale d'accès en cas de connexion simultanée. En outre, tous les jours, des failles potentielles dans des systèmes et/ou des produits sont mises en évidence sur Internet. Aussi, étant donné la nature évolutive des attaques en provenance d'Internet, l'évaluation de la politique de sécurité doit être actualisée de façon régulière et dynamique.

5.2.2. Le risque de réputation, qui peut se propager à l'ensemble de la place

Les risques opérationnels liés à la sécurité des systèmes d'information revêtent un caractère traditionnel. A cet égard, les principes généraux exposés par le Livre blanc de la Commission bancaire de 1996 sur la sécurité des systèmes d'information sont toujours d'actualité. Au delà des risques traditionnellement recensés, le risque spécifique attaché à l'utilisation d'Internet comme canal de distribution des services bancaires et financiers est celui d'une crise de confiance, liée à une perte de crédibilité de la part du public -et non seulement des clients- face à des dysfonctionnements : problèmes techniques, fraudes, malversations, déni de service. On ne peut non plus exclure les attaques visant à déstabiliser un établissement et à ternir son image (caricatures sur le site, images pornographiques, etc).

Les dysfonctionnements constatés dans un établissement ou les incidents rencontrés peuvent ternir sa réputation et le déstabiliser. Partant, ils comportent un risque de contagion à l'encontre de la communauté bancaire et financière dans son ensemble.

5.2.3. L'analyse du risque par le Comité de Bâle

En mars 1998, le Comité de Bâle a publié un rapport : " *Risk management for electronic banking and electronic money activities* ". Ce rapport recense -sans que la liste ait la prétention de l'exhaustivité- les risques auxquels sont soumis les banques électroniques. La teneur des risques opérationnels et du risque de réputation est particulièrement soulignée.

Le risque opérationnel est décliné en plusieurs risques. L'établissement doit faire face à un certain nombre de menaces : accès non autorisé dans le système informatique, injection

de **virus**, fraudes des employés. Ce risque est induit par certaines vulnérabilités : obsolescence du système, défaillances des fournisseurs d'accès, imprudences des clients, qui utilisent de l'information personnelle (numéros de carte de crédit ou numéros de comptes bancaires) dans des transmissions non sécurisées.

Afin de réduire le risque opérationnel, plusieurs mesures sont préconisées :

- mesures de sécurité visant à prévenir (pare-feu, mots de passe, techniques de cryptage), détecter et contenir des fraudes ou des dysfonctionnements ;

- mesures visant à évaluer le niveau effectif de sécurité du système (tests de vulnérabilité, audit externe) ;

- mesures visant à sensibiliser les clients aux enjeux de la sécurité.

Le risque de réputation est également souligné. Les clients face à des défaillances du système -diffusion large et rapide de fausses informations, usurpation d'identité à des fins malveillantes, attaque de sites- peuvent quitter la banque en masse.

Le Comité de Bâle devrait, dans le courant de l'année 2001, émettre à nouveau des recommandations en matière de maîtrise des risques des banques électroniques. Les différents principes en matière de contrôle interne, d'externalisation, de sécurité et de respect des données transmises seront déclinées en codes de bonne conduite. L'accent sera mis en particulier sur la sécurité et le respect de la vie privée des clients, sources de risques juridiques et de réputation, qui peuvent se propager à l'ensemble de la place.

5.3. Identification/authentification, intégrité, confidentialité et non répudiation des transactions

5.3.1. Les besoins de sécurité des transactions bancaires et financières en ligne

Suivant le type de transactions, un certain nombre de besoins de sécurité doivent être remplis, pour permettre aux utilisateurs d'Internet, d'atteindre un niveau de confiance satisfaisant dans les opérations bancaires et financières en ligne :

- pouvoir correctement identifier et authentifier son interlocuteur ;

- avoir l'assurance que les messages qu'il envoie n'ont pas été altérés dans le transport (intégrité) ;

- avoir l'assurance que ces messages n'ont pas été portés indûment à la connaissance de tierces parties (**confidentialité**) ;

- et avoir l'assurance que l'interlocuteur ne peut nier être l'auteur d'un message (**non-répudiation**).

A l'heure actuelle, la plupart des solutions utilisées par les fournisseurs de services bancaires ou financiers en ligne pour leurs relations avec les particuliers (et dans certains cas les professionnels) ne permettent pas de garantir la **non-répudiation**[8], dans la mesure où les secrets (code confidentiel, clé privée) confiés au client sont stockés ou transitent en clair dans son PC qui constitue un environnement vulnérable aux attaques depuis le réseau (**chevaux de Troie** et **virus**). Notons que dans le domaine du «B to C» (Business to Consumer), la solution **cyber-Comm** utilisant un lecteur sécurisé de carte à puce permet d'assurer la **non-répudiation** des paiements par cartes bancaires sur Internet.

Dans cette situation, les clients peuvent contester les opérations effectuées à réception des relevés correspondants. Dans l'incapacité d'opposer à leurs clients la preuve de leur implication, les établissements n'ont d'autre choix que d'annuler la transaction en subissant éventuellement les pertes correspondantes ou d'aller au contentieux, en prenant un risque d'image significatif.

Les infrastructures de clés publiques (voir dans le glossaire **cryptographie à clef publique)** dans lesquelles interviennent des **autorités de certification**, qui émettent des **certificats** permettant de sécuriser la transaction, et les cartes à microprocesseur sont des contributions essentielles à la couverture de ces besoins.

Il convient toutefois de signaler que tous les pays n'ont pas la même aversion au risque et certains peuvent s'accommoder d'un environnement où les transactions sont répudiables. Il reste que cette incertitude juridique a un coût qui est facturé au client.

5.3.2. La cryptographie à clé publique apporte des solutions aux besoins de sécurité des transactions bancaires et financières en ligne...

Pour sécuriser les échanges, ont été principalement utilisés jusqu'à ce jour des systèmes à clés secrètes, dans lesquels chaque couple émetteur/récepteur possède sa propre clé secrète. L'émetteur utilise la clé pour chiffrer tout ou partie du message. Le récepteur, déchiffrant le message, s'assure que le message a bien été émis par le bon émetteur. Simultanément, le chiffrement du message garantit que celui-ci ne peut être intercepté par un tiers. Ce système est mal adapté à Internet. En effet, dans une architecture décentralisée, chaque fois que l'on crée un nouveau couple émetteur/récepteur, il faut créer une nouvelle clé secrète. Si un utilisateur doit communiquer avec quelques centaines de correspondants, il lui faudra alors gérer un nombre équivalent de clés et les faire parvenir de façon sûre.

En revanche dans une infrastructure à clé publique, chaque acteur dispose d'un couple clé sécrète/clé publique. La clé privée est gardée secrète pour qu'une seule personne puisse l'utiliser. A l'inverse, la clé publique est connue et utilisée par tous. Ce couple de clés ou bi-clé est conçu de telle sorte qu'un message crypté en utilisant l'une des clés peut être décrypté en utilisant l'autre, et seulement l'autre. L'utilisation de la clé privée générera la signature d'un document. Tout lecteur de ce document ayant accès à la clé publique de l'utilisateur sera alors à même de vérifier cette signature. Ce mécanisme présente une analogie avec l'acte de signature manuscrite.

---

8) Impossibilité pour l'utilisateur ou le prestataire de nier qu'il est l'auteur de la transaction et que celle-ci existe bien.

Mais, pour que la clé publique devienne un véritable passeport électronique et identifie de façon sûre une seule personne, une opération supplémentaire est nécessaire : un tiers certificateur doit intervenir pour garantir que la clé publique d'une personne est bien la bonne. Il s'agit, en effet, d'empêcher qu'un escroc présente à la communauté sa clé publique en la faisant passer pour la clé publique d'une autre personne.

5.3.3. ...mais les organisations à mettre en place sont complexes...

Du fait de la nécessité de générer et distribuer les certificats dans le cadre de procédures sécurisées, les infrastructures à clés publiques ont été mises en œuvre, jusqu'à maintenant, principalement au sein de communautés fermées d'utilisateurs, qui sont généralement de taille réduite.

En outre, lorsque deux internautes cherchent à établir une relation commerciale sur Internet, il est improbable qu'ils disposent de certificats émis par la même autorité de certification. Chacun d'entre eux n'a aucune raison a priori de faire confiance à **l'autorité de certification** de l'autre. Le **protocole SSL** permet en théorie à un particulier d'authentifier le serveur du commerçant ou de la banque avec lequel il rentre en relation[9] ; dans la pratique, il peut consulter le **certificat** de clé publique de son interlocuteur, signé par l'autorité de certification de celui-ci ; mais quelle confiance peut-il faire a priori à cette autorité, en particulier si elle se situe dans un pays étranger ?

6. Interopérabilité des autorités de certification

L'interopérabilité des autorités de certification est une condition nécessaire du développement de la confiance : elle peut être obtenue soit par des accords bilatéraux de reconnaissance mutuelle, soit de façon plus simple, par des architectures arborescentes avec des autorités mères qui fixent au niveau international les règles (politiques de certification) applicables aux autorités filles, et assurent la promotion auprès du public visé de leur image de marque. Ces infrastructures se mettent en place progressivement dans le domaine bancaire, notamment dans le secteur inter-entreprises (GTA, IDENTRUS).

5.3.4. ... et les cartes à puce sont un complément indispensable des infrastructures à clés publiques

D'autres difficultés techniques restent à résoudre si l'on cherche à assurer la **non-répudiation** des opérations. En particulier, la conservation des secrets (clé privée, code confidentiel) permettant à l'utilisateur de donner son consentement aux transactions ne peut se faire pour l'instant de façon sûre dans un environnement de type PC où des **virus** ou des **chevaux de Troie,** dont le seul but est de capturer ces secrets, peuvent être téléchargés par mégarde. La mise en oeuvre d'une sécurité satisfaisante nécessite l'utilisation de dispositifs matériels spécifiques, à savoir une carte à microprocesseur et un lecteur sécurisé. Aux Pays-Bas, Interpay met en œuvre une solution similaire à **Cyber-Comm**. En Allemagne, la BfG BANK et la RVB MAINZ ont toutes deux retenu depuis avril 1998 la solution de la carte à puce comme **interface** de sécurité, à la suite de la SPARDA BANK de Hamburg, qui la première a développé ce projet. Les banques françaises ont pris de l'avance dans ce domaine avec **Cyber-Comm** et sa solution sécurisée de paiement par cartes bancaires fondée sur le protocole **SET.**

9) Les différentes versions du protocole SSL remplissent des fonctionnalités différentes. Si le protocole SSL V.2. permet d'authentifier le serveur du commerçant ou de la banque avec lequel il entre en relation, mais pas le contraire, le protocole SSL V.5. permet d'identifier le client et le serveur. Dans ce cas, le client doit posséder un certificat produit soit par la banque soit par un PSC externe.

5.3.5. L' analyse des risques induits par les prestataires de service de certification (PSC) intervenant dans le secteur bancaire et financier

Les préoccupations des autorités bancaires obéissent à une double logique. Il s'agit de s'intéresser, d'une part, au titre de l'article 4 de la loi du 4 août 1993, aux préoccupations liées à la sécurité des paiements, qui font actuellement l'objet d'une étude prospective entre Banques centrales au niveau international, et d'autre part, à la sécurité de la relation entre l'établissement de crédit ou l'entreprise d'investissement et ses clients, où le point d'appui réglementaire est l'article 14 du règlement 97-02 sur le contrôle interne et l'article 15 de la loi bancaire.

L'article 14 du règlement n° 97-02 relatif au contrôle interne dispose que :

" Les établissements de crédit déterminent le niveau de sécurité informatique jugé souhaitable par rapport aux exigences de leurs métiers. Ils veillent au niveau de sécurité retenu et à ce que leurs systèmes d'information soient adaptés. Le contrôle des systèmes d'information doit notamment permettre :

a) de *s'assurer que le niveau de sécurité des systèmes informatiques est périodiquement apprécié et que, le cas échéant, les actions correctrices soient entreprises ;*

b) de s'assurer que les procédures de secours informatique sont disponibles afin d'assurer la continuité de l'exploitation en cas de difficultés graves dans le fonctionnement des systèmes informatiques.

Le contrôle des systèmes d'information s'étend à la conservation des informations et à la documentation relative aux analyses, à la programmation et à l'exécution des traitements ".

L'article 15 de la loi bancaire dispose, quant à lui, que " le Comité apprécie également l'aptitude de l'entreprise requérante à réaliser ses objectifs de développement dans des conditions compatibles avec le bon fonctionnement du système bancaire et qui assurent à la clientèle une sécurité satisfaisante ".

À ce titre, les autorités bancaires ne peuvent rester indifférentes aux risques juridiques (voir à ce propos le point 8.1.2. sur la maîtrise du risque juridique au regard du recours aux **PSC**) et financiers (usurpation d'identité, altération, détournement de transactions, possibilité de répudiation), qui résulteraient **d'autorités de certification** utilisant des dispositifs techniques défaillants, ou ayant des politiques de certification peu sûres.

Dans la mesure où les structures de certification sont en cours de formation et que des travaux de normalisation sont en train d'être menés, il serait prématuré de vouloir dresser, à ce stade, une liste exhaustive des exigences de sécurité. Il reste que les risques induits par les **PSC** intervenant dans le secteur bancaire et financier devraient être analysés avec précision.

5.4. Risques en matière de blanchiment présentés par l'utilisation d'Internet

Le blanchiment est le fait de faciliter, par tout moyen, la justification mensongère de l'origine des biens ou des revenus de l'auteur d'un crime ou d'un délit ayant procuré à celui-ci un profit direct ou indirect. Constitue également un blanchiment le fait d'apporter un concours à une opération de placement, de dissimulation ou de conversion du produit direct ou indirect d'un crime ou d'un délit. Le délit de blanchiment est considéré comme aggravé lorsqu'il est commis de façon habituelle ou en utilisant les facilités que procure l'exercice d'une activité professionnelle. Trois étapes sont ainsi distinguées pour la réalisation d'opérations de blanchiment :

- le placement consiste à introduire les fonds provenant d'un crime ou d'un délit dans le système bancaire, notamment par le moyen de dépôts en espèces ;

- la dissimulation consiste à masquer l'origine criminelle des fonds, grâce à des virements et montages financiers ;

- la conversion consiste à investir les fonds dissimulés dans les circuits économiques licites, par le biais d'investissements divers.

5.4.1. Services financiers sur Internet et perméabilité au blanchiment

Les opérations bancaires effectuées sur Internet ne paraissent pas présenter de risques de nature spécifique en matière de blanchiment d'argent. En revanche, trois facteurs principaux accroissent les risques traditionnels : **facilité d'accès au réseau** sans contrainte géographique, matérielle ou temporelle, **dématérialisation, et rapidité des opérations**.

Ces trois facteurs, dans un contexte de traitement automatisé des opérations, rendent le contrôle des flux financiers plus complexe, tant au moment de l'entrée en relation avec le client que lors de la réalisation des transactions financières.

5.4.1.1. Ouverture de compte et entrée en relation avec la clientèle

Le risque de blanchiment survient essentiellement à propos des clients nouveaux d'une "banque Internet", qu'elle soit ou non intégrée à une banque traditionnelle. Il est lié à l'accomplissement à distance des formalités administratives d'ouverture de compte, en l'absence d'un entretien impliquant la présence physique du client. Bien que de même nature que dans une banque traditionnelle, les problèmes liés à l'identification du client, personne physique ou morale, sont accrus de par la dématérialisation de l'entrée en relation :

- fausse identité pour une personne physique, avec production de faux documents justificatifs ;

- identification d'une personne morale dont l'existence juridique réelle ne peut être vérifiée ou qui exerce une activité fictive ;

- ouverture de compte au nom de structures juridiques domiciliées dans des territoires dans lesquels des dispositions ont été prises pour garantir l'anonymat de leurs ayants droit ;

- authentification de la signature du client, qui s'impose également pour la réalisation des opérations bancaires.

En outre, des renseignements tels qu'un changement d'adresse ou la mise en œuvre d'une procuration peuvent dissimuler une modification de l'identité des utilisateurs du compte. En conséquence, le suivi administratif des titulaires des comptes ouverts à distance devra être aussi rigoureux que l'ouverture du compte.

Il est à souligner que la difficulté d'établir avec certitude l'identité d'un client est encore plus grande pour des clients non-résidents pour lesquels les organismes financiers disposent de moins de moyens pour vérifier certains renseignements communiqués par le client.

5.4.1.2. Dématérialisation et automatisation des opérations

Les services financiers offerts sur Internet se distinguent de ceux offerts à distance par téléphone ou par courrier par la dématérialisation et l'automatisation totale de la relation avec le client.

Le risque de blanchiment est d'autant plus fort que les opérations financières utilisées à cet effet (opérations en espèces et scripturales) s'effectuent dans un processus entièrement automatisé avec des opérateurs n'ayant pas de relation personnelle avec leur gestionnaire de dossier, contrairement à ce qui se produit dans une banque traditionnelle.

Or, ce qui peut caractériser une "banque Internet" c'est d'une part la possibilité offerte au client - et la volonté de ce dernier - de traiter lui-même ses opérations à distance, et d'autre part pour la " banque Internet " une réduction considérable des coûts de gestion en personnel. Il est à craindre que quelques gestionnaires de dossiers soient en charge d'un nombre considérable de clients au point de ne pas connaître suffisamment leur clientèle, même s'ils sont dotés de systèmes de surveillance. Dans ce contexte, certains clients peuvent profiter de la dépersonnalisation de leurs relations avec l'établissement teneur de compte pour effectuer des opérations de blanchiment.

5.4.1.2.1. Les opérations d'espèces, retraits et versements

Il convient ici de souligner que le fonctionnement d'un compte intégralement géré sur Internet est parfaitement assimilable à celui d'un compte classique, en termes d'étendue des opérations réalisables par le client.

En effet, une fois le compte ouvert à distance sur Internet, des opérations de retraits ou de versements d'espèces pourront être effectuées automatiquement en recourant à des DAB ou à des guichets automatiques libre service, sans aucun contact physique entre le client et son banquier.

En outre, même dans l'hypothèse où selon des accords passés entre une "banque Internet" et une banque traditionnelle, cette dernière assurerait un service de retraits ou de versements d'espèces au profit des clients ayant ouvert un compte auprès de la "banque Internet", il subsisterait néanmoins un risque lié à la non-connaissance du client et de son profil de compte par la banque traditionnelle, ou simplement à une mauvaise application des mesures anti-blanchiment par la banque traditionnelle.

Il reste que l'introduction massive d'espèces dans le circuit bancaire par des blanchisseurs s'effectue plutôt auprès de guichets de banques traditionnelles, situées de préférence dans des zones peu contrôlées, notamment les paradis réglementaires. Les fonds font ensuite l'objet de transferts par le réseau bancaire traditionnel ou Internet.

5.4.1.2.2. Les opérations scripturales

Il s'agit essentiellement des opérations de virements, transferts qui permettent de véhiculer des capitaux.

Les ordres de transferts, transmis par le client et qui feraient l'objet d'un traitement automatisé par le service des transferts de la "banque Internet", autorisent des mouvements de capitaux sans qu'un gestionnaire de dossier puisse opérer un quelconque contrôle de vraisemblance de l'ordre de transfert par rapport au profil du compte, compte tenu notamment des revenus du titulaire, de son activité, de son statut de résident ou de non résident, de la destination des fonds.

L'automatisation du processus détruit la mémorisation naturelle par le gestionnaire du compte des caractéristiques de fonctionnement de ce dernier, et n'apporte plus l'opportunité de mieux connaître le client à l'occasion d'entretiens courants dans une banque traditionnelle.

La "banque Internet" est susceptible de disposer d'une clientèle plus largement cosmopolite, comprenant potentiellement une part importante de non-résidents qui pourraient être tentés de chercher à bénéficier d'une certaine opacité des opérations à travers des processus automatisés. La gestion à distance facilite également les mouvements de fonds via le réseau Internet sous la forme de virements, éventuellement internes dans le cas d'opérations de compte à compte au sein de la même "banque Internet".

Dans l'état actuel de la technologie en matière de système de paiement, il convient de souligner que l'automatisation totale (" *straight-through-processing* ") des virements transfrontaliers -c'est-à-dire les plus risqués en matière de blanchiment des capitaux- est encore difficile en raison notamment de la multiplicité des canaux de paiement utilisables et des problèmes de standardisation des messages au niveau international. Toutefois, ce risque ne peut être négligé dans la mesure où ces obstacles à l'automatisation seront probablement levés de façon progressive.

A défaut d'un système de surveillance approprié à des opérations effectuées selon un processus automatisé, la " banque Internet " amplifie les risques de blanchiment qui existent déjà avec des banques traditionnelles.

Par conséquent, l'automatisation et la dématérialisation des opérations autorisées par Internet obligera les établissements à modifier leurs techniques classiques de contrôle des opérations.

5.4.1.3. Facilité d'accès par Internet à des techniques traditionnelles de blanchiment

Est visée ici, non pas l'utilisation par les blanchisseurs de services bancaires offerts à d'autres fins que le blanchiment sur Internet, mais la mise en œuvre grâce à Internet des techniques traditionnelles de blanchiment que sont l'utilisation des paradis fiscaux ou la création de sociétés écrans :

- les services bancaires offerts sur Internet par des banques installées dans les territoires non coopératifs, où la législation sur la lutte contre le blanchiment est insuffisante ou inexistante et la législation sur le secret bancaire très protectrice du client ;

- les sites Internet proposant de créer des sociétés dans des paradis fiscaux, et offrant divers services bancaires off-shores ou des services de domiciliation et de prête-noms comme actionnaires ou dirigeants de sociétés.

Internet permet un accès plus rapide et plus facile à ces services et constitue dès lors un risque non négligeable de développement des opérations de blanchiment.

5.4.2. Monnaie électronique

Est désignée sous le vocable de **monnaie électronique** une créance sur l'émetteur de cette monnaie, incorporée dans un support électronique et acceptée en paiement par des tiers autres que l'émetteur. Le support électronique peut être une carte à microprocesseur, et l'on parle alors de **porte-monnaie électronique** (PME). Lorsqu'il s'agit d'un serveur placé sous la responsabilité de l'émetteur et accessible depuis un PC équipé d'un logiciel adéquat par l'intermédiaire du réseau Internet, on parle de **porte-monnaie virtuel** (PMV).

5.4.2.1. Porte-monnaie électroniques (PME)

Les risques de blanchiment liés au développement des porte-monnaie électroniques, en particulier des PME anonymes et de ceux qui permettent de réaliser des opérations de transfert de valeur électronique de carte à carte, ont fait l'objet d'analyses dans le cadre des travaux de révision de la directive « blanchiment » ; elles sortent a priori du cadre de ce rapport consacré aux risques de blanchiment générés par les opérations bancaires et financières sur Internet.

On signalera simplement que le rechargement des PME est possible sur Internet directement à partir d'un compte bancaire ou en utilisant une carte bancaire classique ; le paiement des commerçants virtuels sur Internet est également proposé par de nombreux systèmes. Ces opérations se font alors à l'aide d'un lecteur de cartes à microprocesseur connecté au PC. Elles ne génèrent pas de risques autres que ceux qui ont déjà été identifiés pour les PME utilisés de manière traditionnelle : les PME, lorsqu'ils sont anonymes ou dotés d'une

fonction de transfert de carte à carte, peuvent servir à des opérations de blanchiment, car ils permettent de dissimuler des revenus ou de transférer des fonds, mais ce risque peut être limité par certaines caractéristiques des PME, telles que le plafond de rechargement de la carte, la limitation du nombre de rechargements possibles de la carte, la limitation du nombre maximum de cartes par client, les modalités de chargement des PME.

Certaines de ces caractéristiques sont délibérément choisies par les promoteurs des PME eux-mêmes ; à défaut, les autorités devront s'interroger sur l'opportunité de les rendre obligatoires.

Pour sa part, la Banque de France considère qu'il est souhaitable de rendre obligatoire l'identification des personnes auxquelles est délivré un PME dont la capacité maximale excède un certain montant et/ou l'identification des clients effectuant des opérations d'acquisition ou de rechargement de monnaie électronique excédant un certain montant autrement que par débit d'un compte ouvert auprès d'un établissement de crédit assujetti à une obligation d'identification.

5.4.2.2. Porte-monnaie virtuels (PMV)

Les porte-monnaie dits virtuels (PMV) permettent d'utiliser une réserve de valeur pour l'achat de services offerts sur Internet à partir des ordinateurs personnels. Le risque d'utilisation de ces PMV par des blanchisseurs est lié au fait que la réserve de valeur est détenue de manière anonyme. Elle pourrait donc être utilisée de façon anonyme, pour acquérir des actifs (financiers notamment) ou transférer des fonds.

Ce risque apparaît cependant limité puisque que cette réserve de valeur est constituée ou reconstituée par débit d'un compte bancaire (production d'un numéro de carte bancaire pour l'opération de chargement ou rechargement) ; il demeure que cela ne garantit pas que le titulaire dudit compte soit identifié mais seulement une traçabilité de l'opération. Il n'est d'ailleurs pas exclu que le chargement ou rechargement d'un PMV puisse provenir d'un PME lui-même anonyme.

On doit souligner à cet égard que, conformément à la directive n° 2000/46 du 18 septembre 2000 concernant l'accès à l'activité des établissements de monnaie électronique et son exercice, les émetteurs de PMV et de PME devront avoir le statut d'établissement de crédit et être assujettis à ce titre aux obligations d'identification de leurs clients ainsi qu'à la déclaration de soupçon prévues par la directive n° 91/308 du 10 juin 1991 relative à la prévention de l'utilisation du système financier aux fins de blanchiment des capitaux.

Une autre atténuation du risque susvisé provient de la capacité maximale de chargement des PMV, qui limite la nature et le montant des transactions pouvant être réalisées au moyen de cet instrument. Cette contrainte résulte de la pratique actuelle mais non d'une obligation légale.

Enfin, il convient de signaler un risque de dérive qui consisterait à offrir aux titulaires des PMV d'autres services permettant de mobiliser les fonds concernés, que le seul service de paiement dédié ; on verrait alors apparaître de véritables comptes bancaires anonymes.

6. Les risques sur les clients et sur les contreparties

6.1 L'anonymat du client

L'anonymat relatif du client, surtout lorsqu'il est non-résident, rend plus difficile la détermination de sa capacité juridique et financière, ce qui pourrait conduire certains acteurs, dans un contexte de vive concurrence, à négliger les règles de base en matière de gestion du risque client. Ceci présente un réel danger dans la mesure où Internet donne accès à des opérations financières évoluées à des populations nouvelles (en particulier en matière d'opérations d'investissement) pour lesquelles les pratiques traditionnelles des professionnels, fondées sur la connaissance historique de clients à la fois fidèles et expérimentés, seraient totalement inadaptées.

6.2. Les effets sur la gestion du risque client de la concurrence, avivée par Internet

Les économies d'échelles importantes permises par Internet, ainsi que les évolutions technologiques permanentes, permettent et favorisent une concurrence extrêmement vive sur ce secteur, encore accrue par le faible seuil à l'entrée qui favorise la multiplication des acteurs, souvent de faible taille.

Le risque est d'autant plus élevé que le public visé, n'ayant souvent aucune culture technique, n'est pas préparé à accepter une défaillance du service qui lui est fourni. On peut donc craindre de sa part une faible fidélité à l'égard des prestataires, ce qui conduit à prévoir des mouvements importants de la clientèle, prompte à quitter un intermédiaire pour un autre en cas de problèmes techniques, notamment des délais de traitement élevés.

Cet état de fait pourrait conduire certains d'entre eux à négliger la maîtrise des risques au profit de leur rentabilité immédiate. En outre, une entreprise de petite taille, en cas de succès, peut se trouver prise de court par un volume de traitement du risque clients auquel elle n'est pas préparée.

6.3 La faible culture de prudence de certains prestataires de services sur Internet

Sur ce marché coexistent des établissements expérimentés, agissant soit par eux-mêmes, soit par une filiale, le cas échéant en joint-venture avec un partenaire technique, et des entreprises nouvelles, créées rapidement. Les premières, même si leur maîtrise de ces techniques nouvelles reste à démontrer, ont déjà une culture du risque, qui fait parfois défaut aux secondes.

TROISIÈME PARTIE

LA MAÎTRISE DES RISQUES

L'opposition entre une relation physique de l'établissement avec ses clients, dans le cadre d'une agence, et une relation à distance, regroupant à la fois la banque par téléphone, la télématique et Internet, semble peu pertinente. Il semble plus intéressant de distinguer entre des modes de relations humains, qui impliquent l'intervention d'un collaborateur ayant une liberté de décision, et les canaux automatisés.

- **Les canaux d'échange humains** : guichet, courrier, téléphone, télécopie

Le collaborateur est en mesure d'effectuer certains contrôles répondant à des situations imprévues ou spécifiques, sur la base d'une attribution personnelle de responsabilité sur les opérations qu'il engage.

Il est à noter que certaines activités menées par un canal Internet relèvent cependant d'un traitement humain, notamment dans le cas de l'activité de crédit à la consommation. Même si des informations sont échangées par Internet, elles donnent lieu à une analyse par un collaborateur, après entretien avec le client, avant tout engagement de l'établissement.

Dans ce cas de figure, la gestion du risque passe par la définition de procédures et le contrôle de leur respect ex-post par le contrôle interne de deuxième niveau.

- **Les canaux d'échange automatisés** : minitel, **audiotel**, télétransmission (dont Internet), écrans d'accès au système d'information mis à la disposition des clients

Cette solution particulière se rencontre fréquemment dans le domaine de la prestation de services d'investissement. Les écrans permettant d'accéder aux systèmes informatiques de routage d'ordres vers les marchés peuvent être délocalisés chez le client (généralement un institutionnel) ou mis à disposition de clients, souvent des particuliers, soit dans des locaux appartenant à l'établissement, soit dans les locaux d'un établissement tiers. Quel que soit le schéma retenu, cet accès direct aux systèmes internes de l'établissement engendre des exigences sécuritaires particulièrement aiguës.

Le client est en relation directe avec un système d'information : les informations et ordres reçus sont traités par le système conformément aux règles prédéfinies. Si un contrôle indispensable n'a pas été prévu, l'ordre sera exécuté sans possibilité de l'arrêter, voire même sans que l'établissement en soit informé.

Dans ce cas, la maîtrise des risques est fondée sur la définition de règles de gestion rigoureuses. Le contrôle interne de deuxième niveau doit être consacré à la vérification de leur correcte application par le système.

Les risques financiers et opérationnels encourus par les établissements de crédit et les entreprises d'investissement offrant leurs services en ligne militent en faveur d'un renforcement des moyens de contrôle. Tout particulièrement, il s'agit de préciser dans le cadre de

recommandations de bonnes pratiques les règles relatives au contrôle interne, fixées par le règlement n° 97-02 du Comité de la réglementation bancaire et financière.

7. Document relatif à la stratégie commerciale Internet de l'établissement

A ce titre, l'établissement devrait formaliser sa stratégie commerciale sur Internet, dans un document validé par les organes exécutif et délibérant, qui développerait en particulier le plan de développement de l'activité, en termes de services offerts, de clientèle, de volume d'activité et de rentabilité, en tenant compte de manière exhaustive des facteurs de risques techniques et commerciaux. Sur la base d'hypothèses prudentes, l'établissement validerait ainsi le montant des fonds propres requis pour assurer la pérennité de l'activité, y compris dans le cas d'une situation de crise, technique ou commerciale.

A tout le moins, trois types de risques de crise devraient être pris en compte : le risque commercial de forte chute du produit net bancaire, le risque d'atteinte à l'image et à la réputation de l'établissement suite à des problèmes techniques, le risque technologique d'inadaptation du système face à la croissance de l'activité.

Il est souhaitable que ce document relatif à la stratégie commerciale soit mis à jour et discuté à chaque étape du projet.

L'établissement devrait également avoir mis par écrit sa politique de maîtrise des risques (de contrepartie, juridique et technique) et l'avoir fait valider par son organe délibérant. Le responsable du contrôle interne devra recevoir une compétence explicite et exhaustive sur toutes les questions relatives à la sécurité des opérations sur Internet. Ce document servira de référence pour apprécier les dispositifs de sécurité mis en œuvre (voir point 8.1.1.).

Des recommandations plus spécifiques relatives à la maîtrise du système d'information, à la sécurité juridique, à la maîtrise du risque sur les clients et les contreparties, au contrôle de la rentabilité des opérations et à la lutte contre le blanchiment sont exposées ci-après.

7. Assise financière et suivi de la rentabilité

7.1. Vérification au moment de l'agrément de la solidité de la structure financière

Parmi les différents aspects qu'elles examinent dans le cadre d'une demande d'agrément, les autorités compétentes apprécient la viabilité et la rentabilité attendues du projet d'entreprise.

Elles analysent ainsi les moyens financiers dont disposera l'établissement et le soutien financier dont il pourra bénéficier, le cas échéant, de la part des apporteurs de capitaux.

Ces analyses s'appuient notamment sur des projections financières, généralement à trois ans, des principaux états comptables et des ratios prudentiels. Il va de soi que l'examen de ces caractéristiques financières prend en compte la dimension du projet en termes d'activités envisagées, de risques associés encourus et de parts de marché espérées.

Jusqu'à présent, les projets concernant l'exercice d'activités bancaires ou financières par Internet qu'ont eu à connaître les autorités portent presque exclusivement sur des demandes d'agrément d'entreprises d'investissement, adossées à des groupes bancaires ou financiers existants, ou constituant des acteurs nouveaux sur les marchés.

Les projets des entreprises d'investissement, agréées jusqu'à présent, qui peuvent être de dimensions variées, présentent les caractéristiques suivantes :

- ces établissements ont essentiellement demandé un agrément pour le seul service de réception/transmission d'ordres pour le compte de tiers. Quelques-uns ont également souhaité être autorisés à effectuer les services d'exécution d'ordres pour le compte de tiers ou de placement. Dans ce dernier cas, une tendance semble se dégager allant vers la mise en place d'un accès aux marchés primaires obligataires ou actions grâce à Internet. Enfin, un nombre réduit d'entreprises a demandé et obtenu une habilitation pour assurer la tenue de compte-conservation ;

- certains intermédiaires agréés, visant le marché de l'Internet, ont opté pour une offre de type " discount broker ", c'est-à-dire à des tarifs (généralement forfaitaires) plus attractifs que ceux jusqu'alors le plus fréquemment pratiqués. L'offre de services d'investissement peut être complétée par un accès à des données économiques et financières en provenance de fournisseurs d'informations connus. En revanche, d'autres intermédiaires Internet privilégient une offre de services plus large, associant par exemple plusieurs services d'investissement et la mise à disposition d'analyses financières, de forums ou d'outils de simulation, d'aide à la décision et à la gestion de portefeuille ;

- un grand nombre d'établissements a retenu une organisation fondée sur un large appel à l'externalisation ou au développement de partenariats avec d'autres prestataires de services d'investissement ou informatiques.

En matière de développement et de gestion financière prévisionnelle, certaines constantes peuvent également être dégagées :

- tout d'abord, s'il est indéniable que la nouvelle économie a un potentiel de croissance très fort, l'acquisition et la conservation de parts de marché, notamment pour les nouveaux entrants, restent difficiles à évaluer et risquent d'être d'un coût croissant ;

- positionnés sur un marché très concurrentiel, les prestataires de services d'investissement doivent donc être connus et reconnus, ce qui exige de mettre en place une politique mercatique et publicitaire aux moyens conséquents et de s'assurer de la qualité des services technologiques utilisés (en termes de sécurité, de facilité d'accès, de rapidité de réalisation des opérations financières, d'adaptation à l'évolution des logiciels et des matériels, etc).

Ces spécificités des intermédiaires Internet se traduisent sur le plan financier par une structure des charges où les frais généraux (publicité et informatique) sont en général de montants très élevés.

Les autorités d'agrément sont amenés à s'assurer que les établissements disposent de moyens financiers adaptés à la nature et au volume des activités envisagées. En tout premier lieu, les montants de capital minimum prévus par la réglementation doivent être respectés. Ces minima varient selon le type de statut demandé (35 MF pour les banques, 12,5 MF pour les sociétés financières, de 0,5 MF à 12,5 MF pour les entreprises d'investissement en fonction des services exercés). De plus, l'activité de teneur de compte-conservateur nécessite un capital minimum de 25 MF.

D'autre part, les autorités d'agrément s'assurent que le niveau de fonds propres permet le respect des normes de gestion définies par le Comité de la réglementation bancaire et financière.

Il a ainsi été constaté que les projets d'entreprises d'investissement exerçant par Internet requerraient, dans la quasi totalité des cas, des moyens initiaux en capital largement supérieurs au capital minimum réglementaire afin de respecter, notamment, la règle imposant un rapport minimal de 25 % entre les fonds propres et les frais généraux conformément à la norme européenne. En outre, le retour sur investissements n'étant généralement pas programmé avant la deuxième année au plus tôt, une mise de fonds initiale conséquente apparaît d'autant plus nécessaire.

Aussi les activités menées via Internet, lorsqu'elles ne sont pas développées au sein de groupes bancaires existants, sont–elles proposées par des établissements qui s'appuient assez fréquemment sur un actionnariat diversifié, pouvant comprendre des personnes physiques à l'origine du projet, mais aussi des associés à caractère institutionnel (bancaire ou financier) ou issus d'autres secteurs professionnels (de l'informatique en particulier), ayant la capacité d'apporter le soutien financier nécessaire pour faire face à l'évolution des activités ou à d'éventuelles difficultés.

Outre la vérification de cette possibilité de soutien financier qui peut être formalisée par un engagement spécifique, les autorités d'agrément s'assurent également que la qualité

des apporteurs de capitaux et l'organisation de l'actionnariat favorisent la viabilité du projet. Cette appréciation, qui s'inscrit dans le cadre des missions confiées aux autorités et qui s'appuie sur la doctrine progressivement établie, doit notamment prendre en compte l'absence d'expérience bancaire ou financière de certaines personnes morales associées dans le cas de projets largement orientés vers le support de l'Internet.

Les critères d'appréciation retenus par les autorités d'agrément, qui reposent sur des principes généraux, restent bien adaptés à l'examen de projets sur Internet. Cependant, afin de renforcer le diagnostic financier, il semble opportun de demander la réalisation systématique de scénarios de crise, qui doivent permettre d'apprécier le niveau d'aversion au risque des intervenants et plus fondamentalement leur assise financière sur un horizon de temps déterminé.

8. Etablissement de scénarios de crise pour apprécier la solidité de la structure financière

Sur les deux postes de charge sensibles constitués par les coûts technologiques -qui, s'ils sont mal maîtrisés, peuvent générer des risques opérationnels, des risques de marché, des risques de réputation- et les coûts publicitaires, il apparaît souhaitable que les établissements élaborent des scénarios de crise permettant :

- **d'évaluer l'impact sur le compte de résultat d'une chute de volumétrie du nombre d'opérations, causée par exemple par un mouvement de désaffection de la clientèle. La mise en œuvre de provisionnements pour risques opérationnels résultant d'une défaillance technique ponctuelle peut être envisagée ;**

- **de tester le niveau de résistance à une " guerre " publicitaire ou tarifaire. A titre d'exemple, des chutes spectaculaires de marge ont eu lieu aux États-Unis et/ou sont prévues sur les produits les plus banalisés.**

7.2. Le suivi de la rentabilité

7.2.1. Le contrôle de la rentabilité des opérations et l'article 20 du règlement n°97-02 du Comité de la réglementation bancaire et financière

Cette disposition réglementaire trouve directement à s'appliquer aux opérations de crédit sur Internet. Dans son esprit, elle peut être étendue à l'ensemble de l'activité Internet de l'établissement.

Article 20

" La sélection des opérations de crédit doit également tenir compte de leur rentabilité, en s'assurant que l'analyse prévisionnelle des charges et produits, directs et indirects, soit la plus exhaustive possible et porte notamment sur les coûts opérationnels et de financement, sur la charge correspondant à une estimation du risque de défaut du bénéficiaire au cours de l'opération de crédit et sur le coût de rémunération des fonds propres ".

7.2.2. Suivi de la rentabilité globale

9. Bonnes pratiques en matière de suivi de la rentabilité globale

Sont exposées ci-après des bonnes pratiques en matière de suivi de la rentabilité globale. L'établissement, en particulier en phase initiale de son activité, évalue la rentabilité future de ses activités, sur la base d'hypothèses prudentes, notamment sur le poste marketing et en suit la rentabilité effective. Les calculs de rentabilité intègrent des scénarios de crise, couvrant l'hypothèse d'une fuite massive de la clientèle.

La rentabilité devrait être analysée sous l'angle :

- d'une nouvelle entreprise (y compris filiale spécialisée de groupe) : Internet est le centre de l'activité, et, s'agissant d'une entreprise nouvelle ou en croissance, la question principale porte sur les prévisions d'activité de l'établissement, qui conditionnent le délai pour parvenir à la rentabilité ;

- d'une extension d'activité d'un établissement ancien : dans ce cas, Internet est plutôt un canal complémentaire offert à la clientèle existante, et accessoirement le moyen de conquérir des clients nouveaux. Le problème est plutôt de distinguer, parmi les coûts et les produits de l'activité générale, l'apport particulier de l'activité Internet.

Dans les deux cas toutefois, la rentabilité des fonds importants engagés est une question importante, voire cruciale. Elle doit être considérée comme stratégique et retenir l'attention de la direction de l'établissement. Les recommandations suivantes pourraient être formulées à cet égard.

L'établissement devrait tenir compte, pour calculer la rentabilité effective et estimer la rentabilité prévisionnelle de ses opérations par un canal automatisé, de l'ensemble des éléments de coûts et surtout de risques particuliers à ce mode de communication, qu'il met en regard des avantages et économies attendues (le coût stratégique du défaut de développement de l'activité doit être évalué). En particulier, la rentabilité calculée inclut :

- les coûts de démarchage et de publicité ;

- le risque de fraude. L'établissement doit prendre en compte à la fois les dommages financiers directs causés par la fraude et ses conséquences en termes d'image.

Il est raisonnable de compléter la réflexion par l'étude de scénarios de crise, sur la base d'hypothèses extrêmes, impliquant des moyens importants pour rétablir la continuité de l'entreprise et sa crédibilité vis-à-vis de ses clients et partenaires. Les hypothèses pourraient être :

- une attaque majeure du système en vue de provoquer son indisponibilité et ruiner la crédibilité technique de l'établissement ;

- un défaut de conception entraînant une dégradation inacceptable des performances du système face à une pointe de charge, provoquant la fuite de la clientèle et nécessitant des travaux importants pour rétablir le niveau de service promis aux clients ;

- une campagne systématique de dénigrement menée par des concurrents sur la base de problèmes techniques, réels ou imaginaires.

Les calculs de rentabilité prévisionnelle doivent démontrer que l'établissement disposerait dans ces situations extrêmes des moyens permettant de financer les mesures de rétablissement de la situation.

En parallèle, l'établissement calcule la rentabilité des opérations par type d'opérations et par catégories de clients, permettant de déterminer si les efforts mercatiques sont bien orientés et si la clientèle développée est optimale en termes de rentabilité.

Lorsqu'il intervient de manière distincte (notamment pour des clientèles différentes) sur plusieurs canaux de distribution (Internet + téléphone, voire agences), l'établissement devrait suivre et anticiper la rentabilité de ses opérations en distinguant chaque canal, avec pour objectif de tenir compte des coûts spécifiques à chacun d'eux, et des caractéristiques des clients qui l'utilisent plus particulièrement. Un suivi fin doit permettre notamment de connaître la rentabilité de l'extension de l'activité à des populations nouvelles de clients.

8. La maîtrise des risques opérationnels

8.1. L' intégration des activités Internet dans l'organisation du contrôle interne

Comme pour toute activité bancaire et financière, il est important que l'activité en ligne soit fermement sous le contrôle des organes de direction et des instances de contrôle interne de l'établissement, et le cas échéant du groupe.

8.1.1. Rôle des organes exécutif et délibérant

Préalablement au lancement d'un projet Internet, l'organe exécutif devrait formaliser sa stratégie dans un document validé par l'organe délibérant. Celui-ci détaille, en particulier, le plan de développement de l'activité, en termes de services offerts, de clientèle, de volume d'activité et de rentabilité, en tenant compte de manière exhaustive des facteurs de risques techniques et commerciaux. Sur la base d'hypothèses prudentes, l'établissement valide le montant des fonds propres requis pour assurer la pérennité de l'activité, y compris dans le cas d'une situation de crise, technique ou commerciale. A tout le moins, trois types de risques de crise doivent être pris en compte : le risque commercial de forte chute du PNB ; le risque d'atteinte à l'image et à la réputation de l'établissement suite à un problème technique ; le risque technologique d'inadaptation du système face à la croissance de l'activité.

10. Document relatif à la maîtrise des risques de contrepartie, juridiques et techniques

L'établissement devrait également avoir mis par écrit sa politique de maîtrise des risques et l'avoir fait valider par son organe délibérant. Ce document présente, notamment, les principes retenus en matière de risques :

- **de contrepartie : critères de sélection des clients, des contreparties et des marchés, évaluation et suivi du risque de crédit…**

- **juridiques : définition du niveau de risque jugé acceptable en raison des limitations de responsabilités inscrites dans les conventions tant avec les clients qu'avec les prestataires et sous-traitants ;**

- **techniques: politique de sécurité de l'établissement pour chacune de ses activités mettant en jeu des systèmes d'information (sécurité à la fois physique et logique). Le recours au guide d'élaboration d'une " politique de sécurité Internet " du Forum des compétences, présenté ci-après en annexe, est recommandé.**

Ce document doit être actualisé. Certaines informations peuvent cependant figurer dans des rapports dont l'objet dépasse le strict cadre d'Internet (politique générale de maîtrise des risques de l'établissement par exemple).

L'organe délibérant de l'établissement doit disposer, sur une base au moins annuelle, de documents de suivi précis lui permettant d'apprécier la rentabilité des activités de

l'établissement sur Internet, tant à l'occasion du lancement de l'activité qu'au moment de son extension à d'autres services ou clientèles.

Lorsque la dimension de l'activité Internet ne justifie pas un examen détaillé par l'organe délibérant de l'établissement, ces documents sont à tout le moins validés par les instances appropriées (par exemple un comité de pilotage), bénéficiant d'une délégation claire de l'organe exécutif.

8.1.2. Rôle du responsable du contrôle interne

Il devrait avoir un droit de regard et une responsabilité clairement établis sur l'activité Internet, en particulier lorsqu'elle est en tout ou partie externalisée. Ce domaine fait partie intégrante de son programme de contrôle, y compris quand ces fonctions sont externalisées. Il intègre dans son rapport annuel une information sur la sécurité de l'activité.

Lorsqu'il ne peut procéder lui-même aux contrôles correspondants, il devrait s'entourer de compétences techniques. Cette compétence est à l'évidence acquise au niveau du responsable de la sécurité des systèmes d'information, mais il convient alors de prendre garde au principe de séparation des tâches, qui veut que les acteurs du contrôle ne soient juges et parties.

8.1.3. Coordination des projets Internet au sein de l'établissement ou du groupe

La multiplicité des projets au sein d'un même établissement, ou *a fortiori* d'un groupe, peut justifier qu'un responsable unique de la coordination soit nommé, rattaché à un niveau de décision suffisamment élevé, et toujours du côté " utilisateurs " de l'établissement. Il est utile que sa mission inclue, au delà de la coordination du pilotage des différents projets, la garantie que les exigences de l'établissement en matière de contrôle interne sont bien prises en compte par chaque projet. Son ordre de mission peut utilement formaliser, en ce sens, les relations avec le responsable du contrôle interne.

8.2. La sécurité juridique

8.2.1. Connaissance du cadre juridique de l'activité

11. Bonnes pratiques en matière de maîtrise du risque juridique

Des recommandations générales relatives à la sécurité juridique sont exposées ci-dessous. En particulier, préalablement à tout exercice de son activité dans un nouveau pays ou avec des clients couverts par le droit de ce pays, l'établissement procède ou fait procéder à une étude sur le cadre juridique des activités en ligne. Cette étude sert de base à la rédaction des conventions avec les clients, ainsi qu'à la rédaction des procédures relatives aux contrôles à l'ouverture de relations. L'établissement veille à la sécurité juridique de toutes les opérations engagées avec ou pour le compte de son client. Il s'assure en particulier du caractère certain de son consentement à toute opération.

Préalablement à tout exercice de son activité dans un nouveau pays ou avec des clients couverts par le droit de ce pays, l'établissement procède ou fait procéder à une étude juridique couvrant en particulier les questions suivantes :

- le droit applicable aux services offerts et opérations effectuées sur le site ;

- pour chaque produit, les règles relatives à l'exercice de l'activité envisagée (notamment l'obtention d'un agrément). Lorsque le droit local prévoit des restrictions d'accès de certaines catégories de clients au produit en cause, l'étude doit indiquer les mesures qui doivent être prises pour éviter d'entrer en relation avec eux sur ce produit (par exemple *disclaimer* ou encore blocage d'accès) ;

- les règles relatives à la capacité des personnes à effectuer des opérations bancaires et financières (condition de majorité ou de capacité juridique, les conditions d'accès au type de service proposé,…) ;

- les conditions de forme de la prestation de services envisagée, notamment les conditions déclaratives ou les obligations de vérification (consultation de fichiers d'incidents par exemple) à l'ouverture d'un compte ;

- les régimes spécifiques de protection des clients (droit de la consommation, règles applicables à l'information des investisseurs,…), et notamment les règles d'ordre public qui s'imposent aux parties ;

- le régime fiscal ;

- les règles d'ordre public applicables à la preuve.

Cette étude sert de base à la rédaction des conventions avec les clients, ainsi qu'à la rédaction des procédures relatives aux contrôles à l'ouverture de relations. Elle tient compte

de la nature du site envisagé, en distinguant selon qu'il s'agit d'un site de simple information, de proposition commerciale (concrétisée par un autre canal) ou d'un site transactionnel.

Lorsqu'il sollicite spécifiquement la clientèle non résidente d'un État déterminé, l'établissement veille à ce que les informations requises, le cas échéant, par le droit local de cet État soient fournies sur son site Internet et les autres supports utilisés.

A contrario, l'établissement détermine les pays pour les résidents desquels, compte tenu de l'incertitude sur le droit applicable, les risques juridiques d'ouverture de compte apparaissent non maîtrisables. Il met en place sur son site les éléments permettant de maîtriser son risque (*disclaimer* par exemple). Il indique clairement les pays dont les résidents ne peuvent ouvrir de compte chez lui et informe les personnes consultant le site du droit applicable et des juridictions compétentes.

8.2.2. Les prestataires de services de certification (PSC)

La politique de certification est l'ensemble des procédures et règles de sécurité appliquées par **une autorité de certification** (ou exigées de ses prestataires) pour une catégorie donnée de certificats.

En effet, on peut avoir des politiques différentes pour des certificats destinés à des transactions de nature différente : les exigences sécuritaires au niveau de la fabrication et la délivrance des certificats seront renforcées pour des échanges d'informations sensibles (par exemple en matière de défense) ou des transactions de gros montant.

Les métiers de la certification se segmentent autour de trois grandes composantes :

- **l'autorité d'enregistrement** : elle effectue la vérification d'un certain nombre d'informations concernant la personne demandant l'octroi d'un **certificat** de clé publique, notamment son identité, et adresse un message normalisé à l'opérateur de certification «encapsulant» ces informations ;

- **l'opérateur de certification** : il fabrique le **certificat** de clé publique à partir du message envoyé par l'autorité d'enregistrement, le signe, en assure la publication, gère sa révocation éventuelle ;

- **l'autorité de certification** : c'est le donneur d'ordre des prestataires précédents, qui assume la responsabilité finale vis-à-vis des tiers ; il définit la politique de certification, gère éventuellement la marque associée à son activité, les problèmes d'interopérabilité, conserve la clé secrète servant à signer les certificats, etc.

Suivant les cas, certains des trois métiers peuvent être exercés par la même entité. Les politiques de certification comprennent notamment les exigences visant les autorités d'enregistrement quant à la documentation exigible du demandeur de **certificat**. Il y a autant de politiques de certification que de catégories de certificats gérés par des autorités de certification. Il est impossible de dégager a priori des exigences qui seraient communément

admises, par exemple pour l'identification des demandeurs de certificats. Toutefois, des exigences ou recommandations commencent à apparaître :

- **Les exigences gouvernementales**

Dans la politique de certification PC2 édictée par la Commission Interministérielle pour la Sécurité des Systèmes d'Information pour les besoins de l'administration française, on trouve pour les politiques dites « niveau moyen et élevé » des spécifications précises pour l'identification des personnes physiques et morales. Par exemple, pour une société anonyme, il faut les informations suivantes : nom, raison sociale, adresse du siège social et numéro de téléphone, numéro SIRET, extrait du registre du Commerce où la société est enregistrée, composition et répartition du capital de la société.

Pour une personne physique, le nom, la fonction, l'adresse, le numéro de téléphone, une fiche individuelle d'état civil et une pièce d'identité avec photo sont les éléments nécessaires. En outre, le demandeur doit se présenter en personne auprès de l'autorité d'enregistrement.

- **Les recommandations du CENB**

Dans le Technical Report 402, le Comité Européen de Normalisation Bancaire fait un certain nombre de recommandations aux banques qui souhaiteraient évaluer les pratiques d'autorités de certification dont elles envisageraient de reconnaître les certificats pour leurs propres besoins.

Le rapport précise que, pour des applications à faible risque, le demandeur n'a pas nécessairement à se présenter en personne à l'enregistrement, (ce qui montre bien que les préoccupations de blanchiment étaient étrangères à la rédaction du rapport, voir point 8.4.).

Pour les personnes physiques, la production d'un document d'identité valide du type passeport ou permis de conduire est recommandée ; les informations conservées par l'autorité doivent contenir le nom complet, l'adresse, la nationalité, et un numéro d'identification national lorsque c'est possible. Pour les entreprises individuelles, on ajoute à ces informations le numéro identifiant l'entreprise, son nom et son adresse. Pour les autres personnes morales, qui sont enregistrées par les Chambres de Commerce, l'information enregistrée doit contenir le nom de cette personne, son numéro identifiant, le numéro d'enregistrement, l'adresse postale, et le nom des dirigeants et membres du Conseil d'administration. Un extrait du registre de la Chambre de Commerce doit être fourni.

L'examen des exemples précédents montre que les banques pourraient exiger des autorités de certification des modalités particulières d'identification des demandeurs de certificats avant d'accepter dans le cadre de leurs applications en ligne les certificats émis.

- **Les bonnes pratiques**

S'il est, en tout état de cause, trop tôt pour apprécier et mesurer les risques que présente l'utilisation des certificats comme moyen d'identification des clients en matière bancaire et

financière, sont définies ci-après un certain nombre de bonnes pratiques concernant la délivrance des certificats. Il est rappelé qu'en tout état de cause les établissements restent responsables de la vérification de l'identité des clients et s'exposent aux sanctions disciplinaires de la Commission bancaire s'ils ne respectent pas les obligations à leur charge en la matière (voir le point 8.4.1.4.).

12. Bonnes pratiques concernant la délivrance des certificats

Ces bonnes pratiques seraient les suivantes :

- **la certification " bancaire " devrait faire l'objet d'un standard européen ;**
- **le PSC est accrédité ;**
- **un cadre contractuel clair devrait être établi entre le PSC et l'établissement. Ce dernier doit pouvoir contrôler les activités de son prestataire de services de certification ;**
- **les pièces justificatives de l'identité du client doivent être envoyées systématiquement par le PSC à l'établissement, qui en assure la conservation, afin de contribuer à la vérification de l'identité du client.**

8.2.3. Preuve et contrôle

Dans le cadre des règles applicables, tant sur la sécurité de l'information qu'en matière de piste d'audit, l'établissement devrait s'assurer que les éléments de preuve vis-à-vis des tiers sont conservés de manière sécurisée (disponibilité, **confidentialité** et caractère non réfutable) et accessibles sans délai (notamment en cas de conservation par un tiers).

L'étude juridique précitée indiquera notamment sous quelles conditions ces éléments de preuve peuvent être conservés de manière dématérialisée.

Il est recommandé aux établissements de crédit et aux prestataires de services d'investissement de faire un inventaire des actes juridiques transmis par voie électronique par l'établissement ou par ses clients. Dans le cadre de cet inventaire, il convient de distinguer les transactions soumises à un formalisme écrit *ad validitatem*, de celles qui ne le sont pas.

En effet, en l'état actuel des textes, lorsque l'écrit-papier est une condition de la validité même de l'acte, la conclusion d'une transaction exclusivement par voie électronique est exclue.

Dès lors, ce n'est que lorsque l'écrit est requis *ad probationem* que la question de l'utilisation d'un procédé fiable de signature électronique peut se poser (signature simple, signature avancée …). Dans ce cas, la fiabilité de la signature intéresse la sécurité de la transaction. Les établissements sont invités à évaluer les risques qu'ils prennent en n'assurant pas cette sécurité notamment s'agissant des transactions jugées sensibles.

13. Le recours à des prestataires de services de certification (PSC) accrédités

Dans ce cadre, il convient manifestement de privilégier le recours à des PSC accrédités. La directive " signature électronique " prévoit en effet que les États membres peuvent instaurer des régimes volontaires d'accréditation des PSC, visant à améliorer le niveau de service offert (voir point 3.2. sur le droit de la preuve).

On peut s'attendre à ce que les conditions fixées par le décret " signature électronique " et les normes en cours d'élaboration visant les dispositifs de création de signature, les PSC et les certificats deviennent une référence, qui serait utilisée par le juge et/ou les experts en cas de litige. S'il convient de suivre attentivement l'évolution de la jurisprudence dans ce domaine, il est prudent de s'appuyer sur des prestataires de services de certification accrédités.

Il est rappelé que les relations contractuelles avec des PSC externes à l'établissement de crédit ou au prestataire de services d'investissement doivent faire l'objet d'une convention -comme pour tout autre prestataire externe- précisant notamment les modalités de contrôle du PSC par l'établissement de crédit ou le prestataire de services d'investissement.

8.2.4. Sécurité juridique en cas de mise en relation

Dans le cas de " **portails** " reliés aux sites d'autres prestataires bancaires ou financiers, la responsabilité du prestataire en cas de problème sur les services proposés devrait être étudiée et maîtrisée.

L'établissement signe une convention avec chaque établissement pour lequel il propose un lien sur son site. Cette convention décrit en détail le partage des responsabilités quant aux clients qui entreraient par cette voie en contact avec l'établissement lié. Les deux établissements veillent à informer clairement les personnes qui accèdent au site de ce partage de responsabilités, notamment en établissant clairement que le client qui active le lien va être mis en relation avec un autre établissement.

8.3. La maîtrise du système d'information et la sécurité des transactions

8.3.1. Vérification au moment de l'agrément de la maîtrise du site web

8.3.1.1. La maîtrise de la prestation externe

Les motivations traditionnelles de la prestation externe de certains services dans un établissement bancaire sont liées au recentrage sur les métiers de base, à la réduction des coûts ou encore à la recherche d'expertises pointues.

Aujourd'hui, l'apparition de nouveaux canaux de distribution de produits bancaires ou financiers en ligne semble encourager le recours à la prestation externe. En effet, ces

nouveaux canaux de distribution requièrent un positionnement rapide ainsi qu'un niveau technologique et une réactivité maximale.

La prestation externe est susceptible de toucher la conception et la distribution d'une large gamme de produits bancaires alors que traditionnellement seules les opérations de traitement semblaient être concernées.

Les incitations à l'externalisation de certains services proposés par Internet sont diverses. Elles tiennent à la recherche de l'expertise technologique, à la nécessaire rapidité de positionnement sur un marché, à la maîtrise des coûts ou encore à l'inadéquation des services de traitement des opérations conçus à l'origine pour d'autres fonctionnalités moins exigeantes (traitement *« batch »* plutôt que temps réel).

Les services bancaires ou financiers sur Internet sont variés et couvrent :

- la simple information sur l'ensemble des produits proposés par la banque, auquel cas il n'existe pas nécessairement de lien entre les données de la banque et le serveur ;

- la communication entre la banque et le client, lui permettant la consultation de comptes, la réalisation d'opérations classiques, auquel cas il existe un lien avec la base de données de la banque ;

- le site transactionnel, nécessitant un lien avec les données clientèle mais également avec des données de marché sous forme d'historique, de recherche, voire d'aide à la décision.

Ces services font l'objet de différents schémas d'organisation. Le même établissement peut assurer l'ensemble des services requis, en ayant recours, le cas échéant, à un mandataire pour en assurer la réalisation technique. Il peut également travailler avec d'autres prestataires de services avec lesquels il demande à ses clients de conclure des contrats spécifiques. Enfin, une société peut ne pas être un prestataire habilité si elle agit comme mandataire exclusif d'un prestataire. Ce dernier schéma a été utilisé lors du lancement de nouvelles sociétés de courtage en ligne avant qu'elles ne sollicitent un agrément.

Ainsi, selon le positionnement choisi par l'établissement, les conséquences d'une externalisation sur la sécurité des systèmes d'information ne seront pas identiques.

Acheter un service clé en main auprès d'un prestataire externe permet à tout le moins de proposer un service à la clientèle en se positionnant immédiatement sur un secteur fortement concurrentiel. En effet, l'un des premiers facteurs de réussite d'un site bancaire ou financier virtuel est la qualité du service en termes de disponibilité et de rapidité d'accès et d'exécution des ordres.

En conséquence, l'établissement doit être capable de gérer en temps réel et non plus en différé des volumes importants de transactions. Or, certains systèmes n'ont pas été conçus pour le traitement en temps réel des informations ni pour des volumes de transactions importants.

Le choix du prestataire externe devrait donc s'effectuer sur la base de critères tels que :

- l'assise financière et le risque de défaillance : ce risque est-il examiné et évalué périodiquement ?

- les moyens de contrôle du prestataire (exigence, notamment, d'une clause d'audit) ;

- son expérience ;

- la clarté des responsabilités juridiques des conventions liant le prestataire externe et l'établissement, en continuité d'exploitation mais aussi en cas de liquidation du prestataire ;

- la possibilité de se désengager de ces accords, sous quel délai et à quels coûts ?

- les plans de continuité des services offerts par le prestataire externe ;

- le degré de transparence du prestataire permettant à l'établissement contractant d'évaluer périodiquement les systèmes de contrôles internes propres au prestataire externe ;

- le degré de sécurité offert par le prestataire externe en termes de respect du secret professionnel.

En parallèle l'établissement devrait se poser les questions suivantes :

- sur quel type de site l'établissement souhaite-t-il se positionner ? De quelle technologie a-t-il besoin ? L'externalisation répond-elle à ce besoin ? Est-elle compatible avec l'architecture actuelle de son système d'information ?

- cette architecture est-elle suffisamment souple ou modulaire pour en changer ?

- le degré de compétence technique du management est-il suffisant pour apprécier les conséquences de l'externalisation ?

- les besoins de la clientèle font-ils l'objet d'une bonne compréhension de la part du prestataire externe, permettant qu'il n'y ait pas d'augmentation du risque de perte de clientèle ou simplement de risques transactionnels, voire de réputation (chiffrage du pourcentage de clientèle et de produit net bancaire susceptible d'être concerné) ?

- comment l'établissement va-t-il mesurer son degré de dépendance vis-à-vis du prestataire externe et l'implication du management est-elle suffisante pour permettre de réexaminer périodiquement la question de savoir si la solution de la prestation externe est toujours adaptée aux besoins de l'établissement et si le choix du prestataire est pertinent : le choix de la prestation externe doit pouvoir être remis en cause globalement ou partiellement ;

- peut-il y avoir des risques de " débordement " du prestataire pouvant générer des risques de perte de contrôle opérationnel ?

- de quelle autonomie dispose le prestataire ?

- sur quels domaines ?

- ces domaines pourraient-ils être des domaines réglementés ?

- le prestataire dispose-t-il du dispositif de contrôle que l'établissement aurait lui-même exigé si le développement de ces prestations avait été réalisé en interne et de quels moyens l'établissement dispose-t-il pour les imposer ?

- les moyens de diffusion de l'information ou de la formation par le prestataire dans l'établissement sont-ils jugés suffisants pour ne pas accroître le degré de dépendance de l'établissement vis-à-vis du prestataire ?

- la dimension coût étant l'une des sources de profitabilité et l'un des éléments sur lequel l'établissement est susceptible de réagir pour s'adapter à la concurrence, l'établissement devrait s'assurer qu'il dispose en permanence de l'ensemble des informations lui permettant d'apprécier les différentes composantes du coût de son investissement ;

- si des processus d'externalisation ont lieu auprès de différents prestataires, la direction dispose-t-elle d'une vision globale des risques encourus ?

- dans le cas où le prestataire fournirait des services à plusieurs clients simultanément, ce prestataire a-t-il adapté le niveau de sécurité de ses systèmes de telle manière qu'un incident touchant un client ne se répercute pas sur les autres ?

En ce qui concerne les autorités d'agrément, la problématique de l'externalisation peut se résumer de la manière suivante :

14. La maîtrise de la prestation externe (au moment de l'agrément)

L'externalisation entraîne un risque de séparation des responsabilités juridiques (restant à l'établissement) et opérationnelles (chez le prestataire externe). Les autorités d'agrément devraient donc faire en sorte que ce risque soit minimal, en demandant aux établissements d'exercer un contrôle suffisant sur les activités de leurs prestataires externes.

Par ailleurs, dans le cas où un prestataire fournit des services à plusieurs établissements, les autorités sont amenées à veiller à ce que la concentration des risques opérationnels chez ce prestataire n'induise pas un risque systémique trop important.

8.3.1.2. Des exigences sécuritaires plus poussées en matière d'agrément

Les dispositions qui suivent concernent les nouveaux entrants sur le marché. S'agissant des entreprises d'investissement ou des établissements de crédit déjà agréés, il est prévu au point 2.2.1. d'établir une procédure de déclaration auprès de l'autorité d'agrément. À l'occasion

de cette déclaration, le CECEI examinerait pour les établissements déjà constitués si l'ouverture du site reste compatible avec les éléments de bon fonctionnement de l'établissement appréciés lors de son agrément.

8.3.1.2.1. La démarche "questionnaire"

En partant du constat que les services bancaires ou financiers sur Internet sont assez typés : gestion de compte, virements, ordres de bourse, un questionnaire type a été élaboré, portant à la fois sur les aspects techniques et organisationnels de la sécurité. L'objectif n'est pas d'obtenir une étude exhaustive de la sécurité ou de valider les choix techniques détaillés, mais de s'assurer que le porteur de projet a pris en compte avec suffisamment de diligence les aspects sécuritaires.

15. Questionnaire « sécurité » au moment de l'agrément

- Description de l'architecture globale du système d'information (incluant l'établissement et ses partenaires externes), avec schéma des flux d'informations et des traitements associés.

- Pour chaque entité de ce système d'information ainsi que chaque liaison entre entités, quels sont les moyens techniques et organisationnels envisagés afin de prévenir, détecter ou corriger des problèmes sécuritaires ? («firewalls», détecteurs d'intrusions, outils de détection automatique de failles…).

- Description des moyens de veille technologique concernant les défauts sécuritaires des matériels / logiciels utilisés.

- Qui est chargé de l'installation, de la configuration, de l'évaluation, de la maintenance des équipements ou logiciels de sécurité ? (notamment des firewalls).

- Modalités du dépouillement et de l'exploitation des pistes d'audit.

- Description des moyens de secours envisagés (redondance, back-up…).

- En cas de défaillance, en combien de temps les moyens de secours peuvent-ils être opérationnels?

- Description des méthodes de protection des communications (au regard de l'authentification, l'intégrité, la confidentialité, la non-répudiation).

- Quels sont les outils utilisés ? (logiciels, tokens, cartes à puce, …).

- Description des procédures de login (mots de passe, échanges de clés, jetons de sessions, …) et des mesures de sécurité associées.

- Comment s'assure-t-on de la disponibilité des systèmes ? moyens de supervision ? quelle est la capacité en nombre de connexions simultanées / nombre d'ordres par heure ?

- Description des moyens humains (nombre, qualification, répartition des fonctions) affectés à la sécurité et à la surveillance des risques ?

- Sécurité des e-mails ? (vis-à-vis en particulier du risque d'intrusion et des aspects authentification / intégrité / confidentialité).

- Moyens de sécurité physique ? (des locaux, du matériel, …).

- Moyens techniques ou organisationnels mis en place pour prévenir le risque d'attaque ou de complicité interne à l'entreprise ?

- Liste des interventions passées ou prévues de cabinets de conseil externes à l'entreprise concernant le système d'information (audits, «hackers» professionnels, conseil pour la mise en œuvre de systèmes, …).

- Liste des prestataires externes "opérationnels" (exemple : teneur de compte, conservateur) et description de leur expérience dans le domaine ; quelles sont les relations contractuelles, le partage des responsabilités ? quels moyens / procédures de contrôle l'entreprise a-t-elle mis en place vis-à-vis des prestataires externes.

- L'entreprise a-t-elle souscrit une police d'assurance concernant les risques opérationnels ? si oui, description des garanties.

8.3.1.2.2. La démarche d'expression des objectifs de sécurité

La démarche exposée au point précédent, actuellement mise en oeuvre, pourrait, après un retour d'expérience suffisant, être remplacée par une démarche plus systématique consistant à demander que le dossier d'agrément contienne les éléments suivants :

(a) **expression des besoins de sécurité** : à partir de la stratégie de l'entreprise et des textes réglementaires s'appliquant à elle, de la description de son environnement, etc ;

(b) **liste des menaces** : constituée à partir de la liste des biens à protéger, elle devrait être pondérée par l'appréciation de la probabilité de la réalisation de chaque menace et par l'évaluation de ses conséquences ;

(c) **liste des objectifs de sécurité**, visant à prévenir, détecter et éventuellement contenir la réalisation des menaces identifiées ;

(d) **et par ailleurs** : description de l'organisation de l'établissement en matière de sécurité du système d'information : moyens, rattachement hiérarchique du responsable, liens avec le contrôleur interne.

Lorsque l'architecture technique du système d'information de la société est déjà déterminée, il s'agirait de demander à celle-ci de décrire les mesures sécuritaires permettant

de mettre en œuvre au niveau des composantes de son système d'information les objectifs de sécurité et de se livrer à une analyse des risques résiduels.

8.3.1.2.3. Impact d'une "certification" sécuritaire sur les démarches précédentes

Les établissements pourraient faire certifier leurs sites web sur le plan sécuritaire selon un **profil de protection** (voir à ce sujet le point 8.3.4). Une telle certification pourrait être prise en compte dans les démarches exposées aux points précédents en faisant alors bénéficier l'établissement concerné d'une présomption de conformité pour la partie "site web" de son système d'information.

8.3.2. La maîtrise du système d'information

8.3.2.1. L'article 14 du règlement n° 97-02 du Comité de la réglementation bancaire et financière

Le Livre blanc sur la sécurité des systèmes d'information de la Commission bancaire de 1996 avait anticipé, en les détaillant sous la forme de bonnes conduites, les modalités d'application de l'article 14 du règlement n° 97-02 du Comité de la réglementation bancaire et financière. Les grands principes de ce Livre blanc restent toujours d'actualité.

Article 14

Les établissements de crédit déterminent le niveau de sécurité informatique jugé souhaitable par rapport aux exigences de leurs métiers. Ils veillent au niveau de sécurité retenu et à ce que leurs systèmes d'information soient adaptés. Le contrôle des systèmes d'information doit notamment permettre :

a) de s'assurer que le niveau de sécurité des systèmes informatiques est périodiquement apprécié et que, le cas échéant, les actions correctrices soient entreprises ;

b) de s'assurer que les procédures de secours informatique sont disponibles afin d'assurer la continuité de l'exploitation en cas de difficultés graves dans le fonctionnement des systèmes informatiques.

Le contrôle des systèmes d'information s'étend à la conservation des informations et à la documentation relative aux analyses, à la programmation et à l'exécution des traitements.

Plus peut-être que pour toute activité bancaire et financière de base, la sécurité est un impératif lorsque celle-ci est liée à un service en ligne. En effet, au-delà des conséquences financières directes d'un incident technique (panne, dysfonctionnement ou fraude), l'atteinte à l'image de l'établissement pourrait, compte tenu de la " volatilité " probable de la clientèle, mettre en cause l'existence même de certains acteurs du marché.

16. La maîtrise du système d'information, que ce dernier soit externalisé en tout ou partie ou interne à l'établissement

Sur le fondement de l'article 14 du règlement n° 97-02 relatif au contrôle interne des établissements de crédit sont exposées ci-après des recommandations relatives à la maîtrise des systèmes d'information. En particulier, l'établissement devrait démontrer qu'il maîtrise tous les aspects du système d'information utilisé, y compris lorsque celui-ci est confié à un prestataire extérieur, que ce soit pour le développement comme pour l'exploitation technique. L'établissement devrait avoir accès à toute l'information sur les spécifications fonctionnelles et techniques du système, et déterminer librement le paramétrage. Il devrait vérifier que le système, qu'il soit interne ou externe, répond en permanence à ses exigences, à la fois de performance et de sécurité (disponibilité, intégrité, confidentialité, audit et preuve). Le libre accès des autorités de tutelle ou instances de contrôle aux installations externes devrait être garanti par une clause contractuelle. Les relations avec les prestataires externes devraient être formalisées dans des conventions claires et précises, en application de ces principes.

Les établissements doivent en particulier disposer de garanties quant aux performances et aux possibilités de redimensionnement du système. Ils doivent également s'être assurés que les mesures de protection contre les risques qu'ils ont définies sont effectivement appliquées dans le système.

L'expérience a montré que les établissements peuvent externaliser de façon systématique leur activité sans pour autant disposer de moyens de contrôle satisfaisants. L'Internet a renforcé ce processus.

La rédaction actuelle de l'article 14 du règlement n° 97-02 relatif au contrôle interne vise la maîtrise de l'ensemble du système d'information de l'établissement qu'il soit externalisé ou non : " *Les établissements de crédit déterminent le niveau de sécurité informatique jugé souhaitable par rapport aux exigences de leurs métiers. Ils veillent au niveau de sécurité retenu et à ce que leurs systèmes d'information soient adaptés* ".

Pour plus de clarté, l'alinéa 1er de l'article 14 du règlement n° 97-02 pourrait préciser ce point. Modifié, il disposerait que :

" Les établissements de crédit déterminent le niveau de sécurité informatique jugé souhaitable par rapport aux exigences de leurs métiers. Ils veillent au niveau de sécurité retenu et à ce que leurs systèmes d'information soient adaptés, que ces derniers soient externalisés en tout ou partie, ou internes à l'établissement ".

8.3.2.2. Règles générales

La politique de sécurité de l'établissement (voir le point 8.1.1 relatif au rôle des organes exécutif et délibérant), pour son volet technique, devrait être détaillée dans des documents

décrivant la manière dont ses principes sont mis en application dans le système d'information. Le " Guide politique de sécurité Internet " du Forum des compétences, en annexe, présente une trame pour l'élaboration d'une telle politique.

Les dirigeants ou à défaut leurs représentants pour le domaine technique, devraient connaître les fonctionnalités des systèmes d'information utilisés par l'établissement. Ils démontrent que l'organisation mise en place en interne a permis la validation par les utilisateurs des spécifications détaillées de ces systèmes (notamment du point de vue de la gestion des risques et de la sécurité) à un niveau adéquat.

L'établissement est en mesure de vérifier la validité permanente des paramètres, calculs et algorithmes utilisés par le dispositif pour filtrer les opérations de sa clientèle ainsi que leur conformité aux règles de gestion inscrites dans les procédures internes. En particulier, il apparaît nécessaire qu'il dispose, non seulement de la documentation technique, opératoire, fonctionnelle et de maintenance, relative au logiciel, mais également qu'il ait, parmi son personnel, un nombre suffisant d'agents ayant la compétence nécessaire pour qu'à tout moment de la plage d'exploitation, l'un d'eux ait la maîtrise des données et du paramétrage externe. En cas de défaillance de l'éditeur du logiciel, l'établissement doit avoir pris les mesures pour s'assurer de la maîtrise des sources. D'une manière générale, le recours à une société de développement externe, l'achat d'un progiciel, voire l'externalisation des prestations ne doit pas faire obstacle à la maîtrise par l'établissement du produit qu'il met en œuvre et dont il assume la responsabilité, tant vis-à-vis de ses clients que des autorités de tutelle et de contrôle. Il importe, en particulier, que les conventions d'achat ou de mise à disposition du logiciel prévoient, pour l'établissement, la possibilité d'accéder aux données techniques nécessaires à cette maîtrise.

Le responsable du contrôle interne doit disposer de moyens lui permettant de vérifier le respect de la politique de sécurité, en particulier pour le contrôle des prestataires extérieurs. Il est destinataire des informations adéquates sur les performances du système au regard du développement de l'activité ainsi que de rapports sur les incidents techniques, selon les orientations prescrites par la politique de sécurité Internet. Il synthétise ces observations, à l'intention de la direction générale, en particulier à l'occasion du rapport annuel sur le contrôle interne.

8.3.2.3. Les relations avec les prestataires de services et sous-traitants

Avant de commencer ses activités, l'établissement devrait signer une convention avec chacun de ses prestataires et sous-traitants.

Cette convention prévoit les engagements techniques de chaque prestataire. Elle indique notamment le niveau de qualité de service sur lequel il s'engage (défini de manière précise et mesurable) et les cas de force majeure où cet engagement est réduit ou suspendu. En cas de panne, la convention prévoit le délai maximum garanti d'indisponibilité du service ou, dans les cas où une telle garantie est exclue, les moyens que le prestataire s'engage à mettre en œuvre pour résoudre la difficulté.

Dans le cas d'un prestataire chargé du développement d'applications ou d'outils système, la convention prévoit, dans la mesure du possible :

- l'accès sans restriction de l'établissement à toute information utile à la maîtrise du système, de nature technique ou fonctionnelle sur les produits ou services mis à sa disposition. L'établissement doit en particulier avoir accès à l'intégralité de la documentation technique et fonctionnelle des applications, objet du contrat ;

- le plafond de capacité de l'application ou de l'outil système, notamment en volumes de charge ;

- les délais nécessaires pour l'extension de cette capacité, et la limite ultime à laquelle celle-ci est soumise ;

- les garanties financières à l'appui de ces engagements ;

- un délai de préavis pour le retrait du prestataire du support de son produit.

La convention prévoit par ailleurs les moyens de contrôle mis par le prestataire à la disposition de l'établissement pour garantir la mise en œuvre de ses engagements, et la mise à disposition sans restriction de toutes les informations qui pourraient être demandées par les autorités de contrôle, ainsi que la possibilité pour celles-ci de procéder à toute vérification jugée utile dans les locaux du prestataire.

Enfin, la convention doit déterminer sans ambiguïté les droits sur tout élément logiciel utilisé par l'établissement, en particulier la faculté ou non de les commercialiser auprès d'autres établissements.

8.3.2.4. La disponibilité

L'établissement devrait s'assurer que les dispositifs de secours sont en place pour garantir le niveau de disponibilité défini dans sa politique de sécurité (en termes de limites d'indisponibilité et de délai maximum de remise en production après une panne). Ces dispositifs sont régulièrement testés.

En outre, l'établissement dispose de procédures lui permettant de faire face aux situations d'indisponibilité du service en cas de force majeure. Ces procédures reposent sur des moyens soit internes, soit externes, auxquels il peut être fait appel en cas de besoin dans des conditions de délai et de niveau de services prédéfinis.

L'établissement s'assure de la disponibilité en toutes circonstances d'une copie de toute donnée qui peut être requise par un client, par une entreprise de marché ou par les autorités de place. Il met en place les sauvegardes nécessaires.

8.3.2.5. L'intégrité et la confidentialité de l'information

L'établissement devrait s'assurer que la protection de l'intégrité et de la **confidentialité** sont conformes tant aux principes de sa politique de sécurité qu'aux engagements pris vis-à-vis des tiers. Ce contrôle porte à la fois sur les flux d'informations et sur les données conservées.

Il veille en particulier à assurer la sécurité des moyens d'authentification (mots de passe) transmis aux clients ou utilisés par eux.

L'établissement vérifie que la sécurité est suffisante quelles que soient les conditions de conservation des données, à des fins de secours ou d'archivage, en particulier lorsqu'elles sont externalisées. L'établissement veille à obtenir de ses prestataires les engagements nécessaires ainsi que l'autorisation de mener sur ce point toutes les vérifications utiles.

8.3.2.6. Les performances du système d'information

L'établissement devrait démontrer que son système respecte à tout moment (sauf cas de force majeure prévue dans les conventions) les engagements de performance pris à l'égard des clients. Il démontre que le système de suivi des risques et des engagements, qu'il soit manuel ou automatisé, fonctionne en toutes circonstances, même en pointe de charge.

La rapidité du sous-système de vérification de provision du client est critique (en particulier pour des activités de courtage boursier en ligne). Une durée trop longue de contrôle ne doit pas conduire les clients à faire pression pour en obtenir le débrayage.

L'établissement s'assure que les possibilités, notamment en délais, de redimensionnement des systèmes en cas de croissance imprévue des volumes à traiter sont cohérentes avec les engagements de qualité de service pris à l'égard des clients.

8.3.2.7. Preuve/contrôle et piste d'audit

L'établissement devrait s'assurer qu'une trace de tout événement sensible est conservée, sur un support qui garantit sa confidentialité, et surtout son intégrité et son exploitabilité, notamment par les contrôleurs. La liste des évènements sensibles est établie dans la politique de sécurité. Elle comprend, notamment, en fonction de la nature de l'activité :

- toute création, modification ou suppression de client ;
- toute opération financière ou ayant des conséquences financières ;
- toute acceptation de franchissement de limite par un client ;
- toute création, modification ou suppression de privilèges ou droits d'accès au système ;
- toute intervention sur le dispositif de filtrage des opérations des clients, notamment en vue de le débrayer.

Les règles de sécurité prévoient également les mesures d'information sur ces évènements (modalités de communication, données rapportées, périodicité) des dirigeants (ou des personnes qu'ils ont désignées à cette fin) et du responsable du contrôle interne.

L'établissement conserve également le maximum d'éléments sur les transactions effectuées en ligne (en particulier, les ordres reçus des clients). Ces informations doivent être mentionnées dans la convention signée avec eux au regard du respect des dispositions de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Il conserve notamment les éléments permettant d'identifier le cheminement suivi par l'ordre pour lui parvenir. En outre, il assure au client un droit d'accès et de modification des données le concernant.

8.3.2.8. Les rapports sur le contrôle interne et sur la mesure et la surveillance des risques

L'importance des aspects relatifs à la sécurité de l'information justifie que ces questions soient traitées en détail dans les rapports annuels sur le contrôle interne, notamment pour tenir compte des adaptations permanentes des systèmes d'information pour les maintenir au meilleur niveau technologique.

Il s'agit de rappeler ici la teneur de l'article 42 du règlement n° 97-02 relatif au contrôle interne, qui dispose que le rapport annuel sur le contrôle interne comprend notamment :

- *"Une description des modifications significatives réalisées dans le domaine du contrôle interne au cours de la période sous revue, en particulier pour prendre en compte l'évolution de l'activité et des risques ;*

- *une description des conditions d'application des procédures mises en place pour les nouvelles activités".*

Conformément à l'analyse du point 2.2.1. (l'ouverture d'un service par Internet constituerait un élément notable du mode de fourniture des services, modifiant les conditions d'exercice de l'activité bancaire ou financière), les mesures prises au titre du contrôle interne en matière de services bancaires ou financiers en ligne devraient être tout particulièrement détaillées.

En outre, s'agissant du rapport sur la mesure et la surveillance des risques visés à l'article 43 du règlement n° 97-02 relatif au contrôle interne, il est rappelé que les risques liés à la sécurité des systèmes d'information devraient faire l'objet de développements particuliers.

8.3.3. Exemple d'infrastructure de sécurité, utilisant la cryptographie asymétrique

Une infrastructure à clés publiques est composée au minimum d'une autorité de certification, des outils nécessaires aux fonctions d'autorités d'enregistrement et d'un dispositif technique de production de certificats. L'analyse qui suit porte sur les infrastructures à clés publiques, sachant que le champ couvert par la directive " signature électronique " ne se limite pas, en théorie, à cette technologie.

8.3.3.1. Conditions pour pouvoir bénéficier de la présomption de fiabilité

Au point 5.3. ont été mentionnés les besoins de sécurité des transactions bancaires et financières en ligne. Le point 3.2. expose, quant à lui, le droit de la preuve et les notions de signature électronique simple et «avancée».

Rappelons qu'à l'heure actuelle, la plupart des solutions utilisées par les fournisseurs de services bancaires ou financiers en ligne pour leurs relations avec les particuliers (et dans certains cas les professionnels) ne permettent pas de garantir la **non-répudiation**[10] , dans la mesure où les secrets (code confidentiel, clé privée) confiés au client sont stockés ou transitent en clair dans son PC qui constitue un environnement vulnérable aux attaques depuis le réseau (**chevaux de Troie** et **virus**). Il s'agit de noter que dans le domaine du B to C, la solution **Cyber-Comm** utilisant un lecteur sécurisé de carte à puce permet d'assurer la **non-répudiation** des paiements par cartes bancaires sur Internet.

D'après l'article 1316-4 du code civil, précisé par le décret " signature électronique ", il faudra démontrer pour pouvoir bénéficier de la présomption de fiabilité :

- le respect des conditions fixées au dispositif de création de signature utilisé, respect qui sera présumé notamment dans le cas où ce dispositif aura été certifié ;

- le respect des conditions fixées à l'article 6 pour le **certificat** utilisé et le **PSC** qui l'a fourni.

Ces conditions sont difficilement remplies par des dispositifs de création de signature sous environnement PC. En effet, le dispositif devrait garantir que les données utilisées pour la création de la signature, c'est à dire les clés, puissent être protégées de manière fiable par le signataire légitime contre leur utilisation par des tiers. Il reste que la **confidentialité** de données stockées dans un environnement PC n'est guère assurée. De même, alors que le dispositif ne doit pas modifier les données à signer, on ne peut en avoir la certitude dans un environnement PC perméable aux **virus** et chevaux de Troie.

8.3.3.2. Exemple de mise en œuvre d'une infrastructure à clés publiques

Est exposé ci-après un exemple simplifié d'infrastructure établissement/client où l'établissement assure le rôle **d'autorité d'enregistrement** et de **certification** et fait appel à un tiers de confiance externe pour opérer la certification.

La combinatoire autorité de certification/autorité d'enregistrement peut être très variable. Chaque établissement devrait étudier les options les mieux adaptées à ses contraintes (nombre de certificats, coûts, contraintes juridiques…).

On notera que cet exemple offre un haut niveau de sécurité par comparaison avec les pratiques moyennes actuelles (avec notamment une authentification forte au moyen d'une carte à puce), mais ne garantit toutefois pas totalement l'intégrité des données puisque avant d'être signées, celles-ci transitent sur le PC de l'utilisateur qui, comme on l'a vu ci-dessus, ne peut pas être considéré comme totalement sûr.

---

10) Impossibilité pour l'utilisateur ou le prestataire de nier qu'il est l'auteur de la transaction et que celle-ci existe bien.

8.3.3.2.1. Une procédure d'obtention de certificat et de stockage sur carte à puce

1. Un client fait une demande d'obtention de carte à puce afin d'accéder aux services en ligne sécurisés, proposés par l'établissement de crédit ou le prestataire de services d'investissement.
2. L'établissement récupère et vérifie les informations concernant le client. Il joue donc le rôle d'autorité d'enregistrement.
3. Une carte à puce vierge est affectée à un client. A l'initiative de l'établissement, la carte à puce génère une bi-clé et la mémorise.
4. Les informations concernant le client ainsi que la clé publique générée par la carte sont transmises au tiers de confiance pour obtenir un **certificat**.
5. Le tiers de confiance produit le **certificat** et le signe avec une clé privée.
6. Le **certificat** est retourné à l'établissement qui le stocke sur la carte à puce ainsi que dans son annuaire d'entreprise.
7. La carte à puce est personnalisée et est transmise au client.
8. À réception de la carte à puce, le client modifie le code PIN permettant d'accéder à la clé privée stockée sur la carte.
9. Le client demande à l'établissement de valider son accès aux services en ligne souhaités.

8.3.3.2.2. Une procédure d'authentification

1. Le client souhaite accéder à un service en ligne de l'établissement.
2. Le client se connecte (via une liaison sécurisée) sur le site de l'établissement et sollicite une authentification.
3. Le navigateur invite le client à introduire sa carte à puce dans le lecteur de carte et à saisir son code PIN (supposé correct).
4. Le lecteur de carte établit la signature électronique de la demande de connexion.
5. Le navigateur envoie la demande de connexion ainsi que la signature.
6. Le serveur de l'établissement vérifie, d'une part, la signature de la demande de connexion à partir du **certificat** stocké dans l'annuaire d'entreprise et, d'autre part, s'assure que le **certificat** n'est pas révoqué.
7. Si le processus se déroule normalement, le client accède au service de la banque.

8.3.3.2.3. Une procédure de signature électronique

1. Le client valide une transaction dont l'ensemble des éléments est résumé dans une page.
2. Le navigateur invite le client à saisir son code PIN (supposé correct).
3. Le lecteur de carte établit la signature électronique des éléments de la transaction.
4. Le navigateur envoie la transaction accompagnée de la signature.
5. L'établissement contrôle la transaction en vérifiant notamment la signature (supposée correcte).
6. L'établissement envoie au client une page de confirmation incluant tous les éléments de la transaction.

8.3.3.2.4. Une organisation

Seule une analyse de vulnérabilité méthodique pourra mettre en exergue ou confirmer les détails de l'organisation requise pour gérer les technologies envisagées. Cependant, on peut déjà dégager des pôles incontournables.

8.3.3.2.4.1. Gestion des utilisateurs finaux

Miser sur une logistique externe de certificats ne signifie pas que l'établissement ne s'impliquera pas dans ce qu'on appelle " l'enrôlement ". L'attribution d'un **certificat**, doté de propriétés particulières, relève de la volonté de l'établissement. Il en est de même pour la spécification des critères d'attribution, de reconduite, de révocation, de suspension de certificats.

Une mauvaise organisation sera visible de l'extérieur et préjudiciable à la sécurité du système d'information.

Les cas particuliers d'utilisation du système par la clientèle devront être pris en compte : utilisateurs " backups ", départs en congés de longue durée (maternité, maladie, congés sabbatiques) et devront être traités d'une manière suffisamment réactive pour que l'entreprise cliente ne soit pas tentée de dévoyer le système (confier le code PIN de la carte à puce à un tiers, etc).

8.3.3.2.4.2. L'opérateur de confiance

La description du rôle précis de l'opérateur de confiance et de l'établissement de crédit ou le prestataire de services d'investissement ne devra souffrir aucune approximation.

8.3.3.2.4.3. La génération des certificats

La **non-répudiation** sera lourde de conséquences dans ce domaine. L'organisation et les moyens techniques devront faire en sorte que, d'une manière absolument incontestable, l'établissement de crédit ou le prestataire de services d'investissement ne puissent avoir connaissance de la clé privée du client.

8.3.3.2.4.4. La gestion de l'archivage

Il ne faut pas négliger l'importance d'une bonne gestion de l'archivage. Celui-ci pose le problème de la conservation, dans le temps, des modes de preuve et demande une étude approfondie.

8.3.3.2.4.5. La protection de la clé privée

L'utilisation de la carte à puce procure un standard très élevé de sécurité pour protéger physiquement une clé privée.

Dans le cas d'une solution moins sécurisée où la clé privée est conservée sur le disque dur, des moyens de contrôle d'accès doivent être notamment utilisés. En cas de copie des fichiers d'identification numérique et des clés secrètes d'un ordinateur à l'autre, un mot de passe sécurisé doit être utilisé.

8.3.4. La maîtrise du risque de réputation, qui peut se propager à l'ensemble de la communauté bancaire et financière, plaiderait en faveur de la mise en place d'un référentiel de sécurité qui serve de fondement à une certification, voire à une labellisation des sites web financiers

De graves dysfonctionnements rencontrés par un service bancaire en ligne peuvent susciter de la part de la clientèle une perte de confiance et, par propagation, porter préjudice à l'ensemble de la communauté bancaire.

17. La définition au sein du Comité français d'organisation et de normalisation bancaire (CFONB) d'un « profil de protection », référentiel de sécurité de place

Un établissement n'offrant pas de bonnes garanties de sécurité ferait courir un risque d'image pour la place toute entière. La vocation première d'un référentiel de sécurité applicable à ce niveau serait donc de garantir, de façon publique, la conformité du dispositif de sécurité adopté par un établissement, en regard d'un ensemble de critères constituant une " cible de sécurité " communautaire.

La définition d'un tel référentiel de sécurité a motivé la saisine du Comité français d'organisation et de normalisation bancaire (CFONB) par le Secrétariat général de la Commission bancaire, afin que soit élaboré un " profil de protection " (PP) adapté aux risques des sites web financiers transactionnels susceptible de déboucher à terme sur un processus de certification.

Dénommé " **profil de protection** ", ce référentiel de sécurité, de nature fonctionnelle et modulaire, doit conserver un caractère souple et être, dans la mesure du possible, neutre technologiquement. De nombreux profils de protection[11] existent déjà et leur utilisation, en plein développement, est vivement encouragée par la Commission européenne.

Un des points fondamentaux est que la définition d'un référentiel de sécurité devrait s'inscrire dans le cadre des **Critères communs** fixés au plan international, afin de déboucher sur des certifications pouvant faire l'objet de reconnaissance mutuelle entre tous les États signataires. Dans ces pays, une autorité publique (en France la **DCSSI**)[12] est chargée de présider à la certification sur des bases communes.

La certification devrait ainsi avoir pour objet de garantir le niveau de sécurité offert par tout site soumis à l'obligation d'agrément, non seulement aux yeux des autorités de contrôle françaises, mais aussi étrangères en raison de la vocation internationale croissante des services bancaires en ligne. En tant que standard international, les **Critères communs** s'imposeraient alors immédiatement comme une référence obligée pour une recherche de reconnaissance mutuelle entre différents pays du (ou des) futur(s) PP susceptible(s) d'être défini(s).

---

11) À titre d'exemple, il existe des profils de protection pour les sites web institutionnels gouvernementaux, les lecteurs transactionnels avec carte à puce (cyber-Comm), les DAB, les firewalls à exigences élevées et réduites, le porte-monnaie électronique ...

12) La Direction centrale de la sécurité des systèmes d'information est une direction dépendant des services du Premier ministre (Secrétariat général de la défense nationale). 14 pays sont parties aux Critères communs : Allemagne, Australie, Nouvelle-Zélande, Canada, Espagne, États-Unis, Finlande, France, Grèce, Italie, Pays-Bas, Norvège, Royaume-Uni et Suède. Dans chacun de ces pays existe une structure semblable à la DCSSI : Allemagne (BSI), R.-U. (CESG), Australie (DSD), Canada (CSE), États-Unis (NIST/NSA)...

8.3.4.1. La vocation prudentielle du profil de protection

8.3.4.1.1. Référentiel de sécurité pour l'agrément de nouveaux entrants

L'agrément (au sens de la loi bancaire et de la loi de modernisation des activités financières) de nouveaux entrants souhaitant exercer leurs activités via Internet passe actuellement par la constitution d'un dossier comportant un questionnaire spécifique "Internet" (voir point 8.3.1.1.1).

La certification vis-à-vis d'un référentiel reconnu pourrait être prise en compte dans l'examen du dossier du porteur de projet en faisant bénéficier celui-ci d'une présomption de conformité aux demandes des autorités d'agrément pour la partie "site web" de son système d'information.

8.3.4.1.2. Référentiel pour le contrôle permanent de la sécurité des systèmes d'information

La certification sur le fondement de ce PP répondrait, en partie, aux exigences prudentielles posées par l'alinéa 1er de l'article 14 du règlement n° 97-02 du Comité de la réglementation bancaire et financière qui dispose que :

" Les établissements de crédit déterminent le niveau de sécurité informatique jugé souhaitable par rapport aux exigences de leurs métiers. Ils veillent au niveau de sécurité retenu et à ce que leurs systèmes d'information soient adaptés ".

A ce titre, la certification ne constituerait qu'un élément complémentaire intégré au dispositif global de sécurité, lequel doit rester sous l'entière maîtrise de la direction générale de l'établissement.

8.3.4.1.3. Ce profil de protection devrait répondre aux recommandations du Comité de Bâle…

La vocation internationale du PP implique en effet que les exigences de sécurité s'appuient sur des normes ou des recommandations internationales. Il est convenu en conséquence de prendre en compte les recommandations relatives à la sécurité des banques électroniques, qui seront émises, au premier semestre 2001, à l'issue des travaux en cours au sein du groupe « *Electronic banking* » du Comité de Bâle sur le contrôle bancaire. Ces recommandations devraient couvrir les exigences spécifiques en matière de " Disponibilité, Intégrité, **Confidentialité** et Preuve " et encourager la mise en place de dispositifs permettant la **non-répudiation**. La question d'inclure ou non la spécification du poste client est cependant posée, s'agissant de couvrir la sécurité des transactions et la **non-répudiation**.

8.3.4.1.4. …et faciliter ainsi les démarches des établissements pour obtenir un agrément dans les juridictions hors espace économique européen.

La certification par rapport à ce référentiel, reconnu internationalement en raison du standard choisi, devrait servir de garantie pour les autorités de contrôle étrangères quant au niveau de sécurité des sites des établissements concernés (" banques électroniques ") qui désireraient fournir des services dans leurs juridictions.

18. La dimension internationale du « profil de protection »

Il serait donc de l'intérêt des établissements de pouvoir bénéficier d'une certification conforme aux Critères communs, lorsqu'ils souhaitent fournir des services au delà de l'Union européenne, selon un référentiel répondant aux recommandations du Comité de Bâle sur le contrôle bancaire relatives à la maîtrise des risques encourus par les banques électroniques, qui seront adoptées au courant du premier semestre 2001. Les représentants de la France sont d'ailleurs intervenus en ce sens au sein du groupe « *Electronic banking* » du Comité de Bâle.

8.3.4.2. La mise en place éventuelle d'une labellisation

Certains besoins sécuritaires, au-delà de la cible d'évaluation qui sera adoptée pour le PP, pourraient être jugés importants par les établissements. La réponse se situerait dans une labellisation complémentaire permettant de garantir la qualité du site concerné, notamment en regard des critères juridiques devant entourer la relation commerciale sur un plan bilatéral.

19. La labellisation des sites

La création d'un label englobant ces aspects répondrait ainsi à l'objectif d'offrir une assurance supplémentaire de légitimité aux clients, tout en constituant un argument commercial pour les établissements qui l'adopteraient. Par ailleurs, des réflexions supplémentaires devraient être menées afin de permettre une gradation des labels, qui selon les diverses exigences de sécurité couvertes, sont par nature différents. Il est jugé souhaitable que le label, instrument destiné à maîtriser le risque d'image, soit défini au sein des organisations professionnelles.

8.3.4.3. Le choix d'une approche modulaire : la définition de plusieurs profils de protection

La définition de profils de protection s'incrirait dans une approche modulaire et progressive. Il est proposé de définir un PP " site web financier transactionnel " de base. À ce titre, le périmètre du PP serait l'infrastructure d'accès à Internet, définie par le Guide " politique de sécurité Internet " du Forum des compétences, annexé au présent Livre blanc (partie 2, point 3.1. et suivants du Guide). L'infrastructure d'accès à Internet est l'ensemble des points d'accès Internet, zones d'interconnexion entre le réseau public (Internet) et les équipements frontaux du site.

La cible de sécurité de ce profil de protection serait de s'assurer que des réponses satisfaisantes et adaptées à l'évaluation par l'établissement de ses risques soient apportées aux menaces susceptibles de porter préjudice aux utilisateurs, aux menaces portant sur le fonctionnement des services et aux menaces susceptibles de porter atteinte aux clients et aux services.

Des profils particuliers pourraient être définis pour couvrir les spécificités des différents services bancaires et financiers transactionnels : services de gestion de compte et de moyens de paiement, courtage en ligne et gestion de portefeuille, et opérations de crédit en ligne.

- **Des réponses aux menaces susceptibles de porter préjudice aux utilisateurs**

- **L'atteinte à la vie privée** (écoute, conservation illicite d'informations personnelles),

- **l'usurpation d'identité** d'un utilisateur autorisé,

- **la répudiation** pour les transactions jugées sensibles par l'établissement,

- **la perte d'intégrité** des flux d'information, et du poste client le cas échéant.

- **Des réponses aux menaces pesant sur le fonctionnement du service**

- La permanence de la **disponibilité des systèmes** doit être au cœur des préoccupations des responsables. C'est ainsi qu'en raison des menaces spécifiques de l'Internet, notamment en matière de déni de service, la fiabilité des systèmes de secours ('back-up') doit être particulièrement renforcée,

- la **répudiation,**

- la maîtrise des risques d'**intrusion** (accès illicite, contournement du contrôle d'accès, modification des règles),

- l**'usurpation de l'identité** des exploitants du système,

- la perte d'**intégrité**,

- les **fraudes et malversations internes** représentent les menaces les plus conséquentes. La mise en place conjointe de mesures assurant un contrôle efficace des accès, ainsi que de modalités d'attribution des autorisations réellement discriminantes, est seule de nature à juguler ce risque.

- **Des réponses aux menaces susceptibles de porter atteinte à la fois au service et aux clients**

- Le **risque de détournement de sites** (*web spoofing*), qui consiste à substituer à des sites " officiels ", et parfaitement honorables, des services dont le moindre effet est de nuire à l'image des premiers, et à l'extrême de fonder un système de fraude engageant leur responsabilité, faute de preuves contraires suffisantes,

- le formalisme des contrats bancaires et financiers, les contrats électroniques devant s'adapter aux exigences formelles de l'écrit-papier, et les modalités d'archivage.

Ces dernières exigences devraient être particulièrement analysées sous un angle à la fois juridique et technique et devraient faire l'objet, de la part du CFONB, de travaux complémentaires pour chacun des services financiers considérés : services de gestion de compte et de moyens de paiement, courtage en ligne et gestion de portefeuille, et opérations de crédit en ligne.

8.3.4.4. Modalités de la certification

8.3.4.4.1. La démarche de certification

La démarche de certification, sur le fondement du PP, pourrait s'inscrire dans le cadre du Schéma national d'évaluation et de certification de la sécurité des technologies de l'information[13] , qui précise le contexte réglementaire et l'organisation nécessaire à la conduite d'une évaluation par une tierce partie et à son contrôle, conduisant à la délivrance de certificats. L'évaluation selon les **Critères communs** exige le recours à un Centre d'évaluation de la sécurité des technologies de l'information (CESTI), accrédité par la **DCSSI** pour mener la certification. Une fois l'évaluation achevée, il reviendra à la **DCSSI** de délivrer un certificat susceptible d'être reconnu au niveau international.

8.3.4.4.2. Possibilité d'offrir des fonctionnalités plus larges que celles qui sont décrites dans le profil de protection

C'est dans sa cible de sécurité que le commanditaire de l'évaluation explique quelles sont les fonctions offertes par son produit ou son système, en plus de celles qui sont prévues dans le profil de protection. Il devrait aussi expliquer, le cas échéant, quels sont les besoins de sécurité supplémentaires qui découlent de l'ajout de ces nouvelles fonctions.

La cible de sécurité retenue par le commanditaire pourrait aller au-delà de l'expression d'une simple conformité au profil de protection. Il s'agirait dans ce cas de faire évaluer un certain nombre de fonctions sécuritaires supplémentaires à travers son produit et/ou son système.

8.3.4.4.3. Cas d'une modification du produit ou du système

La technologie relative aux sites Internet étant en perpétuelle évolution, un certificat ne peut avoir de période de validité fixe. Cela impliquerait que soit mis en place un mécanisme de maintenance assorti d'une procédure d'évaluation des conséquences sécuritaires des changements à intégrer dans le temps.

8.3.4.4.4. Coût d'une évaluation selon les Critères communs

Le processus de certification impliquant les CESTI et la DCSSI requiert :

- Un investissement initial (formation des responsables techniques / sécurité aux **Critères communs**) que devra fournir l'établissement qui n'a jamais mené à bien ce type d'évaluation.

- Un coût externe lié à la prestation du laboratoire d'évaluation. Ce coût dépend des moyens humains et des équipements qui sont mis en œuvre. Il est donc largement proportionnel à la complexité du produit ou du système évalué, ainsi qu'au niveau d'assurance requis en matière de sécurité.

---

13) Le Schéma définit l'organisation nécessaire à la conduite des évaluations de sécurité dans les meilleures conditions de coût, d'efficacité et d'impartialité. La DCSSI, dans son rôle d'organisme de certification, agrée et contrôle les centres d'évaluation (CESTI) et délivre les certificats officiels à l'issue des évaluations.

Le coût d'une évaluation selon les Critères communs varie sur une échelle de un à dix selon le niveau d'assurance[14] retenu EAL1+ ou EAL4+. À ce titre, on peut pressentir une gradation des exigences de sécurité intégrant tout ou partie des points suivants :

- le niveau de compétence des équipes ;

- l'examen par l'évaluateur de l'architecture et des spécifications fonctionnelles du système ainsi que de la documentation utilisateur pour vérifier leur adéquation avec la cible de sécurité produite ;

- des tests des fonctions de sécurité de la cible, conduits par des tiers indépendants ;

- une analyse indépendante des vulnérabilités de la cible, démontrant sa résistance à des attaques de bas niveau ;

- la mise en place d'une gestion de configuration.

Un coût interne lié au suivi de l'évaluation et à la fourniture de la documentation (d'autant plus faible que des bonnes pratiques en matière de développement et d'intégration ont été mises en œuvre ou que l'évaluation est faite en amont).

8.4. La maîtrise des risques de blanchiment

8.4.1. Problèmes d'application de la réglementation en matière d'identification des clients

8.4.1.1. Obligations légales et réglementaires en matière d'identification des clients

8.4.1.1.1. En l'état actuel, les établissements financiers sont soumis à la réglementation relative à la lutte contre le blanchiment des capitaux, quels que soient les canaux utilisés pour effectuer les opérations

La loi n°90-614 du 12 juillet 1990 impose aux organismes financiers, " avant d'ouvrir un compte, de s'assurer de l'identité de leur cocontractant par la présentation de tout document écrit probant ". Le décret n°91-160 du 13 février 1991 précise la nature des documents exigés :

- pour une personne physique : un document officiel portant la photographie de celle-ci ;

- pour une personne morale : la présentation de l'original ou l'expédition ou la copie certifiée conforme de tout acte ou extrait de registre officiel constatant la dénomination, la forme juridique et le siège social, ainsi que les pouvoirs des personnes agissant au nom de la personne morale.

---

14) Le niveau d'assurance est déterminé par une échelle allant de EAL1 à EAL7. EAL1 est prévu pour une évaluation sans développeur (analyse des fonctions de sécurité de la cible d'évaluation, spécifications fonctionnelles de la cible, tests indépendants des fonctions de sécurité). EAL2 est une évaluation indépendante de bas niveau (conception générale des sous-systèmes, revue des tests boîte-noire, des fonctions de sécurité effectuées par le développeur, recherche de vulnérabilités élémentaires). EAL3 est une évaluation de niveau moyen (notamment tests boîte-grise, recherche des vulnérabilités justifiée par le développeur, gestion de configuration de la cible). EAL4 est une évaluation boîte-blanche complète (recherche indépendante des vulnérabilités, contrôle du développement par rapport à un modèle de cycle de vie, gestion de configuration automatisée). EAL 5 est un haut niveau d'assurance obtenu par le recours à une méthode de développement rigoureuse. EAL 6 et EAL7 sont respectivement une évaluation des systèmes présentant un fort et un très fort degré de risques.

Les organismes financiers doivent conserver les références ou la copie de ces documents. La même obligation pèse sur eux pour les clients occasionnels réalisant des opérations dont la nature et le montant sont précisées dans le décret susvisé (somme supérieure à 50.000 F, location de coffre).

La loi précise, en outre, que lorsque l'organisme financier suspecte que son interlocuteur pourrait ne pas agir pour son propre compte, il se renseigne sur l'identité du bénéficiaire véritable et demande à cet effet la présentation de tout document ou justificatif qu'il estime nécessaire.

8.4.1.1.2. La réglementation susvisée relative à l'entrée en relation avec de nouveaux clients ne peut être appliquée en l'état aux opérations effectuées sur Internet

Toutefois, il n'en va pas de même selon que le client à identifier est une personne physique ou une personne morale. Les exigences de la réglementation actuelle en matière d'identification des personnes physiques ne sont pas applicables parce que ces dernières ne peuvent se dessaisir des documents originaux dont la présentation est requise.

En outre, une pièce d'identité ne vaut pas identification par elle-même mais seulement lorsqu'elle est présentée par son titulaire. En précisant que le document officiel doit porter la photographie de la personne dont l'organisme financier s'assure de l'identité, le décret n° 91-160 du 13 février 1991 susvisé contraint une personne physique à s'exposer personnellement pour identification (voir aussi en ce sens, les recommandations professionnelles de l'Association française des banques relatives à la lutte contre le blanchiment de l'argent de la drogue, mars 1991, page 21).

Il est à souligner que l'article 33 du décret n° 92-456 du 22 mai 1992 pris pour l'application du décret-loi de 1935 relatif au chèque est encore plus explicite : les établissements de crédit et personnes habilitées à tenir des comptes sur lesquels des chèques peuvent être tirés " doivent, préalablement à l'ouverture d'un compte, vérifier le domicile et l'identité du postulant qui est tenu de présenter un document officiel portant sa photographie".

En revanche, l'identification à distance des personnes morales est plus aisée et peut être faite dans le respect de la réglementation actuelle. En effet, les personnes morales peuvent produire par correspondance des copies certifiées conformes ou des extraits originaux de registres du commerce ou de greffe.

Ainsi qu'il est rappelé dans la recommandation n° 10 du **GAFI**, les organismes financiers peuvent également en accédant aux registres publics, par voie télématique (ou autre moyen de consultation à distance), vérifier l'existence et la structure juridique de la société et obtenir des renseignements sur sa forme juridique, son adresse, ses dirigeants et les dispositions régissant le pouvoir d'engager la personne morale.

Enfin, le problème de présentation " physique " des documents n'existe pas pour les personnes morales. Cependant, il reste entier pour la vérification des pouvoirs des personnes habilitées à les représenter.

8.4.1.1.3. Les exigences de la réglementation actuelle en matière d'identification du client représentent cependant une contrainte non négligeable pour les personnes (physiques ou morales) qui souhaitent réaliser des opérations sans que leur identité véritable soit connue

D'une part, la contrefaçon des documents officiels exigés a un coût. En effet, ces documents possèdent tous des " signes de sécurité " ainsi que des références qui sont notamment destinées à distinguer les originaux des contrefaçons. En outre, les organismes financiers exercent un contrôle de vraisemblance sur les documents présentés. Ainsi, l'Association française des banques recommande de rapprocher la signature de la pièce d'identité de celle déposée par le client, d'examiner les anomalies éventuelles du document, de s'assurer de la ressemblance entre la photographie et la personne présentant le document (voir les recommandations professionnelles de mars 1991, page 21). Par ailleurs, la jurisprudence rendue sur l'application de l'article 33 du décret du 22 mai 1992 susvisé est exigeante à l'égard des organismes financiers. Il demeure que ce contrôle est plus difficile pour les documents d'origine étrangère.

D'autre part, on a vu plus haut que l'exposition " physique " auprès de l'organisme financier est incompatible avec une entrée en relation d'affaires à distance pour les clients personnes physiques.

Il en résulte que renoncer aux exigences de la loi de 1990 susvisée et des textes pris pour son application aboutit nécessairement à faire le choix d'une identification moins certaine du client et à une plus grande exposition du système bancaire aux risques de blanchiment : on rappellera à cet égard que l'identification du client est au cœur du dispositif préventif de lutte contre le blanchiment des capitaux. Il convient donc de rechercher la façon de satisfaire ces exigences en adaptant la réglementation existante.

8.4.1.2. Les expériences étrangères

On soulignera tout d'abord que certains pays, les Etats-Unis notamment, n'ont pour l'instant pas marqué de préoccupation majeure en matière de problèmes d'identification des clients à distance. Au Royaume-Uni, les autorités privilégient la connaissance des activités et des opérations du client (" *know your customer policy* ") plutôt que son identification, ce qui peut paraître plus réaliste en termes de résultats attendus dans la lutte contre les opérations de blanchiment réalisées par Internet mais pose un problème de conformité avec la recommandation du **GAFI** relative à l'identification du client.

En revanche, d'autres autorités étrangères se penchent sur la question et commencent à proposer des solutions diverses. La Commission bancaire et financière belge (CBF) a diffusé à ses assujettis (établissements de crédit et entreprises d'investissement) une note visant principalement à cerner les aspects du cadre réglementaire et prudentiel actuel qui s'appliquent spécifiquement à l'environnement d'Internet. Dans cette note, la CBF insiste sur le fait que la loi du 11 janvier 1993 sur le blanchiment n'établit pas de distinction selon qu'une relation d'affaires ou une opération se noue au moyen d'un contact face à face ou d'un contact par courrier, télécopie, e-mail ou Internet. La réglementation exige par conséquent que l'établissement s'assure, au moment de nouer une relation d'affaires avec un client, de l'identité

de celui-ci " au moyen d'un document probant dont une copie est prise et conservée ". Si un établissement veut conclure des contrats ou des opérations à distance avec des clients, sans qu'il y ait de contact face à face, il doit donc mettre en place des procédures spécifiques d'identification qui satisfont à plusieurs conditions de base, parmi lesquelles :

- ces procédures garantissent une identification adéquate des clients, conformément à la réglementation belge ;

- elles ne peuvent pas être appliquées si l'établissement soupçonne ou dispose d'indications permettant de croire que le client évite précisément un contact face à face pour dissimuler sa véritable identité et/ou qu'il est question de blanchiment de capitaux ;

- elles doivent faire l'objet d'une attention particulière de la part des auditeurs internes et externes de l'établissement.

En Allemagne, l'Office fédéral de supervision bancaire a inclus en 1996 des dispositions spécifiques concernant l'identification à distance dans ses normes relatives aux " mesures à prendre par les établissements de crédit pour combattre et prévenir le blanchiment ". Elles prévoient que si, pour une bonne raison, l'identification ne peut être réalisée par l'établissement de crédit lui-même, par l'intermédiaire de ses employés, elle doit être faite pour le compte de l'établissement par des tiers de confiance tels que notaires, avocats, consulats, ambassades, ou selon une procédure d'identification postale, en conformité avec les règles applicables aux établissements de crédit.

En Finlande, l'autorité de surveillance a diffusé un communiqué sur l'identification des clients à distance, selon lequel les participants du marché monétaire doivent appliquer les pratiques habituelles en la matière. Ces pratiques sont applicables à Internet et aux autres services fournis directement aux clients, en particulier lorsque des nouveaux clients souscrivent des actions qui leur sont proposées par téléphone ou par Internet. L'identité du client doit être établie de manière adéquate avant qu'il puisse acheter ou vendre des actions par Internet.

En Suisse, l'ouverture de comptes à distance sur Internet n'est pas possible sans identification formelle du client (par une copie de la carte d'identité par exemple).

Le Service de lutte anti-blanchiment espagnol considère qu'il serait souhaitable de réserver les services bancaires sur Internet aux clients déjà identifiés selon une relation traditionnelle avec l'établissement bancaire.

La proposition de modification de la directive 91/308/CEE relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux (article 3.10) prévoit à cet égard qu'en cas d'ouverture de compte à distance, les établissements relevant de la présente directive doivent prendre les mesures spécifiques et adéquates nécessaires visant à répondre au risque accru de blanchiment de capitaux qui existe lorsqu'ils nouent des relations d'affaires ou effectuent une transaction avec un client qui n'est pas physiquement présent aux fins d'identification. Ces mesures garantissent que l'identité du client est établie en demandant notamment au client de produire des pièces justificatives supplémentaires permettant de s'assurer de l'identité de ce dernier.

8.4.1.3. L'adaptation de la réglementation en vue de la rendre applicable aux opérations initiées sur Internet

L'adaptation de la réglementation ne s'impose que pour les clients personnes physiques. La réglementation peut en effet demeurer inchangée pour les clients personnes morales. Toutefois, concernant ces derniers, il s'agit de rappeler que les règles d'identification s'appliquent également aux opérations sur Internet.

Il conviendrait alors de définir des règles d'identification permettant une sécurisation maximale de l'entrée en relation avec la clientèle tout en tenant compte de l'absence de relation " face à face ", impliquant en conséquence une moindre identification. Il serait possible de s'inspirer du cas des établissements bancaires sans guichets, pour lesquels la problématique apparaît très proche de celle posée par Internet.

Actuellement, les organismes financiers, qui proposent des ouvertures de comptes à distance à leurs clients, procèdent à un certain nombre de mesures additionnelles de vérification et notamment demandent la production de pièces justificatives supplémentaires pour s'assurer de l'identité d'un client. Par exemple, le client doit fournir :

- une photocopie recto-verso de la carte d'identité ou du passeport ;

- deux bulletins de salaire originaux ;

- un original de la dernière quittance EDF-GDF.

Certains organismes financiers adressent au client les instruments de paiement ou les codes qui permettront à ce dernier d'initier des opérations sur son compte par lettre avec accusé de réception. Le retour de cet avis conditionne dans ce cas le début du fonctionnement du compte. En outre, d'autres organismes financiers exigent que la première alimentation du compte soit effectuée par un chèque à l'ordre de la banque à distance tiré sur la banque actuelle du client.

On relèvera que par ce mécanisme d'alimentation des comptes ouverts auprès d'elles, les banques à distance obtiennent une garantie supplémentaire sans pouvoir reporter la charge d'identification sur la banque précédente de leurs clients. Cette assurance est cependant relative ; certaines banques pouvant être moins regardantes sur les procédures de vigilance contre le blanchiment, que ce soit par négligence ou parce que la réglementation qui lui est applicable est moins exigeante que la réglementation française.

Enfin, ces établissements à distance n'exigent pas la présentation du document officiel original, ni même d'une copie conforme, ce qui lève en grande partie la contrainte du coût de contrefaçon de documents ; en effet, le coût de réalisation d'une copie simple de document officiel est souvent bien inférieur à celui d'un original (facilité des montages, disparition des signes de sécurité, etc.).

Des exigences supplémentaires pourraient être obtenues dans le cadre d'une procédure ad hoc, telle que la production par le client d'un relevé d'identité bancaire (RIB) provenant

d'un autre établissement de crédit (ou l'équivalent du RIB dans le cas d'un établissement non résident) accompagné d'une attestation certifiant que le compte visé par le RIB a été ouvert par la production de documents originaux.

Cette voie a également été retenue par le Conseil des Marchés Financiers (CMF), dont la décision n° 99-07 précise les prescriptions et recommandations pour les prestataires de services d'investissement offrant un service de réception-transmission ou d'exécution d'ordres de bourse comportant une réception des ordres via Internet.

Il doit être souligné que cette décision n'a pas pour objectif premier de lutter contre l'utilisation des services d'investissement offerts via Internet à des fins de blanchiment de capitaux, mais, plus largement, de préciser les conditions d'application des règles de bonne conduite édictées aux titres II et III du règlement général du CMF (articles 2.4.12, 2.4.13, 3.3.2, 3.3.5, 3.3.7), lorsqu'un ordre est reçu via Internet.

Certaines des dispositions de la décision susvisée semblent néanmoins particulièrement intéressantes en matière de lutte contre le blanchiment. L'article 4 de cette décision décrit précisément la procédure d'identification du client demandant la réalisation d'une opération via Internet. Il rejoint les modalités décrites au paragraphe précédent, puisqu'il prescrit la réception préalable à la réalisation de toute opération :

- d'une photocopie d'une pièce d'identité en cours de validité (passeport, carte d'identité, permis de conduire) ;

- d'un relevé d'identité bancaire ou un chèque annulé (mais le compte visé pourrait avoir été aussi ouvert à distance) ;

- d'un justificatif de domicile.

Le prestataire confirme au nouveau client qu'il a bien reçu les documents mentionnés en lui adressant une lettre avec avis de réception, qui lui permet d'établir la réalité du domicile qui lui a été communiqué.

Comme il a été indiqué précédemment, cette procédure est également utilisée par certains établissements de crédit et il apparaît souhaitable que le recours à cette dernière soit généralisé. Cet article n'apporte cependant pas de précisions sur le cas des clients personnes morales ; l'article 3.3.2 du règlement général du CMF est à cet égard lui-même insuffisant puisqu'il ne requiert que l'identification des représentants légaux des personnes morales.

Aux termes de l'article 6 de la décision n° 99-07, " le prestataire habilité informe clairement le client qu'aucune opération ne peut être initiée tant qu'il n'a pas reçu les documents prévus à l'article 4, s'agissant d'un nouveau client ". Cette disposition est intéressante car elle souligne bien que la réalisation d'opérations à distance, particulièrement sur Internet, d'une manière complètement dématérialisée et présentée comme un gage de rapidité et gain de temps dans la réalisation des opérations, ne dispense pas le client de fournir aux organismes financiers les informations requises pour lutter contre le risque de blanchiment.

À ce stade, il apparaît nécessaire de souligner que le fonctionnement d'un compte – y compris la réception de fonds et d'instruments financiers – ne peut être autorisé qu'une fois que la procédure d'identification a été achevée. En outre, il est recommandé aux établissements, dans la mesure des possibilités techniques, de déterminer le lieu d'où sont émis les ordres reçus sur leur site, pour que leur attention soit appelée par un ordre en provenance d'un pays sans relation apparente avec le client. Il apparaît également envisageable de définir, au moins pour certaines entreprises, l'adresse physique qui sera seule acceptée pour les échanges de flux sur Internet. Enfin, les établissements doivent rester attentifs à toute évolution technique qui est susceptible de remettre en cause les contrôles en place ou au contraire les faciliter.

20. L'ouverture des comptes à distance

Dans le cas où la reconnaissance physique apparaît imposible à mettre en oeuvre, les organismes financiers qui proposent des ouvertures de comptes à distance à leurs clients doivent procéder à des mesures additionnelles de vérification au nombre desquelles la production de pièces justificatives supplémentaires pour s'assurer de l'identité d'un client. Ces mesures additionnelles de vérification doivent permettre de connaître avec certitude l'identité du client et de satisfaire le degré d'exigence en cette matière imposée par la loi de 12 juillet 1990.

8.4.1.4. L'utilisation de certificats émis dans le cadre de la signature électronique

Il convient de s'interroger sur l'articulation entre les dispositions relatives à la signature électronique et celles concernant l'identification du client dans le cadre de la lutte contre le blanchiment.

Certes, l'utilisation de certificats émis dans le cadre de la signature électronique pourrait constituer un élément nouveau permettant l'identification du client.

Pour autant, la prise en compte par le banquier d'un **certificat** de signature électronique peut-elle suffire à attester que la vérification de l'identité du client requise par la loi de 1990 a été faite ?

Sur le plan technique, on observera que :

- le projet de décret ne décrit pas les " moyens appropriés " d'identification qui seront utilisés par le **PSC** ;

- la nature des informations contenues dans les certificats peut être très différente selon leur destination ;

- les certificats n'offriront pas les mêmes degrés de sécurité. Certains PSC seront " accrédités ", d'autres pas. Le banquier s'expose à des risques de faux certificats, qui ne seraient pas émis par le " vrai " PSC et dont la prise en compte ne vaudrait évidemment pas vérification de l'identité du client.

Sur le plan juridique, la vérification faite par un tiers peut-elle exonérer le banquier de ses obligations en matière de lutte contre le blanchiment ?

La procédure d'identification accomplie par un PSC vise à garantir la fiabilité d'une signature électronique et cet objectif est différent par nature du processus accompli par le banquier, qui vise à s'assurer de l'origine des capitaux échangés dans le système bancaire.

La prise en compte par un banquier d'un seul **certificat** de signature électronique pour identifier son client en vue de satisfaire ses obligations en matière de blanchiment pose un problème de fond puisqu'elle reviendrait à reporter sur un tiers une obligation de vérification d'identité qui, par nature, pèse sur le banquier.

En tout état de cause, il convient de souligner que le recours à une autorité de certification n'exonérerait pas les organismes de leur responsabilité au regard de l'obligation d'identification de leur clientèle imposée par l'article 12 de la loi n° 90-614 du 12 juillet 1990. Le banquier est seul responsable de la mise en œuvre de la législation de lutte contre le blanchiment, au moyen de procédures efficaces de vérification de l'identité du client. Notamment, les établissements devraient toujours être en mesure de démontrer aux autorités de contrôle, par la production de documents justificatifs de l'identité, que l'identification a été effectuée dans les conditions prévues par la réglementation. Les obligations relatives à la conservation des documents d'identification demeureraient également.

En l'état actuel du droit et de la technique, il apparaît dans ces conditions prématuré de considérer qu'un **certificat** de signature électronique puisse attester de la vérification de l'identité du client d'une banque au sens de la loi de 1990.

Par ailleurs, il est à noter que la transposition de la directive sur le «commerce électronique» est indépendante de la question de la vérification de l'identité aux fins de lutte contre le blanchiment. Les mesures prévues par la directive «blanchiment» n'empêchent pas la conclusion de conventions de compte en ligne, les documents justificatifs d'identité pouvant être communiqués par ailleurs.

8.4.2. Problèmes d'application de la réglementation en matière de connaissance des opérations

Dans le cadre de la loi du 12 juillet 1990 et des textes pris pour son application, les organismes financiers doivent exercer une vigilance constante afin d'une part de pouvoir identifier les opérations qui pourraient provenir du trafic de stupéfiants ou d'activités d'organisations criminelles, en vue de les déclarer à TRACFIN (article 3 de la loi du 12 juillet 1990), et d'autre part de constituer un dossier de renseignements pour les opérations de montant élevé caractérisées par une forte opacité (article 14 de la loi du 12 juillet 1990). Dans le même ordre d'idées, des procédures internes doivent être mises en œuvre pour assurer le respect du dispositif de lutte contre le blanchiment. Ces procédures comprennent notamment des règles écrites internes décrivant les diligences à accomplir, ainsi qu'un système de surveillance permettant de vérifier leur mise en œuvre. Ces dispositions ne sont pas incompatibles en elles-mêmes avec la réalisation d'opérations sur Internet.

8.4.2.1. Préoccupations étrangères

Dans la note qu'elle a adressée à ses assujettis sur l'application de la réglementation prudentielle à Internet, la Commission bancaire et financière belge énonce un certain nombre de points requérant une attention particulière sous l'angle prudentiel, points explicités ensuite dans une *check-list* distincte à l'aide de laquelle les établissements utilisant le réseau Internet pourront vérifier le caractère adéquat de leur organisation. Il est notamment mentionné que les établissements doivent se doter de procédures adéquates pour suivre -si possible électroniquement et en temps réel- les transactions du client et le contrôle des risques y afférant, ainsi que d'outils d'analyse permettant de détecter les éventuelles opérations de blanchiment. Des mesures techniques et organisationnelles appropriées doivent être prises pour que, si le respect des dispositions légales l'exige, l'établissement puisse différer la réalisation d'une opération et/ou refuser d'exécuter des transactions pour le compte d'un client le temps de procéder aux vérifications obligatoires.

Aux États-Unis, lors de ses enquêtes sur les services de banque électronique offerts par ses assurés, le FDIC vérifie également l'existence de procédures appropriées pour repérer les opérations complexes des clients.

8.4.2.2. Application aux opérations effectuées sur Internet

Le développement de la " banque Internet " doit s'accompagner pour les organismes financiers de la mise en place d'un système de surveillance informatisé, selon un degré d'automatisation à définir, afin d'exploiter de manière méthodique et systématique le système d'information et de se doter des moyens pour :

8.4.2.2.1. Détecter les opérations nécessitant un contrôle de vraisemblance

Sur ce point, la banque doit établir pour chaque client un profil de fonctionnement du compte et sortir des anomalies circonstanciées lorsque les caractéristiques d'une opération s'écartent sensiblement d'un comportement attendu. Certaines opérations pourraient servir d'indicateurs, permettant de surveiller (sinon contrôler) des mouvements inhabituels ou curieux. Dans un contexte automatisé et de traitement de masse des opérations auquel s'ajoute la possibilité de réaliser ces dernières sur Internet 24h sur 24, le délai nécessaire pour détecter une opération douteuse peut être plus long et conduire à ne l'isoler qu'a posteriori avec l'impossibilité de surseoir à son exécution. Dans la mesure du possible, il est nécessaire que soient mis en place des verrous qui permettent de bloquer la réalisation de certaines opérations répondant aux critères retenus pour identifier les opérations douteuses.

Bien qu'une liste exhaustive de critères soit impossible à établir et sous réserve des observations complémentaires que pourrait apporter TRACFIN, ces derniers pourraient comprendre notamment :

- les fonds en provenance ou à destination de certaines zones géographiques et en particulier des juridictions non coopératives identifiées par les travaux du Groupe d'action finanière (**GAFI**) ;

- des opérations dont les montants apparaissent anormalement élevés au regard du fonctionnement habituel du compte, en particulier pour les opérations supérieures à 1MF ;

- la détection du fractionnement des opérations dont le montant total sur une brève période et à destination d'un même bénéficiaire dépasse les seuils qui donnent lieu à déclaration ou à une vigilance renforcée.

21. Une vigilance renforcée en matière de surveillance des opérations sur Internet

La surveillance des opérations sur Internet en raison de la distanciation des liens avec le client doit conduire les établissements à faire preuve d'une vigilance renforcée ; aussi apparait-il d'autant plus nécessaire que les contrôles ne soient pas uniquement automatisés mais qu'il existe toujours des gestionnaires de compte qui centralisent toutes les informations sur les opérations effectuées sur le compte. Seule l'affectation d'un compte à un gestionnaire unique garantit que ce dernier ait une bonne connaissance de son fonctionnement et soit ainsi plus à même de détecter les opérations douteuses.

8.4.2.2.2. S'assurer que les renseignements qui sont éventuellement exigés lors des ordres de transferts émis par un client sont complets et conservés afin de garder la traçabilité de l'opération

L'article 15 de la loi précitée prévoit que les organismes financiers doivent conserver pendant cinq ans à compter de leur exécution les documents relatifs aux opérations. La faisabilité technique de cette disposition relative à la nature des données qui peuvent être conservées et au support de conservation a été soumise aux établissements.

En ce qui concerne la traçabilité des opérations, l'utilisation d'Internet peut apporter des éléments qui favorisent la localisation des flux. A contrario, le reroutage peut constituer un obstacle à la possibilité d'identifier avec certitude l'origine d'une transaction, aussi convient-il de s'interroger sur les possibilités techniques de contrarier son utilisation.

8.4.2.2.3. Bloquer le cas échéant la réalisation automatique de certaines opérations afin de se donner le temps d'examiner leurs caractéristiques ou d'obtenir un complément d'informations

Il convient de faire remonter à la hiérarchie les opérations les plus importantes pour information ou pour instruction dans le cadre de l'article 3 de la loi du 12 juillet 1990.

On peut cependant s'interroger sur la faisabilité (et la pertinence) de bloquer systématiquement une opération répondant à certains types d'alerte jugés graves (conditions restrictives sur l'automaticité relatives au statut de résident ou non résident, au montant de l'opération, à la localisation du pays émetteur ou destinataire), en attendant une décision de l'établissement de crédit (acceptation ou rejet). En tout état de cause, l'exécution de l'opération n'empêche pas l'établissement de crédit de l'analyser et de faire, le cas échéant, la déclaration de soupçon (en ce sens, article 6 de la loi du 12 juillet 1990).

Le système de surveillance ou de maîtrise d'engagements des opérations entre également dans le champ du contrôle interne que doit exercer tout établissement dans le cadre du règlement n° 97-02 du Comité de la réglementation bancaire et financière. Le risque de blanchiment pourrait être explicitement mentionné de telle sorte qu'il soit traité comme les autres risques mentionnés à l'article 2. En outre, s'agissant d'une " banque Internet ", les procédures qui sont à la base du système de surveillance doivent être structurées.

9. la maîtrise du risque sur les clients

9.1. Les exigences relatives au contrôle de la capacité du prestataire à maîtriser son site web et son activité

L'offre de services financiers à distance, notamment via le canal Internet[15], ne modifie pas la nature des risques inhérents aux activités de crédit ou de services d'investissement mais réclame un renforcement des dispositifs de contrôle interne. Internet permet en effet un accès moins formel et plus rapide aux services financiers pour une clientèle pressée dont le prestataire perçoit plus difficilement le profil de risques. Au moment de l'agrément, ce mode de prestation amène donc à s'interroger sur la capacité d'un prestataire à maîtriser les risques de contrepartie préalablement au démarrage de l'activité.

22. Exigences relatives au contrôle de la capacité du prestataire à maîtriser son site web et son activité

Il est proposé, en la matière, de fixer trois conditions préalables à l'agrément d'un prestataire de services financiers en ligne.

La première viserait à demander à ce que le prestataire candidat à l'agrément rédige des procédures encadrant les critères d'identification et de sélection de la clientèle.

La deuxième consisterait pour le prestataire à établir des modèles de conventions précisant les responsabilités des différentes parties, notamment ses clients qui devraient être classés selon la typologie ciblée.

La troisième consisterait à demander à ce que le prestataire se dote de filtres automatiques en amont de l'acceptation des ordres et d'outils permettant de suivre en temps réel les positions des clients. Les autorités pourraient demander tout élément de preuve au prestataire permettant d'apprécier le caractère opérationnel de ces systèmes de filtre et de suivi avant de se prononcer sur l'agrément. Lorsque le prestataire a recours à un tiers pour leur installation et/ou leur fonctionnement, une convention fixant les responsabilités des parties en termes de moyens et de résultats, notamment en cas de panne ou d'erreur, devrait être établie.

Les développements qui suivent visent à préciser les critères permettant d'apprécier la capacité du prestataire de respecter les conditions d'agrément qui lui sont fixées ci-dessus.

9.1.1. Les exigences relatives aux critères d'identification et de sélection de la clientèle

En amont de toute offre à distance, il conviendrait que le prestataire de services financiers établisse une typologie précise de la clientèle visée (clientèle particulière, clientèle professionnelle) et adapte les procédures préalables au démarrage commercial en fonction de cette segmentation

15) Sont aussi concernés les supports précurseurs de l'offre financière à distance tels les services Audiotel par téléphone, le Minitel, la mise à disposition d'écrans délocalisés.

(définition de limites, accords sur les stratégies d'intervention sur les marchés financiers…). Au moment de l'agrément, le prestataire devrait également déclarer s'il entend offrir ses services à des clients localisés à l'étranger et prouver l'adaptation de ses procédures aux réglementations locales.

Parmi les procédures susvisées, les éléments suivants pourraient être examinés lors de l'agrément :

- une signature manuscrite voire électronique, le cas échéant, des conventions d'ouverture de compte et de responsabilité des parties est recommandée préalablement au démarrage de toute relation commerciale ;

- le prestataire devrait évaluer, préalablement au démarrage puis dans une phase d'essai au début de l'activité, la compétence du client s'agissant de sa maîtrise des opérations et de ses connaissances des instruments financiers et des marchés. Une documentation de base sur l'offre de services et leurs risques doit être élaborée et distribuée aux clients ;

- le prestataire devrait établir une procédure d'identification du client. Le dossier client et les conventions doivent inclure l'ensemble des personnes autorisées à intervenir à partir d'une même machine.

9.1.2. Les exigences relatives au contenu des conventions précisant les responsabilités des parties

Ces exigences se situent en amont du démarrage d'activité et peuvent être complétées par les réflexions propres au contrôle interne. Il conviendrait, à ce titre, de respecter les diligences suivantes :

- afin de faciliter le démarrage d'une relation commerciale, des modèles de conventions adaptés à la typologie de la clientèle ciblée, des marchés d'intervention et des instruments financiers traités doivent être élaborés ;

- le prestataire doit indiquer clairement aux clients les services pour lesquels il possède une habilitation des autorités compétentes, ceux qu'il exerce lui-même et ceux qu'il délègue à des tiers ;

- s'agissant des services d'investissement et selon l'habilitation du prestataire, la convention doit prévoir une description des responsabilités liées aux différentes étapes du cheminement d'un ordre (transmission par le client, réception par le prestataire, exécution ou transmission à un tiers courtier, compensation ou allocation à un tiers compensateur, modalités des règlements/livraisons et du paiement des éventuelles couvertures de marché selon les instruments financiers et les règles des marchés) ;

- selon la typologie des clients, les conventions doivent prévoir des dépôts de garantie minimum préalablement à tout démarrage d'un client ;

- lorsque le prestataire est simple courtier, il doit également signer une convention avec le compensateur des ordres de bourse. Cette convention précise, selon les règles de marché,

les conditions de paiement des dépôts de garantie et des appels de marge selon les marchés et les instruments financiers ;

- les parties doivent préciser les responsabilités en cas d'erreurs et convenir des éléments de preuve sur l'origine et la responsabilité de ces erreurs ;

- les parties conviennent aussi de leurs devoirs d'information réciproques et des délais de confirmation des opérations initiées ;

- dans le cas où la convention signée par le client avec le prestataire autoriserait des découverts, les modalités doivent être précisées.

Dans le respect des exigences susvisées qui pourraient être reprises par les autorités d'agrément, le soin de rédiger des modèles de convention selon la typologie des clients pourrait être délégué conjointement aux associations professionnelles et aux associations de consommateurs.

9.1.3. Les exigences relatives aux filtres et aux outils de suivi

Afin de garantir la sécurité des transactions, les prestataires de services financiers devraient se doter, préalablement à toute ouverture de compte fonctionnant en ligne, d'un système de vérification automatique de l'existence des provisions titres et espèces ainsi que des éventuelles couvertures dont bénéficie le client. Il leur appartient d'établir en parallèle un barème de limites en fonction des clients et de leurs avoirs.

Le filtre devrait notamment permettre :

- de bloquer les ordres dépassant un seuil fixé en francs ou en dépôts de garantie pour les instruments financiers à terme ;

- de gérer ces limites en tenant compte des positions déjà ouvertes ;

- de gérer une limite d'engagement maximal en tenant compte de produits différents ;

- de moduler la procédure de confirmation des ordres en fonction de l'importance des positions, du profil de gains ou pertes ou des caractéristiques de l'ordre au regard des conditions de marché (écart par rapport au dernier cours, marchés peu liquides...) ;

- d'ajuster les limites en fonction du résultat des opérations initiées par le client.

Le responsable du contrôle interne devrait avoir la maîtrise des outils technologiques de contrôle et l'autorité pour valider le paramétrage du filtre selon les contreparties. En complément, les outils de suivi dont le caractère opérationnel devrait être démontré lors d'une demande d'agrément (soit par respect de standards, soit par résultat d'une expertise indiquant leur fiabilité) devraient permettre :

- de visualiser à tout moment les positions des clients, leur situation par rapport aux limites et leurs résultats ;

- d'offrir un système d'alerte automatique lorsque les pertes d'un client atteignent un pourcentage défini de ces avoirs titres ou espèces ;

- d'entamer un dialogue avec le client sur son écran si sa ligne téléphonique est mobilisée par sa machine.

9.2. Recommandations, en matière de contrôle interne, sur l'établissement de la relation avec le client

23. Bonnes pratiques en matière de maîtrise des risques « clients »

Un recueil de bonnes conduites sur la maîtrise des risques clients est exposé ci-dessous.

En particulier, l'établissement devrait vérifier la situation financière de son client sur la base de documents appropriés. Il détermine une limite d'engagement pour chacun de ses clients et la révise régulièrement. Les procédures de l'établissement déterminent les règles applicables en matière de fixation et d'autorisation de franchissement des limites. Pour les dossiers dont la nature et l'importance le rendent nécessaire, les décisions de prêt et d'engagement doivent être prises par deux personnes au moins, ainsi que les décisions d'outrepasser les procédures automatisées. L'établissement effectue un suivi globalisé de l'ensemble des engagements sur un même client ou groupe de clients ou sur une même contrepartie, quel que soit le canal de distribution utilisé (téléphone, Internet, écrans délocalisés). Le suivi tient compte de la consommation de la provision, des garanties déposées, des opérations en cours. L'information sur la marge disponible est constamment tenue à jour.

Lorsque, après avoir consulté les informations mises à sa disposition sur les services proposés par l'établissement, un client souhaite s'engager dans une relation contractuelle avec lui (dans le cas le plus général en ouvrant un compte, d'espèces ou d'instruments financiers), il importe que les dispositions des articles 18 à 24 du règlement n° 97-02 du Comité de la réglementation bancaire et financière soient respectées. L'établissement doit également respecter l'ensemble des règlements professionnels en vigueur, en particulier ceux relatifs à la vérification préalable des couvertures clients, à l'horodatage des ordres, au cantonnement des avoirs de la clientèle, à la rétrocession des appels de marges.

D'une manière générale, l'établissement devrait s'assurer que les moyens qu'il met en œuvre pour traiter les demandes d'ouverture de relations sont adaptés en qualité et en quantité. Tout ou partie des traitements peuvent être automatisés pour faire face à une volumétrie importante de demandes, mais, en aucun cas, l'inadaptation des moyens ne doit conduire à négliger ces contrôles, même partiellement.

Naturellement, les règles suivantes s'appliquent pour un client nouveau qui ne dispose pas déjà d'un compte dans l'établissement et est connu, à ce titre, de l'établissement.

9.2.1. Connaissance du client

Les articles 19 et 21 du règlement n° 97-02 relatif au contrôle interne des établissements de crédit disposent :

Article 19

Sous réserve des dispositions prévues à l'article 23 ci-après, l'appréciation du risque de crédit doit notamment tenir compte des éléments sur la situation financière du bénéficiaire en particulier sa capacité de remboursement et, le cas échéant, des garanties reçues. Pour les risques sur des entreprises, elle doit tenir compte également de l'analyse de leur environnement, des caractéristiques des associés ou actionnaires et des dirigeants ainsi que des documents comptables les plus récents.

Les établissements de crédit constituent des dossiers de crédit destinés à recueillir l'ensemble de ces informations de nature qualitative et quantitative et regroupent dans un même dossier les informations concernant les contreparties considérées comme un même bénéficiaire, sous réserve de l'application de réglementations étrangères, limitant éventuellement la communication d'information.

Les établissements de crédit complètent ces dossiers, au moins trimestriellement, pour les contreparties dont les créances sont impayées ou douteuses ou qui présentent des risques ou des volumes significatifs.

Article 21

Les procédures de décision de prêts ou d'engagements, notamment lorsqu'elles sont organisées par la fixation de délégations, doivent être clairement formalisées et être adaptées aux caractéristiques de l'établissement, en particulier sa taille, son organisation, la nature de son activité.

Lorsque la nature et l'importance des opérations le rendent nécessaire, les établissements de crédit s'assurent dans le cadre du respect des procédures de délégations éventuellement définies, que les décisions de prêts ou d'engagements sont prises par au moins deux personnes et que les dossiers de crédit font également l'objet d'une analyse par une unité spécialisée indépendante des entités opérationnelles.

Au-delà du respect des règles relatives à la lutte contre le blanchiment, la connaissance du statut juridique du client est indispensable pour la maîtrise du risque de contrepartie, compte tenu du caractère international de l'activité.

Sur la base de l'étude juridique citée précédemment, les procédures de l'établissement doivent prévoir les informations et les éléments de preuve qui doivent être demandés au client.

9.2.1.1. Identité du client

Il s'agit non seulement de ses noms et domicile, mais également de son statut juridique. La connaissance de l'adresse personnelle du client est impérative.

L'établissement devrait demander des preuves que le client est majeur. Si le régime juridique du client l'impose, il vérifie qu'il est également capable. Lorsque le client est une personne morale, les procédures prévoient les documents établissant le pouvoir des personnes physiques la représentant dans tous les actes juridiques. L'équivalent des extraits Kbis du droit français est à ce titre exigé, si nécessaire accompagné d'une " *legal opinion* " sur la capacité des dirigeants.

Lorsqu'il recourt aux coordonnées bancaires préexistantes du client pour l'identifier, l'établissement veille à la fiabilité de cette source d'information, en s'assurant que l'établissement teneur du compte est lui-même astreint à des contrôles approfondis (par exemple du fait de l'existence d'une législation anti-blanchiment efficace dans le pays considéré). Il ne peut de toutes façons s'agir que d'une sécurité additionnelle aux contrôles que l'établissement ne peut pas se dispenser d'effectuer lui-même.

Dans tous les cas, l'établissement doit s'assurer que les collaborateurs en charge des vérifications ont la compétence nécessaire pour détecter raisonnablement des pièces incorrectes ou des faux éventuels.

9.2.1.2. Capacité financière du client (article 19 du règlement n° 97-02)

L'établissement s'assure que ses procédures permettent de déterminer la capacité financière du client à faire face à ses engagements. Ces procédures détaillent les éléments d'information demandés à chaque client, qu'il s'agisse de son patrimoine, de ses revenus et de ses engagements financiers.

Dans le cadre de la lutte contre le blanchiment, ces éléments sont essentiels pour permettre à l'établissement d'apprécier le caractère normal des opérations effectuées par la suite par le client, notamment au regard de la profession dont il a justifié ou de ses revenus.

9.2.2. Formalisme de l'ouverture de la relation

Dans l'attente de la reconnaissance du caractère probatoire des échanges dématérialisés, et notamment de la signature électronique comme moyen de preuve du consentement à un contrat, l'échange de documents papier s'impose.

Dans tous les cas, la convention d'ouverture de compte ou de prestation de services[16], est signée en deux exemplaires, dont l'un est conservé par l'établissement dans le dossier du client prévu à l'article 19 du règlement n° 97-02 du Comité de la réglementation bancaire et financière.

---

16) Qui obéit notamment aux prescriptions réglementaires du Règlement général du CMF (art. 2-4-12 et 2-4-13) dans le cas de services d'investissement.

Il appartient à l'établissement de déterminer, selon son activité et la nature des justificatifs demandés, s'il exige de ses clients des originaux ou des copies. Dans toute la mesure du possible, les originaux des justificatifs doivent être préférés.

Aucune opération ne peut être engagée avec le client ou pour son compte tant que toutes les formalités ne sont pas accomplies.

La convention signée avec le client prévoit les règles relatives :

- à la formation et à la preuve du consentement du client aux opérations engagées avec lui ou pour son compte. La convention précise en particulier les règles de conservation des éléments de preuve, notamment les informations conservées et le délai ;

- au droit applicable et aux juridictions compétentes dans le cas d'une relation transfrontalière ;

- au niveau de qualité du service garanti au client, et aux cas de force majeure dans lesquels cette garantie ne joue plus, ainsi qu'aux modalités d'information du client dans une telle éventualité ;

La convention précise les engagements de l'établissement, et la limite de sa responsabilité, au cas où le dimensionnement du système ne lui permettrait pas de faire face aux volumes à traiter en respectant les performances attendues par le client.

Afin de s'assurer de la véracité des informations données par le client sur son identité et son adresse, l'établissement lui adresse par courrier, dans la mesure du possible avec accusé de réception (ou équivalent dans les pays étrangers), la convention d'ouverture de compte signée, accompagnée des éléments nécessaires au fonctionnement du compte (identifiant et mot de passe, par exemple[17]). Le fonctionnement du compte ne doit pouvoir commencer qu'après la réception par l'établissement de l'accusé-réception lui permettant de s'assurer de la réalité de l'adresse indiquée. En outre, pour obtenir plus de garanties quant à l'adresse indiquée par le client, les établissements pourraient demander à ce dernier la production d'un avis d'imposition qui permettrait de disposer également d'une meilleure appréciation de sa capacité financière.

9.3. Le contrôle permanent des risques clients

Les articles 18 à 24 du règlement n° 97-02 du Comité de la réglementation bancaire et financière fixent les règles relatives à la sélection et à la mesure des risques de crédit.

9.3.1. Règles générales

Les procédures de l'établissement devraient déterminer les modalités de l'application de la " règle des quatre yeux " à toute décision concernant un client ou une contrepartie. Elles définissent les plafonds en-deçà desquels un traitement automatique ou une décision

17) A titre de précaution supplémentaire, l'envoi dissocié de ces deux éléments pourrait être utilement envisagé, pour éviter le risque de leur détournement par un tiers mal intentionné.

individuelle est admis. Dans ces cas, elles identifient les personnes autorisées à prendre ces décisions, prévoient les traces conservées et les modalités d'information des responsables, dirigeants et du responsable du contrôle interne.

9.3.2. Appréciation de la limite de risque qui peut être acceptée sur le client

Les règles relatives à l'appréciation de la limite de risques sont fixées par les articles 19 et 24 du règlement n° 97-02 du Comité de la réglementation bancaire et financière.

Article 24

Les établissements de crédit doivent procéder à tout le moins trimestriellement à l'analyse de l'évolution de la qualité de leurs engagements. Cet examen doit notamment permettre de déterminer, pour les opérations dont l'importance est significative, les reclassements éventuellement nécessaires au sein des catégories internes d'appréciation du niveau du risque de crédit, ainsi que, en tant que de besoin, les affectations dans les rubriques comptables de créances douteuses et les niveaux appropriés de provisionnement.

L'établissement détermine si les éléments d'information fournis par le client doivent ou non être complétés par un entretien.

9.3.3. Suivi du risque sur le client

9.3.3.1. L'article 18 du règlement n° 97-02 du Comité de la réglementation bancaire et financière

Article 18

Les établissements de crédit doivent disposer d'une procédure de sélection des risques de crédit et d'un système de mesure de ces risques leur permettant notamment :

a) d'identifier de manière centralisée leurs risques de bilan et de hors-bilan à l'égard d'une contrepartie ou des contreparties considérées comme un même bénéficiaire au sens de l'article 3 du règlement n° 93605 sus-visé ;

b) d'appréhender différentes catégories de niveaux de risque à partir d'informations qualitatives et quantitatives;

c) de procéder, si elles sont significatives, à des répartitions globales de leurs engagements par ensembles de contreparties faisant l'objet d'une appréciation technique de leur niveau de risque, tel que celui-ci est apprécié par l'établissement, ainsi que par secteur économique et par zone géographique.

9.3.3.2. Code de bonne conduite

La limite de risque convenue entre l'établissement et son client (autorisation de découvert par exemple ou montant maximum des positions sur instruments financiers), diminuée de l'utilisation qui en est faite par celui-ci, doit être, en tenant compte des impératifs techniques et organisationnels, tenue en permanence à jour à la disposition du client.

Il est important que l'établissement mette en place de manière effective un suivi globalisé de l'ensemble des engagements sur un même client ou groupe de clients ou sur une même contrepartie, quel que soit le canal de distribution utilisé (guichets, téléphone, Internet, écrans délocalisés).

Le système d'information doit être organisé de manière à suivre en permanence la totalité des risques pris sur un client. L'existence de dispositifs de contrôle et de filtrage distincts pour chaque canal doit absolument être évitée.

Les procédures de l'établissement déterminent les règles de franchissement des limites. Elles prévoient quelles sont les personnes qui peuvent les autoriser, l'application de la règle des «quatre yeux», les traces qui en sont conservées, ainsi que les modalités d'information des dirigeants et du responsable du contrôle interne sur ces franchissements au cours de la période écoulée. Le dispositif de suivi du risque doit prendre en compte les modalités de retour à une situation normale.

Enfin, des procédures dégradées documentées, prévoyant par exemple un suivi manuel, doivent permettre à l'établissement de maîtriser son risque client même en cas d'indisponibilité totale ou partielle de son système de suivi des limites. Toutefois, un ralentissement des performances du système ne doit pas à lui seul justifier que les instructions des clients soient, pour des raisons commerciales, exécutées sans être soumises au système de contrôle des limites.

9.3.4. Recueil du consentement des clients

L'établissement veille à la sécurité juridique de toutes les opérations engagées avec ou pour le compte de son client. Il s'assure en particulier du caractère certain de son consentement à l'opération, même transmis de manière dématérialisée.

Pour toute opération nouée directement par un canal automatisé, l'établissement doit démontrer que les opérations demandées au client pour manifester son accord suffisent pour éviter toute ambiguïté sur son consentement à l'opération.

L'établissement veillera à ce propos à ce que toutes les informations sur les engagements du client, directs et indirects, soient clairement accessibles et validées par le client. Il s'assurera également que le client ne puisse s'engager par erreur, par exemple à l'issue d'une fausse manœuvre ou en croyant effectuer une simple simulation, par exemple.

CONCLUSION

L'Internet bancaire et financier soulève un certain nombre de questions prudentielles, sur lesquelles tant l'évolution du droit que la coopération internationale apporteront des réponses. Ces évolutions demandent à être suivies attentivement et compléteront utilement les développements de ce Livre blanc.

Le Livre vert de la Commission européenne sur le commerce électronique et les services financiers, qui devrait être publié au premier semestre 2001, apportera des précisions en matière de droit applicable et devrait amorcer une nouvelle phase d'approfondissement du marché intérieur fondée sur une harmonisation des règles de protection des consommateurs et des investisseurs.

En outre, le groupe « banque électronique » du Comité de Bâle continue ses travaux et devrait proposer, dans le courant de l'année 2001, un cadre de coopération entre autorités pour le contrôle des banques électroniques, ainsi que des recommandations en matière de maîtrise des risques.

Enfin, la transposition complète des directives « commerce électronique » et « signature électronique », ainsi que la finalisation des directives « services financiers à distance » et « blanchiment », compléteront le cadre d'exercice des activités bancaires et financières en ligne.

La Banque de France et le Secrétariat général de la Commission bancaire suivront avec attention ces développements.

SOMMAIRE

ANNEXES

MEMBRES DU GROUPE DE TRAVAIL

sous la présidence de M. Alain DUCHÂTEAU,
adjoint au Directeur de la Surveillance générale du système bancaire
Secrétariat général de la Commission bancaire (SGCB)

rapporteur : M. Jérôme DESLANDES,
SGCB, Service des affaires internationales

- SOUS-GROUPE " SECURITE "

- **M. Jean-Claude HILLION,** Inspecteur de la Banque de France, **coordinateur**

- M. DELMAS**, Banque de France**
- M. DESLANDES**, SGCB**
- M. FOUQUET**, Banque de France**
- M. LAURETOU**, Inspecteur de la Banque de France**
- M. SINTUREL**, SGCB**

- M. BOURGOGNE**, Crédit lyonnais, Forum des compétences**
- M. EHNI**, CPR-E*Trade**
- M. DELILLE, **Crédit Agricole Indosuez, Forum des compétences**
- M. GAUDICHEAU**, Banque Hervet, Forum des compétences**
- M. GHIDALIA**, Forum des compétences**
- M. GODARD**, Société générale, Forum des compétences**
- M. HERVOIR**, BNP-Paribas, Forum des compétences**
- Mme JOSSERAND**, Banque Sudameris, Forum des compétences**
- M. de La RENAUDIE**, Crédit Agricole Indosuez, Forum des compétences**
- M. Le BRAS**, Crédit mutuel de Bretagne**
- M. METTEAU, **Banque Sudameris, Forum des compétences**
- M. RIT**, Société générale, Forum des compétences**
- M. RITZ**, BNP-Paribas, groupe " sécurité " du CFONB, Forum des compétences**

- SOUS-GROUPE " CONDITIONS D'ACCES A LA PROFESSION "

- **M. Philippe RICHARD,** adjoint au Directeur des établissements de crédit et des entreprises d'investissement de la Banque de France, **coordinateur**

- M. ANDRIES**, Banque de France**
- M. ARNAUD**, SGCB**

- M. CABOTTE**, Banque de France**
- M. DESLANDES**, SGCB**
- Mme LACHAUD**, Banque de France**

- M. BOUILHOL **, Société générale**
- M. d'HEROUVILLE**, Gide Loyrette Nouel**
- M. LAULANIE**, BNP Paribas**
- M. LANSKOY**, Société générale**
- Mme LESTEL**, Crédit Agricole Indosuez**
- Mme PAOLI**, BNP-Paribas**
- Mme PATEL**, Banque Hervet**
- M. RUELLE**, Crédit lyonnais**
- M. SAINT-ALARY**, BNP-Paribas**
- M. de SAINT-MARS**, AFEI**
- Mme SOUSI, **Professeur de droit à l'Université de Lyon III**

- SOUS-GROUPE " CONTRÔLE INTERNE ET BLANCHIMENT "

- **M. Marc FASQUELLE,** adjoint au chef du Service des entreprises d'investissement et des établissements de marché à la Direction du contrôle du SGCB, **coordinateur**

- Mme CLERC**, SGCB**
- Mme COMMENGE, **SGCB**
- Mme GRENOUILLOUX**, Banque de France**
- Mme GASTAL**, SGCB**
- M. ROCHER, **SGCB**

- Mme BUSSERY**, Banque Hervet**
- M. DECOUVOUX du BUYSSON**, Banque Sudaméris**
- M. d' ESTAINTOT, **Crédit mutuel**
- M. LACHARNAY, **Fimatex**
- M. LEGRIS**, Crédit mutuel**
- M. MILAIR**, BNP-Paribas**
- M. OCHONISKY, **Société Générale**
- M. OLLIVIER, **Crédit mutuel**
- M. PISANI**, Banque Sudaméris**
- Mme SCHRICKE**, Crédit Agricole Indosuez**
- M. VAUGIAC, **Fimatex**
- M. WACK, **Crédit Lyonnais**
- M. WAHL**, Caisse Nationale du Crédit Agricole**

Guide d’élaboration d'une “ politique de sécurité Internet ” du Forum des Compétences

Tous renseignements concernant ce guide et son actualisation peuvent être obtenus auprès du Forum des Compétences.

- Téléphone: 01.48.01.69.69 - Télécopie: 01.48.01.69.68
- Mél: forum@forum-des-competences.org

Guide d'élaboration d'une Politique de Sécurité Internet

Décembre 2000

Groupe de réflexion Sécurité Internet

Guide d'élaboration d'une Politique de Sécurité Internet

A l'usage des responsables de la sécurité des systèmes d'information (RSSI) des établissements de crédit et des entreprises d'investissement

Sommaire

Index des figures

Ce guide d'élaboration d'une politique de sécurité Internet est issu des travaux du Forum des Compétences[1], qui a jugé, fort de l'expérience des établissements qu'il regroupe, du caractère indispensable d'une **politique de sécurité Internet (PSI).** La vocation de ce document est d'aider le Responsable de la Sécurité du Système d'Information, qui souhaite écrire ou adapter la PSI de son établissement.

Réactivité et flexibilité sont les maîtres mots des projets Internet. La sécurité Internet n'est en rien étrangère à ces notions dans la mesure où elle est traitée en amont des projets dans le cadre d'une approche générale de la sécurité des systèmes d'information. Il est ainsi conseillé **de promouvoir au sein des établissements une politique de sécurité** plutôt que traiter en aval la partie sécurité des projets Internet. Il s'agit de proposer aux chefs de projet, an amont, un cadre de référence. L'approche sécurité des projets, pour être efficace, doit être soutenue à tous les niveaux par une volonté d'action, c'est-à-dire une politique.

❖

Une politique –telle la politique de sécurité de l'entreprise, la politique de gestion des réseaux (qui inclut la sécurité des réseaux) la politique de gestion du Système d'Information la politique de gestion de la qualité)- est un ensemble de règles ou de principes consignés dans un document destiné à atteindre un certain nombre d'objectifs.

La politique de sécurité exprimera les objectifs de sécurité d'une part, à partir d'une analyse des risques et, d'autre part, à partir d'une évaluation des contraintes (techniques, humaines, économiques, organisationnelles)[2]. L'analyse des risques provient de l'identification des enjeux, des menaces et des vulnérabilités.

La politique se décline en trois volets :

- définition des règles de sécurité ;
- mise en œuvre des moyens matériels, logiciels, permettant de respecter ces règles et de contrôler leur application ;
- mise en œuvre de l'organisation permettant à chaque entité du groupe de collaborer à la politique générale.

La politique de sécurité Internet présente une caractéristique supplémentaire. Si elle repose sur le même modèle que les autres politiques de l'entreprise (analyse des risques et évaluation des contraintes), elle doit également s'intégrer aux politiques existantes et notamment à la politique de sécurité de l'entreprise et à la politique de gestion des réseaux.

De par la nature même du canal Internet –canal de diffusion d'information fondé sur une interconnexion mondiale de réseaux– la politique de sécurité Internet d'une entreprise s'appuie fortement sur la politique de sécurité des réseaux. Mais pour couvrir l'ensemble des risques que présente Internet, il est nécessaire de prendre également en compte :

[1] Le Forum des compétences est une association regroupant un ensemble significatif d'établissements de la Place : la Banque de France, la Banque Hervet, la Banque SUDAMERIS, BNP-Paribas, le Crédit Lyonnais, le Crédit du Nord, le Crédit Agricole Indosuez, La Poste, SICOVAM et la Société Générale.

[2] A la différence d'un dispositif technique, la politique de sécurité :

- établit la corrélation entre les besoins et les moyens,
- Inclut les aspects organisationnels, comme les procédures de mise en œuvre.

- la sécurité des applications Internet ;
- la sécurité liée à l'utilisation d'Internet par les collaborateurs de l'entreprise ;
- la maîtrise des prestations externalisées.

La vocation du RSSI est de prescrire les processus et règles de sécurité et de s'attacher à les rendre contrôlables. Il n'est pas chargé d'assurer la maîtrise d'œuvre ni la maîtrise d'ouvrage des moyens matériels et logiciels permettant de respecter les règles de sécurité. Il n'est pas non plus contrôleur interne mais participe par son action à la maîtrise des risques de l'établissement. A ce titre, le Livre blanc sur la sécurité des systèmes d'information décrit le RSSI : « disposant de la confiance de la Direction générale, suffisamment technicien mais disposant d'une hauteur de vue qu'un trajet dans les différentes directions opérationnelles lui aura permis d'acquérir, il lui appartiendra d'impulser et de coordonner les actions dont certaines seront entreprises par d'autres directions que la sienne.

Il revient aux responsables opérationnels d'exercer le contrôle interne de premier niveau et de s'assurer du respect des diligences et procédures prescrites par la PSI. Le contrôle interne de second niveau est de la responsabilité de la fonction d'audit/inspection. Le contrôle du troisième niveau incombe aux instances externes à l'établissement, dont les autorités de tutelle.

❖

Ce guide est une trame destinée à être adaptée par le responsable de la sécurité des systèmes d'information (RSSI) de chaque établissement. Le présent document n'établit pas de PSI applicable à tous les établissements de crédit ou entreprises d'investissement. Chaque établissement, voire chaque type d'application a des enjeux qui lui sont propres et qui évoluent dans le temps.

La première partie a pour objet de « délimiter le périmètre de la PSI ». Avant de se lancer dans la rédaction d'une PSI, il est en effet légitime de se demander pourquoi les documents généraux de sécurité ne sont pas tout simplement appliqués. En d'autres termes, ce guide propose une démarche de travail, invitant le RSSI à reprendre les éléments de sécurité des documents existants et à les positionner vis-à-vis d'Internet.

La deuxième partie présente l'élaboration de la PSI en tant que projet mené par le RSSI, qui sera confronté à un ensemble de questions : quels seront les participants à la rédaction de la PSI, quel en sera le support, quel calendrier mettre en place ?

Le guide est accompagné d'un support de rédaction thématique. Les membres du groupe de travail du Forum des compétences se sont efforcés de traiter les problèmes de façon générique, sous l'angle des principes (organisationnels, méthodologiques) et non de façon technique[3], afin de conférer au guide une certaine pérennité. Cette partie illustre les thèmes abordés en faisant ressortir les points qui semblent prioritaires.

Ce support est complété par un ensemble de fiches techniques qui approfondissent les sujets relevés dans l'étude thématique.

[3] La partie technique fera l'objet d'annexes ultérieures, qui seront autant que possible tenues à jour par les contributeurs du groupe sécurité Internet du Forum des Compétences.

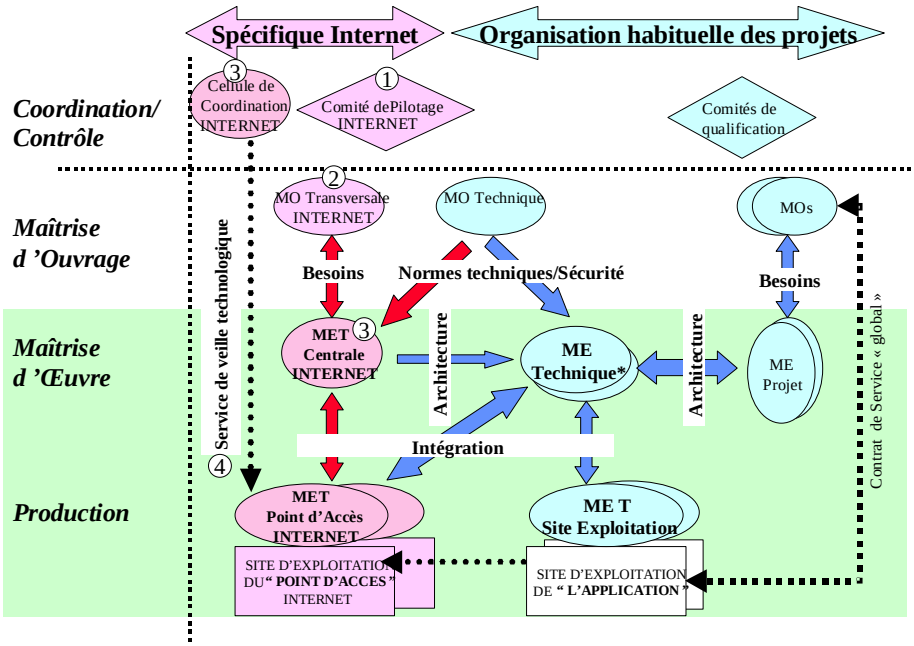
1. Délimitation du périmètre

Tout en s'inscrivant dans la ligne de la politique de sécurité en vigueur, la PSI permet de poursuivre des objectifs spécifiques :

- **la continuité** : les projets Internet tendent à privilégier la réactivité à la pérennité. Mais l'ensemble du dispositif Internet d'une banque doit être durable et sûr. A ce titre, des mesures spécifiques sont à mettre en place. A titre d'exemple, les outils du moment, adoptés à l'occasion d'un projet, doivent être suivis par un service de veille sécuritaire.
- **la cohérence** : les risques résiduels qui sont acceptés par une équipe de projet[4] doivent être cohérents avec le niveau de risque accepté par la PSI.
- **la coordination** : la rapidité d'évolution des nouvelles technologies ainsi que leur diversité rendent nécessaire la coordination des approches. Il s'agit de vérifier, si possible dans le cadre d'un schéma directeur, que la solution du moment est adaptée non seulement aux exigences actuelles mais également aux évolutions programmées.
- **l'expertise** : en accompagnement d'une organisation Internet dédiée, résultat de l'expérience de plusieurs projets, un pôle d'expertise en sécurité doit être constitué afin de capitaliser l'expérience acquise et d'en faire bénéficier les projets à venir.
- **la réactivité :** la rapidité de propagation d'une menace à travers Internet nécessite de se doter d'une structure de réaction adaptée aux incidents.

Ces principes, s'ils sont déjà légitimes dans la politique de sécurité générale, revêtent une ampleur nouvelle quant à l'Internet. L'objet de la définition du périmètre de la PSI est de répondre efficacement à ces enjeux.

1.1. Prendre part à l'organisation Internet



Plutôt que de partir des documents traditionnels en matière de sécurité, et d'examiner s'ils s'appliquent à Internet, il est conseillé au RSSI de prendre part à l'organisation Internet de son établissement. Le RSSI doit faire l'effort d'y participer, et ne pas attendre que les chefs de projets viennent le solliciter[5].

Figure 1 : Exemple d'organisation Internet

[4] L'équipe de projet comprend le responsable bancaire, la maîtrise d'ouvrage et la maîtrise d'œuvre.

[5] La réactivité demandée aux projets combinée au caractère exceptionnel que prennent ces projets pourraient conduire à un affranchissement des règles usuelles de sécurité (alors que l'interconnexion à Internet devrait conduire à un durcissement de ces mêmes règles) .

1.1.1. Les comités orientant l'activité Internet

(Voir Figure 1, mention ←)

La politique de sécurité Internet est directement influencée par les choix en matière de stratégie, de protection d'applications, de point d'accès, de choix de matériel, etc., émanant des Comités de pilotage et des différentes réunions. Un responsable de la sécurité doit y être étroitement associé pour veiller à ce que ces projets ou ces décisions restent cohérents avec les objectifs de l'entreprise.

- ***Note d'organisation Internet***

Cette note propose des structures qui permettront à chaque direction de désigner ses propres représentants aux différentes instances envisagées. Un ou plusieurs **comités de pilotage** Internet peuvent être constitués par la note d'organisation :

- Comité de pilotage Internet : Coordination des activités Internet au sein du groupe, pilote, validation des projets, suivi des budgets alloués par la direction, prise des décisions stratégiques (comme le nombre de point d'accès à Internet).
- Comité opérationnel : Suivi de la qualité du site, d'exploitation, décisions opérationnelles, décisions concernant l'infrastructure (ajouter un service, de nouvelles fonctions).

Le RSSI doit être représenté au moins au comité opérationnel.

- ***Réunion des filiales*** *(françaises, internationales)*

Il s'agit de vérifier le périmètre d'application de la politique : à partir de quel moment une filiale appliquera une politique Internet commune. A ce titre, la partie 1.3 développe les notions de réseaux internes, d'entités associées et de partenaires,

- ***Réunions maîtrise d'ouvrage/maîtrise d'œuvre*** *(Information mutuelle sur les projets des services, Point d'avancement sur la mise en œuvre des nouveaux)*

Eventuellement, ces réunions sont dissociées par MO/ME, points d'accès, projets ou famille de projets. Ces réunions peuvent être l'occasion pour les responsables de la sécurité de faire adopter des normes communes ou de recenser des besoins nouveaux.

1.1.2. Les entités contribuant à la sécurité Internet

- ***MO transversale Internet*** Voir Figure 1, mention ↑

Responsable de la coordination des projets, cette entité pourra mettre en évidence des besoins de sécurité communs aux différents projets (besoins qui pourront donner lieu à la création de « services de sécurité »).

- ***Cellule de coordination - ME transversale Internet*** Voir Figure 1, mention →

Cette entité est chargée de la réalisation des services communs Internet. La cellule de coordination recueille les besoins et diffuse les modèles (architectures, documents), tandis que la ME transversale Internet conçoit les services communs.

- ***Service de veille technologique*** Voir Figure 1, mention ↓

Il peut fournir des informations sur les nouvelles pratiques. Réciproquement, les responsables de la sécurité peuvent demander à ce service de faire des recherches particulières la concernant.

1.1.3. Partie sécurité des projets Internet

Comme pour toute application jugée sensible par la banque, il est nécessaire de constituer un dossier de sécurité ou un manuel de sécurité consacré à l'Internet, dont le caractère sensible résulte de la connexion d'une application du réseau d'entreprise au réseau mondial. Ces documents doivent viser explicitement la PSI. Ces documents sont par ailleurs un révélateur de l'application effective de la politique et donc un moyen de vérifier son efficacité opérationnelle.

- ***Dossier sécurité***

Le dossier de sécurité a pour objet d'analyser les risques propres à un système d'information (en général, une application développée à l'intention d'un responsable bancaire). Dans le dossier de sécurité, sont abordés successivement :

- L'expression des besoins de sécurité (enjeux et ressources à protéger)
- L'analyse des risques
- La description du système (avec ses moyens de protection)
- Les risques résiduels

Le dossier de sécurité est constitué par l'équipe de projet (responsable bancaire et équipe informatique), avec le concours de la structure spécifique à Internet (MO Internet, ME Internet).

- ***Manuels de sécurité***

A destination des services d'exploitation, ils définissent l'infrastructure du point d'accès ou l'exploitation d'une application dans un service au titre de la sécurité. La multiplication des applications Internet sur une plate-forme d'exploitation rend rapidement indispensable l'existence d'un manuel de sécurité valable pour l'ensemble de la plate-forme. Les exploitants pourront consulter ce document de référence lors de la mise en œuvre d'un nouveau projet et maintenir ainsi une cohérence d'ensemble.

1.2. Approfondir la politique de sécurité générale

1.2.1. Textes et documents relatifs à la sécurité des réseaux

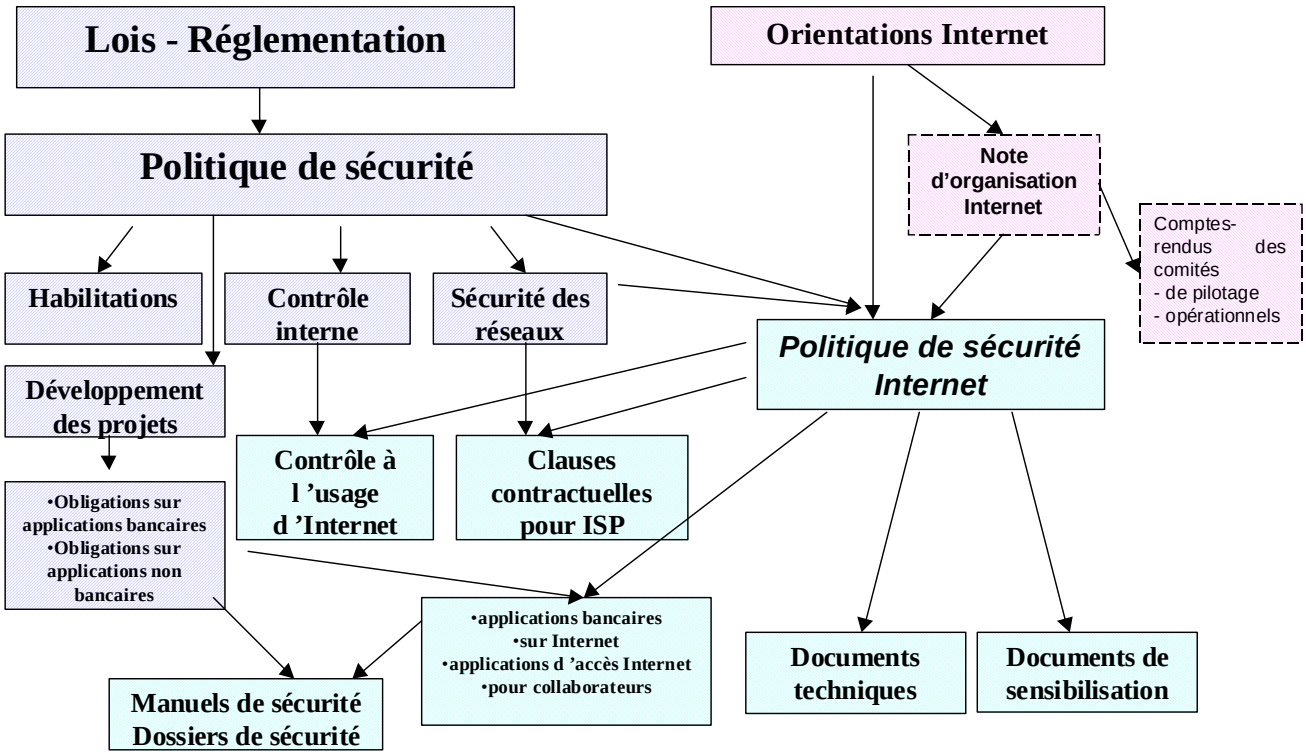


Figure 2 : Hiérarchie des textes et documents

Ces textes et documents comprennent un ensemble de règles de sécurité édictées et déclinées en fonction de chacune des typologies, s'agissant de l'architecture et des modes de fonctionnement. La distinction porte notamment sur le cas des filiales.

- ***Politique de sécurité des réseaux***

Ce texte (ou ensemble de textes) traite des outils mis en œuvre pour assurer la sécurité au niveau de l'ensemble du réseau. Il fait état du recensement des outils (routeurs, éléments filtrants, partition de la DMZ en zones fonctionnelles, outils de détection d'attaques, configuration des éléments filtrants, consolidation des journaux) ainsi que de leur positionnement dans l'infrastructure réseau et de leur administration :

- ***Fournisseurs de moyens réseaux***

Il s'agit de définir les contraintes d'exploitation et d'organisation auxquelles doivent être soumis les fournisseurs pour assurer un niveau de sécurité et une qualité de service sur le réseau, définis par la banque.

Les clauses à respecter dans le volet sécuritaire du contrat ISP couvrent notamment :

- La possibilité pour l'*Internet Service Provider* (ISP) de filtrer un flux sur ses routeurs
- L'engagement sur un temps de transit sur le segment Banque-Provider
- La possibilité pour l'ISP de contrôler l'accès pour détection de flux anormaux

- Les clauses adaptées à certains sites et toute autre permettant une couverture contractuelle.

1.2.2. Textes relatifs à la sécurité des applications

- ***Textes relatifs à la sécurité liée à l'utilisation d'Internet par les collaborateurs de l'entreprise***

Ces textes posent les règles déontologiques vis-à-vis du risque Internet. A ce titre, tout collaborateur est informé des risques liés à l'utilisation d'Internet par une Charte ou une Annexe au Règlement intérieur. Ces textes présentent une information générale sur Internet et posent les principes, qui président à son utilisation par un collaborateur de l'entreprise (définitions - références aux textes sur la messagerie - conditions et modalités d'accès par type de service - règles et obligations d'utilisation - gestion et contrôles).

- ***Applications bancaires***

L'infrastructure de sécurité est présentée sous forme de notes techniques et/ou de recommandations relatives au contrat. Elle comprend la définition de l'architecture, un énoncé de règles extraites de la Politique de Sécurité des Réseaux IP, une mise en perspective de ces règles s'agissant plus particulièrement des applications bancaires et couvre :

- la sécurisation de l'interconnexion du serveur Web avec un réseau extérieur,
- la sécurisation des communications entre le frontal et le système d'information du site,
- la protection du serveur Web,
- la sécurisation des communications entre le client et le serveur Web,
- les choix du fournisseur d'accès à Internet,
- les moyens d'exploitation des systèmes et procédures,

avec, pour chaque partie sécurité, un exposé de la solution actuelle, de ses évolutions et des règles de sécurité. C'est dans le paragraphe consacré à l'évolution que la spécificité des « Applications bancaires » est énoncée.

- ***Applications non-bancaires***

L'infrastructure de sécurité est présentée sous forme de notes techniques et/ou de recommandations relatives au contrat. Elle porte sur la définition d'architecture, sur l'énoncé des règles extraites de la Politique de Sécurité des Réseaux IP et une mise en perspective de ces règles s'agissant plus particulièrement des applications non-bancaires.

1.2.3. Textes généraux de sécurité nécessitant une déclinaison propre à Internet

- ***Contrôles applicables à l'usage d'Internet***

Dans le prolongement de la Charte d'Utilisation, il s'agit, par un ensemble de textes, de définir les types de contrôle, et leurs objets, ainsi que leur sanction éventuelle par une autorité. Ces textes portent sur :

- les statistiques messagerie et génération d'états (en consommations et domaines),
- les statistiques Web et génération d'états (en consommations et domaines),
- la gestion des listes noires,
- l'exploitation des états de suivi.

Ce dispositif doit être conforme aux cadre juridique en vigueur relatif à la surveillance des salariés et au respect de leur vie privée.

- ***Textes relatifs à la sécurité des applications Internet***

Les volets sécuritaires de la conduite de projet et de la relation MO/ME sont ici détaillés à l'intention de chaque Chef de Projet dans sa relation avec les équipes Sécurité (demandes - préconisations - recommandations - validation de propositions - ...) et les règles de développement des applications Internet sont précisées.

1.3. Situation par rapport à intranet et extranet

1.3.1. Internet et les réseaux IP privés

Il existe trois catégories d'utilisation du protocole de communication TCP/IP :

- **Intranet** : communications au sein du réseau local d'entreprise ou assimilé (réseaux locaux reliés par des liens privés)
- **Internet** : communications au travers du réseau Internet. Les participants à ce réseau sont quasiment anonymes et innombrables. Pour cette raison, l'Internet est qualifié de réseau hostile.
- **Extranet** : communications entre entités par l'entremise d'un réseau public, par exemple Internet.

- ***Champ d'application de la PSI***

La Figure 3 : Intranet, extranet et Internet présente les différents points de contact, de raccordement et d'isolement entre Intranet, Internet et Extranet. A travers cet exemple de politique, intranet ne fait pas partie du champ de la PSI, et doit être traité par la politique de sécurité des réseaux (voir partie 1.2.1) ou par un texte particulier.

En revanche, l'extranet dès lors qu'il passe par Internet entre dans le champ d'application de la PSI.Les liens externes IP ne sont pas inclus dans la PSI. Il est vivement conseillé qu'ils soient traités par la politique de sécurité des réseaux.

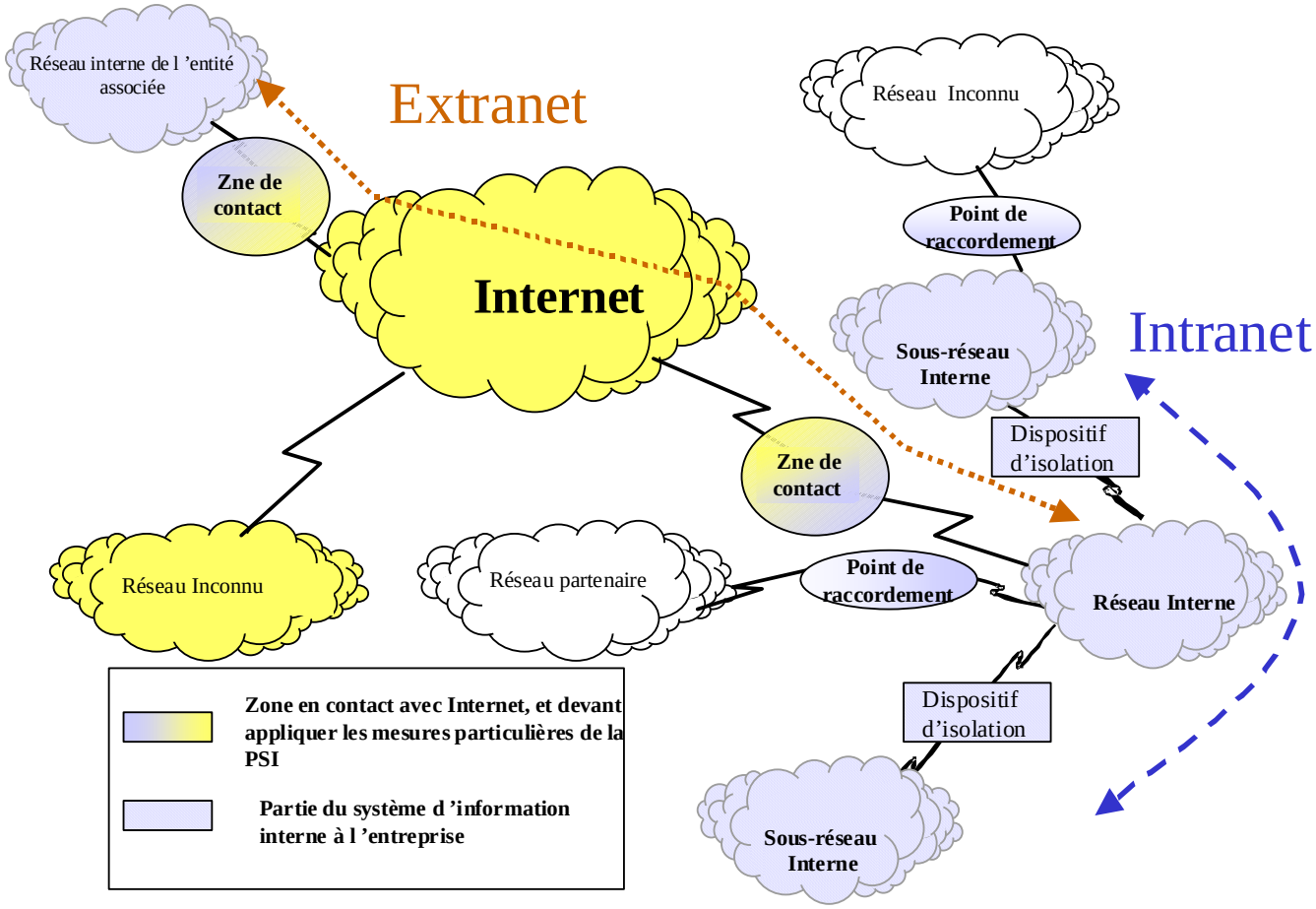


Figure 3 : Intranet, extranet et Internet

Cet exemple d'application de la PSI induit plusieurs dispositions :

- Il existe trois catégories de zones de contact IP :
    1. entre deux réseaux internes (dispositif d'isolation),
    2. entre un réseau interne et un réseau externe (point de raccordement),
    3. entre un réseau interne et Internet (zone de contact Internet).
- L' extranet passant par Internet est traité au même titre que toute connexion Internet
- Il est supposé qu'un réseau partenaire ou extérieur ne redirige pas les flux Internet vers le réseau interne de votre établissement.

1.3.2. Evolution vers des zones de confiance

- ***Les limites de la typologie Internet-extranet-intranet***

A ce jour, il est conseillé de s'appuyer sur les définitions et les distinctions énoncées à la partie précédente. Les systèmes internes des établissements sont interconnectés depuis suffisamment peu de temps pour que ce phénomène fasse l'objet de mesures particulières et identifiées.

Toutefois, **l'homogénéité des protocoles (IP et ses dérivés), rend possible le passage de connexions d'intranet vers Internet ou d'Internet vers le réseau interne via un réseau tiers**. Dans cette perspective, le RSSI sera conduit à considérer sur le même plan toute interconnexion avec un réseau extérieur. En d'autres termes, il n'est plus possible de fonder une politique sur la typologie Internet-extranet-intranet, typologie à laquelle la notion de réseaux affiliés

et/ou non affilié doit être préférée dans la mesure où tout réseau affilié nécessite les mêmes moyens de protection sur le réseau interne.

- ***Présentation, à titre d'exemple, d'un modèle fondé sur l'application de la politique de sécurité des réseaux***

La politique de sécurité définie dans le présent guide couvre :

1) Le fonctionnement, l'architecture et les règles d'usage du réseau interne et des ressources qui y sont connectées (serveurs, postes de travail, équipements « réseau » internes).
2) Idem pour les réseaux d'entités associées.
3) Les interfaces (zones de contact) avec les réseaux partenaires ; les principes généraux d'interface entre les réseaux partenaires et les réseaux inconnus.
4) Les interfaces (zones point de contacts) avec les réseaux d'entités inconnues.

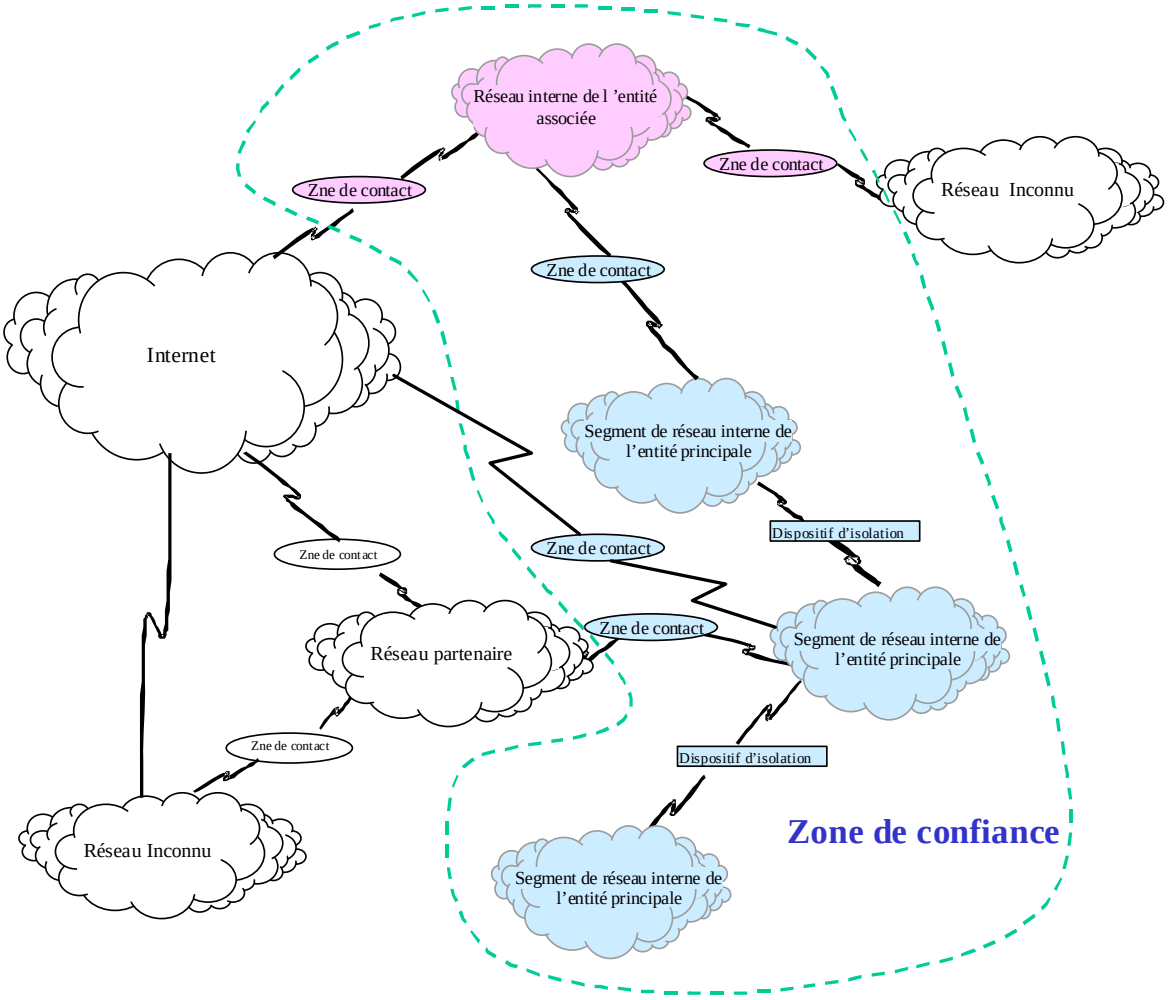


Figure 4 : Réseaux structurés en zone de confiance

Quatre types de domaines peuvent être identifiés :

1. Réseau interne de l'entité de référence (entité qui établit la politique de sécurité): Il s'agit de l'ensemble des réseaux locaux d'une entité juridique unique (domaine de responsabilité unique). Il peut s'agir de réseaux locaux reliés entre eux par un réseau privé.

2. Réseaux d'entités associées. Il s'agit de l'ensemble des réseaux locaux d'une entité juridique distincte de l'entité de référence (en général, des réseaux appartenant à des filiales contrôlées

par l'entité de référence). Le contrôle interne de l'entité de référence s'applique au sens du règlement n° 97-02 du Comité de la réglementation bancaire et financière relatif au contrôle interne. Selon les établissements, les entités affiliées sont autonomes dans la gestion de leurs réseaux ou s'en remettent à l'entité de référence.

3. Réseaux d'entités partenaires. Il s'agit de l'ensemble des réseaux d'une entité juridique distincte de l'entité de référence (en général de réseaux appartenant à des filiales contrôlées).

Même si le contrôle interne de l'entité de référence s'y applique au sens du règlement n° 97-02 du Comité de la réglementation bancaire et financière relative au contrôle interne, le réseau de l'entité de référence et le réseau de l'entité associée constituent des **périmètres de sécurité distincts.**

4. Réseaux d'entités inconnues : Il s'agit de réseaux tels qu'Internet ou tout réseau de sociétés tierces hors de toute relation de contrôle.

1.4. Interconnexion par réseau commuté (RTC, RNIS)

Si la politique de sécurité est ou est perçue comme trop contraignante, la tentation est forte de s'y soustraire en la contournant en utilisant, par exemple, des moyens « parallèles » de connexions Web telles les connexions commutées.

Malgré leur aspect furtif, les interconnexions par RTC ou Numéris à Internet sont dangereuses. Réalisées sur des postes de travail connectés au réseau de l'entreprise elles peuvent être la source d'intrusions profondément dommageables. Même mis en œuvre pour un usage précis, ces dispositifs de connexion commutée sont généralement faciles à détourner pour accéder à Internet.

L'utilisation pour accéder au Web de connexions commutées à partir de postes non connectés au réseau de l'entreprise pourra être envisagée en considérant :

- La nécessité de dédier ces postes à cette fonction. Ils doivent disposer d'un outil antivirus à jour et n'héberger aucune donnée sensible ;
- La difficulté à maintenir ces postes isolés du réseau d'entreprise. La tentation est grande pour l'utilisateur de réaliser une connexion pour, par exemple, transférer les données téléchargées depuis Internet ;
- La difficulté à administrer ces machines, à commencer par assurer leur recensement ;
- La difficulté à en contrôler l'usage.

Il est plus pertinent d'envisager l'accès Internet à partir des postes dédiés sur des infrastructures réseau dédiées interconnectées au moyen de solutions sécurisées.

1.5. Hébergement de services chez un prestataire

Où qu'il soit hébergé, le service est un service de l'entreprise qui l'expose à un ensemble de risques. La décision d'externaliser un service n'affranchit pas l'établissement du respect de ses obligations prudentielles, posées notamment par le règlement n° 97-02 du Comité de la réglementation bancaire et financière. En conséquence, les exigences de sécurité doivent être étendues au prestataire.

En particulier,

- Le service doit être mis en place par des ingénieurs compétents et des spécialistes de la sécurité en environnement Internet ;

- Des tests exhaustifs doivent être réalisés ;
- La surveillance du service doit être assurée avec des moyens techniques et humains adéquats ;
- Un audit périodique et indépendant doit être réalisé sous le contrôle de l'entreprise ;
- La banque doit intégrer au contrat une clause d'audit lui permettant de diligenter des missions de son service interne d'audit/inspection.

Les dispositions applicables à l'hébergement de services chez un prestataire sont développées dans la fiche technique N°19 « Hébergement extérieur: clauses nécessaires au contrôle du niveau de sécurité ».

2.Elaborer et mettre en œuvre la politique de sécurité INTERNET

La politique de sécurité Internet est issue, comme le présente la figure 2 de deux sources :

- la réglementation interne et l'organisation générale de la sécurité,
- les dispositions et l'organisation spécifiques à Internet.

En conséquence, la Politique de Sécurité Internet est un document riche dont la prise en compte par l'entreprise nécessitera un accompagnement adapté, qui peut s'avérer difficile à mettre en œuvre en pratique.

Le présent chapitre identifie les composantes du véritable **projet** que constituent, non seulement la rédaction de la PSI, mais également sa validation, sa diffusion, son application et le contrôle de sa mise en œuvre.

2.1. Préparation du projet jusqu'à la date de lancement

La date de lancement correspond au moment où la Direction Générale publie une note mentionnant :

- La nécessité de disposer d'une Politique de Sécurité Internet
- Le champ d'application de cette politique (en termes généraux)
- L'entité responsable de sa rédaction
- L'entité (ou les entités) responsables de la validation de la PSI avant son adoption
- L'entité responsable de son adoption (il est souhaitable qu'il s'agisse de la Direction Générale elle-même)

Avant même la parution de cette note, il est indispensable que le RSSI prépare le projet, dont les paragraphes suivants proposent un fil conducteur.

2.1.1. Constitution d'une documentation de référence

La documentation de référence doit être constituée en amont, afin de motiver l'adoption d'une PSI et de préciser son contexte réglementaire, technique et financier.
• Documents Internes à l'entreprise

1. **Directives d'Organisation**
   Elles fixent les missions et les responsabilités de différentes entités de l 'entreprise.

2. **Règlement Intérieur**
   Il fixe les obligations des salariés notamment en termes de comportement et de sécurité

3. **Documentation normative**
   Le secrétariat général tient une liste des circulaires et instructions applicables.

4. **Organigrammes fonctionnels de l'entreprise**
   Les organigrammes fonctionnels permettent de quantifier l'effort de diffusion et l'impact financier et organisationnel de la PSI.

5. **Documentation " Informatique "**
   Il s'agit du schéma directeur " Système et Réseau de la méthodologie de gestion de projet des schémas d'architecture. Ces éléments apportent une vue précise de l'existant et permettent d'évaluer l'écart entre la situation présente et la cible fixée par la PSI. Les objectifs de la PSI et/ou le calendrier d'application seront adaptés en conséquence.

6. **Documentation " Activités Internet "**

- ***Documentation de place (France)***

La PSI doit être compatible avec les règlements et recommandations des autorités de tutelle. Lors de l'exposé des risques engendrés par l'absence de PSI, le risque d'infraction de ces règlements doit être souligné.

1. Le livre blanc sur la sécurité des systèmes d'information de la Commission bancaire
2. La réglementation du CRBF (97-02)
3. La réglementation du Conseil des Marchés Financiers n° 99-07 notamment
4. Le Code Pénal (Atteintes aux droits de la personne résultant des fichiers ou de traitements informatiques : art 226-16 à 226-24, atteintes aux systèmes de traitement automatisés de données : art 323-1 323-7).
5. Le Livre blanc sur les conséquences prudentielles de l'Internet de la Commission bancaire et de la Banque de France
7. Les recommandations du Comité de Bâle en matière de sécurité des Banques électroniques (à venir)
8. Profil de Protection d'un serveur Web transactionnel bancaire (à venir)

- ***Documentation Externe (Global)***

1. Site Security Handbook RFC 2196 Cette RFC se veut uniquement informative mais peut servir de modèle à l'élaboration des règles de sécurité logique d'un site.

2. Code of Practice for Information Security Management British Standard BS7799

3. Information Security Guidelines For Financial Institutions, Draft 98/11/24, ISO/TC68 13569

4. Internet access policy : Deterring Abuse, Gartner Group 98/04/10

5. Exemples de PSI

   - Réelles :en provenance d'établissements de crédit ou d'entreprises d'investissement similaires
   - Modèles : issus de la littérature, d'organismes de normalisation, etc…

- ***Bibliographie diverse***

- Statistiques relatives aux sinistres
- Revues de presse
- Relations d'incidents graves

2.1.2. Consultation préliminaire des parties intéressées

En préalable de la rédaction de la politique de sécurité Internet, il est recommandé de conduire les actions suivantes :

- Rassembler les préoccupations des différents acteurs
- Sensibiliser ces interlocuteurs au caractère majeur de l'opération
- Recenser les urgences afin de déterminer un calendrier de diffusion de versions intermédiaires de la PSI (cf. partie jalons de votre projet, p9)
- Permettre à ces interlocuteurs d'anticiper, dans une certaine mesure, la prise en compte des règles qui apparaîtront probablement dans la PSI (budget, allocation de personnel, définition de projets)

2.1.3. Communication à la Direction Générale

- ***Objectifs de la PSI***

Le chapitre 1.2.1 du *Support pour l'élaboration d'une Politique de Sécurité Internet* fournit différentes présentations possibles des objectifs de la PSI. Il est important de mentionner les résultats attendus de son application. En particulier :

- Une baisse de l'exposition aux risques ;
- Une évaluation mieux étayée du degré de risque ;
- Une meilleure audibilité de l'établissement ;
- Une rationalisation des architectures d'où une diminution possible des coûts.

Le chapitre 1.2.2 du *Support pour l'élaboration d'une Politique de Sécurité Internet* détaille les risques associés à l'absence d'une PSI.

- ***Caractéristiques générales de la PSI***

La consultation préliminaire des parties intéressées permet de définir un périmètre d'application de la politique de sécurité (voir le *Support pour l'élaboration d'une Politique de Sécurité Internet*, §1.2.3), c'est-à-dire :

- Le degré de précision de ses règles, leur teneur (principes généraux seulement, mesures générales, mesures d'application) ;
- Les variantes ou cas particuliers imposés par l'observation du terrain (tel que le champ d'application : établissement seulement, filiales de droit étranger, filiales de droit français, succursales en France, à l'étranger) ;
- Les thèmes couverts par la PSI et le rythme d'application (quelle doit être la périodicité de revue de ce texte) ;
- Le cadre général (organisationnel et réglementaire) dans lequel s'inscrit la politique de sécurité Internet

- ***Jalons du projet***

Les jalons importants du projet doivent être communiqués à la Direction :

- Soumission, pour validation
- Calendrier d'éventuelles versions intermédiaires
- Annonce officielle (média électronique, support papier)

- Traductions éventuelles
- Réalisations des objets (procédures, organisations, documentation, méthodes) mentionnés ou impliqués par la PSI
- Réalisation et/ou suivi des opérations associées à la PSI (nominations, recrutements, développements de logiciels et tableaux de bord, etc…)
- Opérations de communication et de diffusion de la PSI et de la documentation connexe

- ***Impact prévisible de la PSI***

Pour pouvoir décider des suites à donner à la démarche, la Direction doit pouvoir estimer l'impact à court et à moyen terme de l'application de la PSI. A ce titre, il s'agit de mesurer précisément le coût de réalisation du projet et ses implications et de mettre en regard, par une analyse coûts avantages, l'impact de la non-réalisation en termes de vulnérabilités.

Cet impact peut être financier, technique, fonctionnel (l'établissement ne sera pas en mesure de satisfaire telle ou telle attente du personnel ou des clients), organisationnel et marketing.

2.2. Conduire le projet

L'établissement de la PSI devra être inséré dans le cadre de **la méthode de conduite de projet** de l'établissement. A titre d'illustration, le RSSI devra suivre l'ensemble des tâches qui concourent à la réalisation de la PSI, organiser le suivi et la communication de ce travail.

De la publication de la PSI résultera un ensemble de documents nécessaires à sa mise en application :

- Description de procédures

  Par exemple, la PSI spécifiera que « *tout courrier électronique comportant des informations relevant du secret bancaire, sera chiffré ; des dispositions techniques seront prises pour que les clefs de chiffrement/déchiffrement ne soient pas transmises par le même canal que le courrier*». Il est clair que cette règle intriguera les personnes chargées de la messagerie électronique ; elles attendront légitimement que des précisions techniques soient fournies. Afin d'éviter que ne soient imaginées, en parallèle, de multiples solutions, une entité devra être en mesure de répondre aux questions dans un délai très bref après l'adoption de la PSI.

- Description de profils de postes

  Par exemple, la PSI pourrait spécifier que « *le dispositif d'accès à l'Internet sera piloté par une personne ayant des compétences adaptées à cette mission.*» ; Dans les jours qui suivront la diffusion de la directive, des précisions sur les compétences requises seront demandées. Il s'agit d'anticiper ces questions.

- Listes de prestataires recommandés

  Par exemple, la PSI pourrait spécifier que « *Les projets […] devront être confiés à des sociétés répondant à certains critères…*» ; Ici aussi, il faudra être en mesure de répondre aux sollicitations en fournissant des listes de critères ou des listes de sociétés.

- Description de méthodes

  Par sa simple existence, la PSI engendrera des projets connexes qu'il convient de ne pas négliger pour ne pas compromettre l'application de la directive.

Il est primordial que soit consultable, dès la diffusion de la PSI, un échéancier de mise en conformité de l'existant. Sans cet échéancier, la PSI sera difficilement réalisable. Cette information est très attendue des maîtrises d'ouvrage, chefs de projets, responsables d'exploitation, architectes de solutions.

Support pour l'élaboration d'une Politique de Sécurité Internet

Traitement par thèmes

Sommaire

Ce document accompagne le document principal « Guide d'élaboration d'une Politique de sécurité ». Comme son titre l'indique, il constitue un support pour l'élaboration d'une Politique de Sécurité Internet. Chaque chapitre de ce document présente un thème à considérer lors de la rédaction de la PSI.

Tous les chapitres ont la même structure :

- Le thème abordé y est d'abord défini et expliqué(§ Objet),
- Afin de marquer l'importance de ce thème, des exemples de risques encourus en cas de non traitement du thème sont donnés (§ Risques associés),
- Les recommandations qui devraient ressortir de la PSI sont présentées en distinguant deux niveaux de priorité. Ces deux niveaux sont une appréciation du Groupe de Travail mais la pertinence du niveau de priorité est laissée au RSSI de l'établissement. Les recommandations fortement prioritaires sont mises en évidence à l'aide d'une calligraphie différente (§ Recommandations).
- Des fiches techniques détaillées dans le troisième document « Fiches Techniques » accompagnent les développements thématiques et sont référencées dans le chapitre afin de dissocier les aspects techniques des thèmes traités (§ Renvoi sur fiches techniques).

Le document ne contient pas, volontairement, d'exemple de rédaction.
En revanche, il est possible d'obtenir une communication d'exemples de textes de politique de sécurité Internet, auprès des établissements eux-mêmes ou auprès des organismes reconnus dans la profession.

1 Présentation de la politique de sécurité Internet

1.1 Objet

La première partie de la PSI doit donner succinctement les orientations principales, ci-après explicitées.

1.1.1 Fixer les objectifs de la politique

- disposer par la PSI d'un référentiel commun (ensemble de principes et de règles) qui permettra aux différentes entités de l'établissement de se positionner vis à vis de la politique ;
- rappeler les principes de continuité, de cohérence, de coordination, d'expertise et de réactivité, qui doivent présider à toute PSI.

1.1.2 Ancrer la PSI par rapport au règlement de l'entreprise.

La PSI doit s'appuyer sur les textes généraux de sécurité et les dispositions prévues pour Internet (voir chapitre 1.2 du Guide d'élaboration d'une PSI). Il convient de choisir soigneusement les textes de référence de la PSI ainsi que les textes devant être modifier afin qu'ils référencent eux-mêmes la PSI.

1.1.3 Champ d'application

La PSI doit particulièrement s'attacher à définir son champ d'application, c'est-à-dire :

- traiter les cas d'infogérance ou de postes isolés comme énoncé dans la partie 1.4 du Guide d'élaboration d'une PSI ;
- fixer le périmètre et la portée de la politique par rapport aux filiales. La portée de la PSI doit correspondre :
  - o à la politique de sécurité générale (document fondateur sur l'organisation de la sécurité, quand elle existe),
  - o à la politique de sécurité des réseaux (voir la partie 1.2 du Guide d'élaboration d'une PSI)
  - o au texte fixant l'organisation Internet ;
- différencier la partie « politique » (organisation, procédures de réalisation, de contrôle …) de la partie « technique » qui est annexée et qui nécessitera une mise à jour plus fréquente.

1.2 Risques associés

1.2.1 En l'absence d'un référentiel, il est difficile d'apprécier le niveau de sécurité Internet

En l'absence de normes de sécurité admises par tous, il est difficile de formuler une appréciation sur le niveau de sécurité d'une application, ou d'un centre d'exploitation. Or, l'interconnexion des systèmes au sein d'un établissement rend indispensable cette vision globale.

1.2.2 Sans traitement des cas d'exception, la PSI peut être contournée par l'infogérance ou les postes isolés

Ces risques sont développés dans la partie 1.4. La PSI est d'autant plus efficace qu'elle est incontournable.

1.2.3 Si le champ d'application de la PSI ne s'étend pas aux filiales, celles-ci peuvent constituer un vecteur de risque

Le champ d'application de la PSI et la notion de réseau de confiance (ces notions sont développées dans la partie 1.3.2) doivent être cohérents. Si on applique des dispositions particulières sur Internet et qu'une entité affiliée ne les respecte pas, elle remet en cause la cohérence du dispositif d'ensemble.

1.3 Recommandations

- Enoncer les objectifs de la politique.
- Faire référence à la politique de sécurité générale, à la politique de sécurité des réseaux et éventuellement au texte fixant l'organisation Internet.
- Le champ d'application de la PSI doit s'étendre aux différentes instances de l'établissement (si celui-ci n'est pas défini dans la politique de sécurité des réseaux).
- La PSI ne doit pas comporter de clauses techniques.

2 Organisation pour appliquer la PSI

2.1 Objet

Afin de permettre **l'application effective** d'une politique de sécurité Internet, il est nécessaire d'expliquer clairement les responsabilités des différents acteurs dans l'application des mesures mises en place. Le document doit proposer des recommandations pour donner aux acteurs les moyens d'assurer leurs responsabilités, et ce dans la durée.
Les recommandations à caractère obligatoire devraient avoir fait l'objet d'un accord des représentants mandatés par les différents acteurs afin de s'assurer que la politique est applicable de façon réaliste.
Le document doit enfin préciser les actions menées en cas de manquement à ces responsabilités.

2.1.1 Lors de l'élaboration ou la mise à niveau de la PSI

o ***Recenser et impliquer tous les acteurs***

Pour chaque famille d'acteurs, il faut préciser dans le document leur implication pour l'élaboration et le maintien de la PSI. Une famille[1] peut correspondre à des types de risques différents ou à des responsabilités distinctes. Ce recensement est également nécessaire pour assurer une bonne application de la PSI. (voir § 2.1.2 du Guide d'élaboration d'une PSI § Consultation préliminaire des parties intéressées).

o ***Valider et suivre la politique de sécurité :***

Les besoins de l'établissement vis-à-vis d'Internet évolueront avec le temps, ce qui nécessitera de revoir la PSI. Le document doit décrire les processus mis en œuvre pour actualiser la PSI.

o ***Assurer la diffusion de la politique de sécurité***

La diffusion de la politique de sécurité doit se faire de façon transversale au sein de l'établissement.

[1] Par exemple : les employés et les utilisateurs internes, les prestataires externes, les administrateurs et les exploitants, la cellule de coordination de la sécurité Internet, les contrôleurs et les inspecteurs, les responsables sécurité, les architectes et les chefs de projets, les stratèges du système d'information, les propriétaires des informations et les banquiers, les directeurs, la hiérarchie, les maîtrises d'ouvrage Internet, le comité de pilotage Internet, le comité opérationnel Internet, les juristes, les responsables de la communication, les partenaires sociaux, les acteurs externes identifiés ou anonymes, les employés des filiales, les hébergeurs …

Le document doit mentionner les procédures de diffusion (destinataires, événements à la suite desquels la politique doit être re-diffusée).

2.1.2 Lors de l'élaboration des projets Internet

Les acteurs impliqués sont la maîtrise d'ouvrage, le responsable bancaire, la maîtrise d'œuvre, les chefs de projets, les comités Internet, les responsables de la sécurité.

o ***Prendre en compte la sécurité en amont des projets***

La PSI doit rappeler les différentes étapes méthodologiques permettant la prise en compte de la sécurité Internet : expression des besoins de sécurité, dossier de sécurité, validation des risques résiduels par les propriétaires des ressources, comité de qualification et/ou de validation, tests et audits de qualification, etc.
Le responsable du projet doit s'adjoindre des compétences sécurité au sein du projet pour l'accompagner. Cet accompagnement se traduit par un programme intégrant les points de validation par les instances de l'établissement compétentes.

o ***S'appuyer sur les architectures et solutions de sécurité homologuées par l'établissement***

Le Schéma Directeur Systèmes et Réseaux constitue la référence en termes de choix de solutions afin de garantir la cohérence de la sécurité au sein de l'établissement.

o ***Comportement à adopter en cas de fonctionnement anormal de l'application***

Le propriétaire des informations doit donner aux administrateurs la conduite à tenir en cas de fonctionnement anormal de l'application (par exemple, lors d'une attaque supputée, les conditions pour que l'administrateur arrête l'application)

o ***Qualifier la sécurité de l'application avant sa mise en ligne (voir 5.1.1)***

2.1.3 Lors de l'usage d'Internet : la sensibilisation

Les acteurs impliqués sont les utilisateurs, la hiérarchie, les responsables de la sécurité et la maîtrise d'Ouvrage Internet.

o ***faire participer les acteurs au maintien et à l'amélioration de la sécurité***

Le document fera référence au règlement intérieur et à la charte Internet. Celle-ci doit constituer un engagement individuel de l'utilisateur signé par lui pour le responsabiliser sur les thèmes suivants :
- Devoir de vigilance[2], devoir d'alerte ;
- Obligation de participer à la restauration de la sécurité des conditions de travail ;
- Obligation de discrétion.

Le document soulignera le rôle déterminant de la hiérarchie dans les actions de sensibilisation et leur suivi. La hiérarchie doit faciliter, favoriser et assurer le bon déroulement des actions de sensibilisation.
Le document précisera les moyens mis en place pour assurer cette sensibilisation, comme par exemple la charte d'engagement, la mise à disposition d'un kit de sensibilisation, les séances d'informations, une lettre sur la sécurité, l'accès à un serveur intranet sécurité, etc …

o ***Faire prendre conscience de la participation à une bonne image de l'établissement sur Internet***

Le document doit indiquer la nécessité pour l'établissement d'effectuer des analyses et des enquêtes pour apprécier la façon dont est perçu l'établissement par la communauté Internet. Il doit

[2] La PSI doit mettre en garde les acteurs vis-à-vis de la non-confidentialité des informations véhiculées sur Internet. Cette mise en garde portera aussi sur l'incertitude quant à l'identité de l'émetteur et à l'authenticité des services proposés sur Internet. Elle sensibilisera également les acteurs aux dangers liés aux virus récents pouvant circuler dans ces messages et dont on ne posséderait pas encore les signatures pour les détecter.

pouvoir contrôler l'utilisation de ses marques, logos (avec l'aide des clients et collaborateurs,….). Toutes les anomalies doivent être centralisées*.*

2.1.4 Lors de l'usage d'Internet : le suivi

Acteurs impliqués : Partenaires sociaux, Juristes, Directions, Hiérarchies, Contrôleurs, Inspecteurs.

o ***Suivre et contrôler l'activité des acteurs et l'utilisation des ressources***

La surveillance permanente permet de mettre en place un système de suivi assurant que les contrôles sont réguliers et remontés à la hiérarchie. Il s'agit de répondre à la demande des services de contrôle internes, de l'inspection ou de collaborer avec les instances externes compétentes en cas de nécessité. Cet aspect est développé au point 4.1.1.

o ***Suivre et contrôler les moyens de sécurité mis en place***

Le document présentera les différentes procédures mises en œuvre pour assurer le suivi et le contrôle des moyens de sécurité de l'établissement vis-à-vis d'Internet. Parmi ceux-ci :

- la supervision et l'exploitation des traces : ces documents précisent notamment les périodes de rétention des traces, les procédures à suivre pour y accéder et les exploiter (voir fiche technique 1 : Suivi et contrôle : exploitation des traces) ;
- la centralisation de la supervision et de l'administration ;
- la surveillance permanente ;
- les contrôles périodiques : ces contrôles permettent de déceler les écarts à la politique de sécurité. Le document doit préciser quels sont les acteurs en charge de ces contrôles : par exemple, la cellule de coordination de la sécurité Internet. Il doit préciser les modes opératoires notamment si ceux-ci peuvent ou doivent être inopinés ou doivent intervenir après avoir prévenu les exploitants ;
- les tests récurrents de solidité : le périmètre des tests sera clairement identifié préalablement. Si l'établissement éprouve le besoin de confier à des experts externes le soin de réaliser ces tests, les clauses contractuelles associées doivent faire objet d'une attention toute particulière (voir fiche technique : Cadre de sous-traitance de test d'intrusion) ;
- les contrôles exceptionnels : ils sont de la responsabilité des organismes de contrôles et de l'inspection. Ils répondent en général à un besoin d'investigation faisant suite à une demande des Directions ou des services d'inspection. Ils peuvent permettre de s'assurer rapidement après un incident majeur de l'état d'une partie des défenses de l'établissement sachant que vis-à-vis d'Internet, la rapidité de réaction est capitale.

2.1.5 Anticiper la violation de la politique de sécurité Internet

o ***Prévoir les réactions aux écarts à la politique de sécurité Internet***

Dans le cas d'une intrusion ou autre type de violation, les acteurs concernés doivent toujours être capables de débloquer les ressources et les compétences pour identifier la nature du problème et en limiter les dommages. La PSI doit indiquer qu'une ressource, un site ou un réseau ne peut pas être considéré comme bien sécurisé s'il n'est pas capable de répondre aux incidents de sécurité de manière adaptée (en rapidité et en efficacité).
La réaction aux incidents est traitée à la partie 6 du support thématique.

o ***Assurer une diffusion rapide et efficace des alertes de sécurité***

La PSI abordera les procédures mises en place pour assurer la diffusion des alertes. Elle doit préciser les acteurs intervenants dans cette diffusion, la marche à suivre pour transmettre les avis d'alertes et les procédures pour mettre en place les parades (voir fiche technique n°4: Suivi : Diffusion des alertes de sécurité et mise à niveau des parades).

2.2 Risques associés

2.2.1 Si cette partie était inexistante ou si des éléments importants n'étaient pas traités, les risques suivants existeraient

- Incapacité à atteindre le niveau de sécurité attendu : En effet, la sécurité est mise en défaut à travers le maillon le plus faible de la chaîne que constitue l'ensemble de ses composants. La politique de sécurité en est un composant majeur.
- Incapacité à régler les différends : Un manquement à une responsabilité d'un acteur vis-à-vis d'Internet ne peut lui être opposé que si cette responsabilité a été clairement identifiée et formellement documentée dans la PSI.

2.2.2 Si cette partie n'était pas correctement rédigée, les risques suivants existeraient

- Non-compréhension : Il est impératif que le texte soit rédigé simplement, clairement et de façon non ambiguë.
- Non-adhésion : Les recommandations à caractère obligatoire doivent avoir fait l'objet d'un consensus
- Non-respect : Ces recommandations doivent être réalistes afin de ne pas être contournées.

2.3 Recommandations

- Recenser et impliquer tous les acteurs (se référer également aux chapitres traitant de la « Délimitation du périmètre » et de « Elaborer et mettre en œuvre la politique de sécurité »)
- Valider et maintenir la politique de sécurité : prévoir et documenter (se référer également au chapitre « Elaborer et mettre en œuvre la politique de sécurité »)
- ***Assurer la diffusion de la politique de sécurité***
- Prendre en compte la sécurité en amont des projets et durant toute leur vie
- Prévoir un budget et élaborer un programme pour la sécurité au sein du projet
- S'appuyer sur les architectures et solutions de sécurité homologuées par l'établissement
- Prendre en compte les contraintes liées au confinement des risques au sein des réseaux internes (Se référer également au paragraphe « Approfondir la politique de sécurité générale - Politique de sécurité des réseaux » du présent guide.)
- Qualifier la sécurité de l'application avant sa mise en ligne (se référer également au chapitre 5.1.1)
- ***Sensibiliser les acteurs, les faire participer au maintien et à l'amélioration de la sécurité***
- ***Faire prendre conscience de la participation à une bonne image de l' établissement sur Internet***
- ***Donner aux acteurs les moyens de comprendre, respecter et adhérer à la politique de sécurité Internet***
- Clarifier et définir les responsabilités de chacun
- ***Suivre et contrôler l'activité des acteurs et l'utilisation des ressources***
- ***Suivre et contrôler les moyens de sécurité mis en place(se référer également au chapitre 5.3.1 « Processus d'évaluation »)***
- Suivre l'actualité des menaces et l'évolution des parades

(Se référer également au chapitre 5.3.2 « Organisation de cette veille » et au chapitre 6 « Réactions aux incidents »)

- Assurer une diffusion rapide et efficace des alertes de sécurité (se référer également au chapitre 6 « Réactions aux incidents »)
- ***Prévoir les réactions aux écarts à la politique de sécurité Internet***
- Prévoir dans l'étude des projets le comportement à adopter en cas de fonctionnement anormal de l'application
- Organiser la cellule de crise et mettre en place d'un plan de réactions aux incidents

Se référer également au chapitre consacré à ce sujet chapitre 6 « Réactions aux incidents »

- Organiser la communication de crise

Se référer également au chapitre consacré à ce sujet chapitre 6 « Réactions aux incidents »

2.4 Renvois sur fiches techniques

Fiche technique 1 : Suivi et contrôle : exploitation des traces

Fiche technique 2 : Suivi et contrôle : centralisation de la supervision et de l'administration

Fiche technique 3 : Tests d'intrusion : Règles en interne et pour la sous-traitance

Fiche technique 4 : Suivi : Diffusion des alertes de sécurité et mise à niveau des parades

Fiche technique 16 : Hébergement extérieur d'un site web

Voir extrait du Livre Blanc sur les infrastructure à clés publiques

3 Infrastructure d'accès à Internet

3.1 Objet

Ce chapitre a pour objet de définir les recommandations en matière de gestion des points d'accès au sein de l'entreprise.

On désigne comme **point d'accès Internet** la zone d'interconnexion entre le réseau public (Internet) et les équipements frontaux du site (établissement ou hébergeur).

En fonction de la taille de l'entreprise et de la couverture géographique, il peut y avoir plusieurs points d'accès Internet. L'ensemble de ces points d'accès correspond à **l'infrastructure d'accès à Internet** de l'entreprise. Si les comités de direction ont statué sur la mise en place d'un point d'accès unique, on peut considérer que le point d'accès et l'infrastructure Internet ne font qu'un.

L'infrastructure d'accès met en œuvre de services communs qui peuvent être techniques :

- DNS (résolution des noms),
- annuaire des usagers,
- dispositif générique de sécurité pour un type d'accès

ou organisationnels

- modèle d'architecture applicable aux différents points
- exploitation centralisée des équipements

3.1.1 Gérer les points d'accès au sein de l'infrastructure d'accès

Le comité de pilotage Internet ou les instances dirigeantes peuvent souhaiter la mise en place de plusieurs points d'accès Internet pour les raisons suivantes :

- autonomie des services qui ont la charge des études et/ou de l'exploitation du point d'accès Internet
- distance géographique entre les sites utilisateurs desservis.

En matière de sécurité, il s'agit de « maîtriser » ces points d'accès, pour obtenir une cohérence dans l'ensemble du dispositif (voir le § 1.3). Concrètement,

- toute création de point d'accès Internet doit être justifiée (voir partie 3.2) sur un argumentaire (fondé sur les deux points ci-dessus).
- L'administration des différents points d'accès peut être centralisée (voir partie 3.5)

3.1.2 Les principes de sécurité applicables à un point d'accès

o ***Refus par défaut***

- sur les protocoles,
- sur les services,
- sur les accès utilisateurs (justification, habilitation, auditabilité …)

L'accès est initialement refusé à tous, et ouvert uniquement aux besoins avérés et consentis.

o ***Redondance des moyens de sécurité***

Le dysfonctionnement d'un élément de sécurité ne doit pas invalider la protection.

o ***Confinement du risque***

L'architecture du point d'accès doit permettre de distinguer différents niveaux d'exposition aux risques (principe de la « pelure d'oignons ») et de mettre en œuvre les différents moyens de défenses en conséquence.
Une DMZ (Zone démilitarisée) est un sous-ensemble d'un réseau compris entre l'extérieur (Internet le plus souvent) et le réseau interne de l'entreprise. Ce sous réseau constitue en quelque sorte la partie publique visible du réseau extérieur. La communication entre cette zone démilitarisée et les autres réseaux (extérieur et intérieur) est contrôlée par des dispositifs de sécurité (routeurs-filtres, coupe-feux).

Sur cette DMZ ne devra être stockée :

- aucune donnée présentant un risque de confidentialité
- aucune information permettant l'usurpation d'identité (entre autres, des certificats)

Sur cette même DMZ,

- les systèmes devront être qualifiés au titre de la sécurité (ce qui peut inclure une revue d'une partie du code).
- tout trafic réseau dont l'analyse permettrait la fraude doit être chiffré ou faire appel à des techniques « non re jouables » lorsqu'il s'agit d'élément d'authentification.

3.1.3 Les services communs au point d'accès

o ***Mise en place d'une « rupture de protocole »***

Initialement étaient utilisées des ruptures protocolaires (par exemple X25), aujourd'hui des **« relais applicatifs de sécurité »** sont possibles.

Ces relais doivent permettre d'appliquer la politique de sécurité :

- analyse du contenu y compris sur les flux chiffrés,
- identification et authentification,
- contrôles d'accès,
- traçabilité des accès et actions.

Cette rupture doit être localisée au même niveau dans le point d'accès Internet afin de distinguer globalement les zones externes non sûres des zones internes (dites de confiance).

o ***Analyse du contenu***

Tout flux –franchissant la rupture de protocole- entrant et sortant doit faire l'objet d'une analyse de son contenu jusqu'au niveau applicatif afin de vérifier la conformité des commandes et arguments passés à la politique de sécurité. Ce qui signifie que le contrôle s'arrêtant au niveau réseau IP (adresse, port, en tête de paquets) n'est pas suffisant. D'où la nécessité de « relais applicatifs de sécurité » comprenant chacun des protocoles autorisés.

Le contrôle doit être traçable et l'intégrité de la configuration de référence doit être vérifiée.

o ***Réduction au strict nécessaire des « canaux franchissant la rupture »***

Le point d'accès doit garder une cohérence d'ensemble. Trop d'architectures différentes passant des zones exposées aux zones privées est un facteur de vulnérabilité. En d'autres termes, les solutions et les défenses doivent être mutualisées, en définissant des modèles d'architectures considérés comme valides pour l'établissements et qui sont instanciés par les différentes applications mises en ligne.

o ***Pas d'établissement de connexion sur l'initiative des réseaux non sûrs***

Les paquets franchissant en entrée la rupture de protocole vers les réseaux internes sont interdits lorsqu'ils correspondent à un début de session. Afin de s'assurer que toutes les initiatives de connexions sont initiées depuis un réseau sûr (interne), le filtrage des paquets doit intégrer le sens d'établissement de connexion.

o ***Protection du point d'accès vis à vis de l'externe et de l'interne***

La protection du point d'accès doit être assurée sur l'ensemble de son périmètre, aussi bien vers des réseaux publics que vers les réseaux internes. Les moyens de protection sont adaptés au risque.

3.2 Risques associés

Si les services d'infrastructure ne sont pas définis, il est fort probable que les chefs de projets Internet ne les mettront pas en place. Les applications ne seront donc pas sécurisées de façon cohérente, et le niveau de sécurité de l'ensemble baissera.

3.3 Recommandations

3.3.1 Gérer le nombre de points d'accès

- ***La création d'un point d'accès doit s'inscrire dans un processus de décision***
- ***La mise en œuvre du point d'accès doit s'inscrire dans un processus d'homologation et de qualification***
- En raison de la complexité de la gestion d'un point d'accès, il est préférable de limiter leurs nombres et de limiter leurs fonctions aux seuls services nécessaires.

3.3.2 Les principes de sécurité applicables à un point d'accès

- ***Refus par défaut (sur les protocoles, les services, les accès utilisateurs)***
- ***Le dysfonctionnement d'un élément de sécurité ne doit pas invalider la protection.***
- ***Un filtrage réseau doit être effectué, Le plan d'adressage du site doit se conformer à la RFC 1918 et de la NAT doit être faite en sortie.***
- Des outils de détection d'intrusion doivent être mis en place.
- ***Un serveur frontal doit être situé sur une DMZ et être protégé d'Internet par un équipement de filtrage.***
  - Les différents services offerts doivent être répartis sur des zones distinctes en fonction de leurs niveaux critiques.
  - Un serveur frontal ne doit en aucun cas contenir des informations de nature confidentielle ni stocker des journaux décrivant des traitements ou contenant des informations de nature confidentielle.
  - Sur la DMZ publique, le code et les sous systèmes sont « qualifiés » en matière de sécurité.
  - Tout trafic réseau dont l'analyse permettrait la fraude doit être chiffré ou faire appel à des techniques « non re-jouables » lorsqu'il s'agit d'élément d'authentification.

3.3.3 Les services communs au point d'accès

- ***Mise en place d'une « rupture de protocole » ou de relais de sécurité pour tout flux passant d'une zone publique à une zone privée.***

- ***Tout flux –franchissant la rupture de protocole- entrant et sortant fait l'objet d'une analyse de son contenu jusqu'au niveau applicatif.***
- ***Les solutions et les défenses sont mutualisées.***
- L'établissement de connexion n'est pas faite par des réseaux non sûrs
- La protection du point d'accès est assurée sur l'ensemble de son périmètre, aussi bien vers des réseaux publics que vers les réseaux internes.

3.3.4 Authentification des clients et intégrité/confidentialité des flux

- Le niveau d'authentification du client est adapté au type de transactions et à leur importance.
- Les mécanismes d'authentification sont fondés sur la délivrance d'un certificat logiciel.
- Le serveur frontal est certifié (pour les connexions SSL) auprès d'un organisme agréé.
- La mise en place des moyens cryptographiques avec les clients est conditionnée au respect des réglementations locales.

3.3.5 Volet sécuritaire du contrat ISP

- ***Un volet sécurité doit être impérativement annexe au contrat.***

Dans le cadre du contrat entre l'ISP et l'entreprise, les clauses suivantes peuvent être demandées :

- Possibilité pour l'ISP de filtrer un flux sur ses routeurs dans les cas de dénis de service
- Engagement de l'ISP sur un temps de réponse maximum à une demande provenant de l'entreprise en matière de sécurité
- Possibilité pour l'ISP de surveiller l'accès, à la demande de l'établissement, afin de détecter un flux anormal tel qu'une attaque par déni de service.

Ces informations ne sont pas exhaustives et doivent être adaptées au type d'accès.

3.4 Renvois sur fiches techniques

Fiche technique 5 : Configuration d'un poste isolé (modem)

Fiche technique 6 : Gestion des noms et adresses publiques (DNS, adressage IP)

Fiche technique 7 : Filtrage IP sur un point d'accès Internet

Fiche technique 17 : Soumission d'un poste aux règles de sécurité applicables aux postes fixes

4 Sécurité par service applicatif

4.1 Objet

Un service applicatif est une catégorie d'application tenant compte à la fois des fonctions bancaires développées et des technologies utilisées pour réaliser ces fonctions. Les mesures de sécurité à mettre en place couvrent à la fois les risques fonctionnels et les risques « techniques » d'où une combinatoire complexe de solutions. La politique de sécurité ne peut décrire les solutions à mettre en place ; l'élaboration des solutions est un domaine d'expertise qui doit être traité par les responsables bancaires conseillés par des experts.
L'infrastructure d'accès décrite dans la partie 3 est un socle qui sera mis à profit par chacune de ces solutions, de même que les recommandations d'exploitation fournies à la partie 5 et les traitements d'incidents décrits en partie 6.

Dans le cadre de ce guide, est privilégiée une approche fonctionnelle en distinguant 5 catégories de besoins :

1. Mise à disposition d'information (Vitrine);
2. Fourniture de services transactionnels ;
3. Accès Internet sortant pour les collaborateurs (de navigation, d'émission et réception du courrier électronique) ;
4. Utilisation de services Internet financiers (tels que des applications de salles de marchés, des traitements d'information d'application à application) .
5. Lorsqu'il sera possible juridiquement de conclure des contrats, qui nécessitaient un formalisme écrit-papier, de façon électronique, des garanties de forme « électronique », semblables aux garanties de l'écrit papier, devront être mises en place, sous peine de nullité du contrat.

Le présent document développe seulement[3] les catégories 3 et 4. Les fonctions de sécurité à mettre en oeuvre pour un serveur institutionnel ont fait l'objet d'un profil de protection en cours de dépôt à la Direction Centrale pour la Sécurité des Systèmes d'Information (DCSSI). Le Comité Français d'Organisation et de Normalisation Bancaire (CFONB) prépare un profil de protection adapté aux risques des sites web financiers transactionnels. Les travaux sur ces sujets sont conformes aux Critères Communs et constitueront un référentiel rigoureux de sécurité.

Les **accès Internet fournis aux collaborateurs de l'établissement** sont proches d'un établissement à un autre. Aussi, le groupe de travail du Forum des Compétences a-t-il pu détailler ses recommandations et compléter les propos tenus dans le présent document par deux fiches techniques.
L'utilisation de services Internet financiers fournis par un tiers comprend une diversité extrême de situations. Les conseils donnés sur cette partie sont plus génériques et méthodologiques que pour la catégorie précédente.

4.1.1 Services de sécurité relatifs aux utilisateurs internes (navigation et messagerie)

Comme l'explique la partie 2.1.4 « Suivre et contrôler l'activité des acteurs et l'utilisation des ressources », les utilisateurs doivent être identifiés et authentifiés et disposer d'une habilitation sur le type de service qui leur est nécessaire.

[3] Le lecteur est cependant invité à lire la fiche technique n°16 sur l'hébergement extérieur de serveur Web et qui énonce un certains nombre de conseils utiles pour la constitution d'un serveur institutionnel.

Les services communément demandés[4] sont la messagerie, la navigation et le transfert de fichiers. Chacun de ces services demande que soient étudiés les principes exposés aux paragraphes qui suivent . Deux fiches techniques détaillent les recommandations pour la messagerie et la navigation.

o ***Identifiant explicite ou transposé***

L'utilisation des ressources Internet ne peut pas être anonyme car il est important de reconnaître l'utilisateur à des fins diverses :

- Mise à disposition des fonctions strictement nécessaires à l'utilisateur : navigation, réception de fichier, émission de fichier, accès au courrier électronique
- historique des échanges, par exemple pour pouvoir instruire une affaire où l'établissement est impliqué en raison de l'activité Internet d'un de ses agents.
- Fraudes et malversations internes
- Etc.

Pour identifier les utilisateurs, la PSI devra choisir l'une des deux options suivantes :

- Utiliser un identifiant explicite, tel que prénom.nom ou matricule. L'utilisateur ne mémorise pas un identifiant supplémentaire, et l'on peut utiliser les référentiels en place. En revanche, les rapprochements entre activité Internet et personne physique seront faciles. Cette situation peut poser un problème en matière de respect de la vie privée.
- Utiliser un identifiant transposé non compréhensible d'une personne extérieure. Le couplage Identifiant Internet/Personne physique n'est pas divulgué et la vie privée est préservée à moins qu'une démarche très spécifique soit engagée (rapprochements). Cela oblige à gérer un nouveau référentiel.

La PSI doit statuer sur l'émission de courriers ou boîtes aux lettres **fonctionnelles** (par exemple : support_clientele@ma-banque.com)

o ***Authentification des utilisateurs***

L'authentification est recherchée afin que l'utilisateur ne puisse répudier ses actions. Le mécanisme d'authentification s'inscrit dans le cadre des dispositions habituelles de sécurité en vigueur dans l'établissement:

- Nature du système d'authentification (mot de passe, « token », etc…) ;
- Règles de gestion du mot de passe (péremption, complexité, renouvellement, transmission à des tiers, etc…) ;
- Protection du référentiel de sécurité ;
- Organisation de l'administration de la sécurité.

o ***Habilitations***

Le système d'habilitation permet de différencier les services accessibles à chaque utilisateur, selon ses besoins réels. La PSI précisera que ces services doivent être définis aussi finement que possible afin de respecter la règle de « moindre privilège ».

o ***Audit***

De manière générale, la PSI devra imposer le strict respect des règles en vigueur dans le pays où seront générés et/ou stockés les journaux (déclarations à la CNIL, *privacy policy*). La PSI devra aussi statuer sur le degré de protection à apporter aux archives.

L'activité des utilisateurs doit être analysable. En revanche, pour des raisons de respect de la vie privée, le rapprochement **activité/personne physique** ne devrait pas être possible sans qu'une démarche volontaire ne soit entreprise (voir le § Identifiant explicite ou transposé)

L'audit doit être possible durant une période assez longue après que l'activité a eu lieu. Bien qu'aucune règle n'impose de durée, il faut considérer que les règles en matière de journaux d'accès à l'Internet devraient être les mêmes que pour l'accès au réseau téléphonique (archivage des journaux des PABX).

[4]D'autres services peuvent être demandés, comme les forums, lieux de discussion (chat),la visioconférence, la voix sur IP, les services pour mobiles etc.

o ***Equipements de filtrage***

L'accès des collaborateurs à Internet (navigation, messagerie, application…) doit être effectué par des relais applicatifs (voir le chapitre 3.1.3 : Analyse du contenu) permettant un contrôle de l'activité. En plus des fonctions expliquées dans ce chapitre, les équipements de filtrage doivent :

- bloquer les accès aux sites déviants ;
- contrôler les fichiers, pièces joints rapatriées ;
- joindre une mention de mise en garde limitatrice de la responsabilité de l'établissement ;
- permettre la mise en œuvre d' une politique anti-virus.

Une sensibilisation des collaborateurs aux risques existants doit être menée par les différentes entités (voir chapitre 2.1.3).

4.1.2 Utilisation de services Internet financiers

o ***Description du risque***

Certains prestataires de services proposent la mise en place de flux IP non standards. Ces solutions exigent souvent :

- la présence d'un module client dans le poste de travail de l'utilisateur ;
- Le libre passage d'un flux inconnu à travers le point d'accès Internet : le protocole utilisé n'est pas documenté et il n'existe pas de relais de sécurité ;
- Dans les cas les moins favorables : le module client nécessite une visibilité en direct (sans translation d'adresse) d'un serveur situé dans le réseau Internet.

Le risque est élevé : les protections étant « aveugles » au flux utilisé par la solution, le code client pourrait[5] héberger un cheval de Troie ou une porte dérobée (l'établissement n'a aucune vue sur la qualité de ce code et la rigueur du suivi des développements).
Malheureusement, ces solutions peu propices à la sécurité des réseaux sont des outils très répandus.

o ***Les approches possibles***

Une première approche consiste à **interdire purement et simplement les solutions ne respectant pas les principes de fonctionnement du point d'accès**:

- normalisation des flux,
- existence d'un proxy pour ces flux,
- pas de routage direct entre le réseau interne et l'Internet

Cette politique doit fixer les règles **avant** la signature des contrats et inciter progressivement les fournisseurs à tenir compte des objections formulées. Il faut prévoir un circuit apte à statuer sur la conformité de la solution et l'homologation du nouveau flux. Dans la pratique, ce type d'approche est difficile à tenir devant la pression des utilisateurs.

Une seconde approche peut nuancer la première : **de tels services sont acceptés à condition que le fournisseur accepte de communiquer la description du protocole qu'il emploie**. L'établissement a alors les moyens de développer un proxy spécifique. Cette politique se heurtera néanmoins à des coûts de développement et à des délais importants de mise à disposition des solutions externes. Sur le strict plan de la sécurité, cette option est pourtant défendable, sous réserve que la publication de la PSI soit accompagnée :

- d'une équipe spécialisée dans les développements de proxy,
- d'une bonne appropriation de la PSI par les clients potentiels de ces solutions de manière à ce qu'ils expriment les exigences de votre établissement très tôt dans la négociation avec les fournisseurs.
- D'une grande rigueur dans l'administration des systèmes d'accès car la pression des directions utilisatrices de ces services est souvent très forte (« si M. X n'a pas accès à ce service vital pour lui, vous serez tenu pour responsable ! » ou bien « c'est un outil de place, pas un trader ne s'en passe

[5] En illustration, il n'est pas rare que ces systèmes se mettent à jour spontanément et à l'insu de l'utilisateur.

aujourd'hui, ce sont mes collègues de la XXX qui m'en ont signalé l'existence ! »)

Une troisième approche consiste à **n'autoriser les modules clients de ces solutions que sur des postes dédiés et non connectés au réseau interne**. Un effort important devra alors être fait pour « suivre » ces installations et s'assurer qu'elles restent dédiées et non connectées. Le risque qu'une machine dédiée soit finalement reliée au réseau, par commodité (en général, accès à une imprimante évoluée), est élevé.

La quatrième approche consiste à **autoriser ces solutions moyennant des destinations sur le réseau interne précisément définies et limitées**. Cette politique accepte les risques d'une communication entre un module client situé sur le réseau interne et un dispositif extérieur peu ou pas connu. Pour limiter ce risque, il s'agit de prendre les mesures suivantes :

- Demander au fournisseur de présenter tout document faisant état des contrôles qu'il pratique au niveau de son réseau et de son développement d'application afin de protéger ses clients.
- Exiger que le fournisseur accepte d'être audité .
- Imposer que l'unité faisant usage de ces services isole son réseau du reste de l'établissement de manière à ne pas propager le risque (troisième approche). La PSI sera donc, dans le cas présent, étroitement couplée à la politique de sécurité du réseau interne.
- Imposer l'utilisation d'un coupe-feu local précisément paramétré dans chacun des postes bénéficiant des services en question. Il est prévisible que ce point se banalisera dans les années à venir. La PSI peut donc anticiper moyennant le fait que les mesures complémentaires d'application soient intelligemment échelonnées.

4.2 Risques associés

Risques	**Exemples de menaces**
Atteinte au point d'accès	• Déni de service • Compromission des systèmes de sécurité propre au point d'accès
Atteinte à l'image de l'entreprise	• Déni de service • Substitution de contenu • Détournement du site • Rebond • Actions collaborateurs
Atteinte au SI de l'entreprise	• Accès et maintient frauduleux à une ressource du SI à travers le point d'accès • Déni de service en interne
Risques associés aux flux entrant	• Virus • code mobile
Risques associés aux flux sortant	• Actions collaborateurs • Virus • code mobile

4.3 Recommandations

- Spécifier l'utilisation d'un identifiant (explicite ou transposé)
- Autoriser ou interdire l'émission de courriers ou boîtes aux lettres **anonymes**
- L'authentification des utilisateurs suit les règles générales de sécurité

- ***Existence d'un système d'habilitation permettant de différencier des services accessibles à chaque utilisateur***
- ***Les activités des utilisateurs peuvent être auditées sur une longue durée (alignée sur les journaux PABX)***
- L'audit des utilisateurs est exceptionnel et ne peut être mis en œuvre par une seule personne (pour respect de leur vie privée).
- ***les équipements de filtrage doivent :***
  - ***bloquer les accès aux sites déviants***
  - ***contrôler les fichiers, pièces jointes rapatriées***
  - ***permettre la mise en œuvre d' une politique anti-virus.***
- ***Proposer une des approches décrites pour la mise en œuvre de services non standards***

4.4 Renvois sur fiches techniques

Fiche technique 8 : Service courrier électronique

Fiche technique 9 : Charte utilisateur d'Internet

Fiche technique 10 : Service navigation WEB

5 Politique et règles d'exploitation

5.1 Objet

Les règles d'exploitation de la sécurité constituent le cadre fonctionnel et organisationnel de l'établissement en vue d'assurer la sécurité et de la rendre contrôlable. Elles ont vocation à garantir la robustesse et la surveillance des infrastructures, le contrôle de l'usage qui en est fait, la capacité à prendre en compte des alertes et à réagir aux incidents courants.

La réaction aux incidents graves et gestion de la crise induite est traitée au chapitre 6.

5.1.1 Qualification initiale des architectures et des outils mis en œuvre

La PSI déterminera le processus de définition et de validation des solutions de sécurité mise en œuvre (voir §2.1.2). L'homogénéité des règles au sein de l'établissement contribue au niveau de sécurité des différents services Internet. Tout changement significatif doit être accompagné d'un travail d'évaluation sécuritaire. En conséquence,

- La plate-forme d'homologation doit être distincte de celle d'exploitation,
- Les tests de qualification comprennent trois volets : audits, revue de codes sensibles, tests d'intrusion.

5.1.2 Veille sécurité, mise à niveau et évaluation périodique

La veille doit porter sur l'évolution:

- des menaces (par exemple les nouvelles techniques d'attaques, la propagation fulgurante d'un virus, l'activité suspecte de groupes malveillants...),
- des vulnérabilités (par exemple la publication de nouvelles failles dans les produits en production) et des produits capables de contribuer à renforcer la sécurité.

La veille est assurée de façon durable et tient compte de la continuité du service. Le document expliquera le risque pris si cette veille sécuritaire n'était pas réalisée. Il mentionnera les deux types de veille à mettre en place ainsi que les acteurs concernés et les procédures à suivre pour assurer la communication entre eux.

5.1.3 Formalisation et contenu des procédures d'exploitation

o ***Contenu des procédures d'exploitation***

Les procédures d'exploitation comprennent :
- la surveillance et la réaction aux incidents de sécurité,
- le contrôle de l'intégrité des infrastructures,
- le contrôle régulier de l'usage.

o ***Maintien de la conformité à la politique de sécurité***

Tous les moyens de sécurité en exploitation doivent pouvoir faire la preuve qu'ils appliquent strictement la politique de sécurité (listes de filtrage sur routeurs, sur firewalls, sur applications, …).
Les règles de sécurité sont traduites en moyens de contrôle, partie technique depuis laquelle on doit pouvoir retrouver la règle de gestion d'origine. Le référentiel concerne autant les règles que leur traduction technique.

5.1.4 Qualification et disponibilité du personnel d'exploitation

La surveillance de l'interconnexion doit être assurée pendant toute la période d'activité soit une surveillance 24/24 et 7/7. Cette surveillance est effective si le personnel est formé aux produits mis en production, ce qui implique les efforts suivants :

1. Rechercher l'application des standards par défaut
   - pérennité des compétences,
   - l'acquisition d'expertise est simplifiée car la technologie est plus « plus simple ».

2. Assurer la capacité de l'exploitant à maîtriser la technologie.

5.1.5 Suivi

- La PSI définira les règles de suivi de l'exploitation. Les comptes-rendus de suivi sont adressés au maître d'ouvrage et au RSSI. Les comptes-rendus sont constitués :
- des rapports d'évaluation périodique de vulnérabilité,
- du tableau de bord sécurité d'exploitation,
- des rapports d'incidents de sécurité

5.2 Risques associés

En l'absence de règles d'exploitation définies au niveau de la PSI, la sécurité ne peut reposer que sur un savoir faire et des pratiques locales difficiles à évaluer et à contrôler.

5.3 Recommandations

5.3.1 Processus d'évaluation

- ***La validation d'un dispositif de sécurité doit reposer non seulement sur une documentation précise de l'infrastructure mais aussi sur une évaluation sur site de sa mise en œuvre assurée par du personnel qualifié.*** Dans le cas d'infrastructures spécifiques, l'avis d'au moins deux experts indépendants est recommandé.
- ***Une évaluation périodique doit garantir que le niveau de sécurité requis est toujours atteint et en particulier que toutes les mises à niveau requises ont bien été réalisées.*** Ces mises à niveau portent non seulement sur les moyens techniques mais aussi sur les procédures.

5.3.2 Organisation de la veille sécuritaire au sein de l'établissement

- On s'appuiera, d'une part, sur des experts avec lesquels un travail dans la durée est assuré et, d'autre part, sur des expertises externes capables d'apprécier le niveau de sécurité avec un œil neuf et à l'aide d'autres méthodes et outils.
- ***Le processus de veille doit permettre de disposer :***
  - ***d'alertes exigeant une réaction rapide telle la mise à niveau immédiate des moyens techniques (application de patches, modification de configuration, mise à jour de l'antivirus...), l'adaptation des consignes de surveillance ou la diffusion de consignes aux utilisateurs.***
  - ***d'informations permettant de renforcer la sécurité en faisant évoluer les architectures et les outils***

5.3.3 Formalisation et contenu des procédures d'exploitation

- ***Les exploitants disposent d'un manuel de sécurité comprenant***
  - ***les procédures de surveillance et de réaction aux incidents***
  - ***les procédures de sauvegarde et d'archivage***
  - ***les procédures de contrôle (analyse des fichiers journaux)***
- ***Les exploitants doivent adapter la configuration de leurs équipements aux règles de sécurité***
- ***Les exploitants disposent de documents pour suivre :***
  - ***les interventions (internes et externes) sur la plate-forme***
  - ***les audits techniques (de qualification, recette)***
- ***Les consignes d'exploitation doivent être tenues à jour dans le cadre du processus de mise à niveau.***

5.3.4 Qualification et disponibilité du personnel d'exploitation

- ***L'exploitant de premier niveau doit avoir reçu une formation adaptée, s'appuyer sur des consignes d'exploitation formelles et pouvoir recevoir l'assistance d'un expert.***
- Il est recensé comme « exploitant de point d'accès Internet »

5.3.5 Suivi

- ***Le tableau de bord périodique (voire plusieurs avec des périodicités différentes) fait partie du processus de remontée d'information***
- La gestion des alertes sur les points d'accès Internet est centralisée

5.4 Renvois sur fiches techniques

Fiche technique 11 : Architecture d'un point d'interconnexion à Internet

Fiche technique 12 : Configuration, contrôle et surveillance d'un serveur exposé à l'Internet

Fiche technique 13 : Identification d'un incident

Fiche technique 14 : Traitement de l'incident

6 Réactions aux incidents

6.1 Objet

Mettre en place une organisation et des moyens pour détecter, identifier, et répondre à un incident de sécurité Internet.

6.1.1 Nécessité

Compte tenu de la forte probabilité d'incidents liés à Internet, de la fréquence, de la diversité des natures de ces incidents et de l'importance des risques encourus, il est indispensable de prendre en compte dans la mise en place de la politique de sécurité les aspects liés à la réaction aux incidents.

6.1.2 Définition sémantique d'un incident

Un incident est un « événement, le plus souvent fâcheux, qui survient au cours d'un fait principal, qui le trouble et dont les conséquences peuvent être graves »

Pour la sécurité Internet, un incident se définit selon trois approches :

- Par constat : Comme un dysfonctionnement par rapport à une situation stable connue et définie comme « normale ».
- Par référence : Comme correspondant à un élément d'une liste de référence des incidents.
- Par concept : Comme une violation de la politique de sécurité Internet.

6.1.3 Mise en garde

Compte tenu de la nature confidentielle de certaines informations relatives à ces chapitres, celles-ci devraient au final, lors de la rédaction du manuel de procédures par l'établissement, être enlevées des parties du document destinées à une large diffusion auprès de personnels non certifiés.

6.1.4 Bibliographie

- Réglement n° 97-02 du Comité de la réglementation bancaire et financière
- Commission Bancaire, Livre blanc sur la Sécurité des Systèmes d'Information, Janvier 1995
- FDIC, FIL-68-99, July 7 1999
- OCC 2000-14, May 15 2000
- CERT Coordination Center, Responding to Intrusions, July 30 1999
- CERT Coordination Center, Preparing to Detect Signs of Intrusions, August 2 1998
- CERT Coordination Center, Incident Reporting Guidelines, April 12 2000 [6]

6.2 Risques associés

Les risques associés sont nombreux :

- Etre dans l'incapacité de déceler ou de « contingenter » un incident ;
- Subir des dommages et ne pas le savoir ;

[6] et toutes les sous-sections associées à ces documents du CERT, notamment :
"Establishing policies and procedures for responding to intrusions", "Establish a policy and set of procedures that prepare your organization to detect signs of intrusions", "Analyse all available information to characterize an intrusion", "Collect and protect information associated with an intrusion", "Prepare to respond to intrusions", "Apply short-term solutions to contain an intrusion".

- Subir des pertes de confidentialité, de disponibilité, d'intégrité, …etc ;
- Véhiculer une image négative auprès de tiers (partenaires, clients, … etc) ;
- Ne pas réagir efficacement par manque de préparation, d'information, de moyens ou de ressources ;
- Créer des effets de panique injustifiés par une communication non-contrôlée et/ou un manque d'analyse des évènements ;
- Déployer des traitements inefficaces ;
- Perdre l'information (donner trop, pas assez d'information ou une mauvaise information.

6.3 Recommandations

Pour un contenu détaillé des chapitres suivants, voir les fiches techniques "Identification d'un incident", "Traitement d'un incident" et "Evaluation post-incident".

6.3.1 Préparer et planifier les procédures

Afin d'assurer un bon déroulement des opérations en situation de réaction aux incidents (situation de stress), il sera pris soin de :

- ***Définir la fréquence d'actualisation des procédures.***
- ***Définir les chaînes de contact, les modes de cascade d'alertes et leur degré de réactivité.***

6.3.2 Identifier un incident

Voir la fiche technique n° 13 " technique "Identification d'un ", et en particulier les points suivants :

- ***Circonscrire l'incident géographiquement et fonctionnellement.***
- ***Alerter les compétences les plus adaptées.***
- ***Qualifier les incidents.***
- ***Valider les remontées d'alertes avant de les diffuser hors des services spécialisés.***
- ***Inclure très tôt dans la chaîne d'information de cet incident les responsables des directions susceptibles d'en ressentir les effets.***
- ***Définir les priorités sur les incidents.***
- ***Obtenir la participation diligente des services de Communication pour les diffusions en externe.***

6.3.3 Traiter un incident

Voir la fiche technique n° 14 "Traitement d'un incident", et en particulier les points suivants :

- ***Arrêter la propagation le plus rapidement possible.***
- ***Recueillir un maximum d'information sur l'incident afin de constituer une collecte d'éléments pouvant servir dans un dossier de justice.***
- ***Trouver un compromis entre la rapidité de réponse et la pertinence de la réponse.***
- ***Exécuter des tests avant de procéder massivement au déploiement d'actions d'endiguement et d'éradication.***

6.3.4 Evaluer les conséquences d'un incident

Voir la fiche technique n° 15 " Evaluation post-incident ", et en particulier les points suivants :

- ***Stocker de manière systématique et organisée l'historique de ses incidents et de leurs résolutions.***
- ***Partager les retours d'expérience.***

- ***Avoir une démarche préventive à l'encontre de variantes potentielles de l'incident subi.***
- ***Envisager d'avancer l'actualisation des procédures après la résolution d'un incident.***

6.4 Renvois sur fiches techniques

Fiche technique 4 : Suivi : Diffusion des alertes de sécurité et mise à niveau des parades

Fiche technique 13 : Identification d'un incident

Fiche technique 14: Traitement de l'incident

Fiche technique 15 : Evaluation des dommages post-incident : historisation

Guide d'élaboration d'une Politique de Sécurité Internet

A l'usage des responsables de la sécurité des systèmes d'information (RSSI) des établissements de crédit et des entreprises d'investissement

Fiches Techniques

Liste des fiches techniques

Sommaire

Fiche n° 1. Suivi et contrôle : exploitation des traces

Définition :

La journalisation a pour but d'enregistrer l'état ou l'activité (évènements) des différents systèmes dans des traces. C'est le principal moyen de couvrir les objectifs de traçabilité de l'activité et d'imputabilité des actions définis dans la politique de sécurité.

Les traces constituent la source d'information privilégiée à chaque fois que l'on souhaite mener une investigation particulière : détection d'une défaillance, étude suite à un incident, aide à la décision, contrôle, recherche de preuves.

La mise en œuvre de traces est le résultat d'un processus de :

- Définition des objectifs et d'une politique de journalisation ;
- Définition des éléments à tracer et des moyens de trace à mettre en œuvre ;
- Définition des règles et des moyens d'exploitation des traces ;
- Contrôle de l'adéquation des traces aux objectifs.

Ce processus doit être réactualisé dans le cadre d'une maintenance régulière.

Risques :

Une mauvaise exploitation des traces se constate :

- **par un défaut d'éléments permettant le suivi des traitements à des fins d'investigation**

  - Qualification de l'incident. Est-ce un incident de sécurité ? Depuis quand est-ce dans cet état ?
  - Détermination de l'origine. Qui est à l'origine de l'incident ?
  - Mesure de la portée. Quels systèmes ou applications ont subi un impact ?
  - compréhension du mécanisme. Comment cela s'est-il produit ?

  Indépendamment de tout sinistre, les traces et l'analyse qui en est faite est un moyen pour les responsables sécurité de s'assurer de la qualité de l'administration.

- **par un risque généré par les traces elles-mêmes**

  Ci-après sont exposés quelques travers possibles:

- La collecte des informations est frauduleuse ou déloyale. Cette analyse vaut en particulier pour les données nominatives : les informations sont conservées au-delà de la durée prévue, les informations sont communiquées à des personnes non autorisées ;
- Le traitement fait l'objet d'un détournement de finalité.

Critères de Qualité :

Pertinence des traces

Une politique de traces est définie en fonction de la nature des risques que l'on veut circonscrire. Le contenu des traces et l'exploitation que l'on en fait doit être révisé en fonction de l'évolution des risques. On cherchera un compromis entre la surabondance de trace et le manque d'information :

- La surabondance de traces ne facilite pas leur exploitation. De plus, les performances et le volume des traces restent des critères importants à prendre en compte.
- On tracera en priorité les événements « anormaux ». Cela suppose que l'on ait analysé quelle est la nature des événements anormaux susceptibles d'être rencontrés afin de les détecter et de les tracer.
- Ne tracer que les événements anormaux n'est pas suffisant. Ainsi, le fait de ne tracer sur un firewall que les datagrammes rejetées est utile si on a une politique de poursuite systématique contre toutes les tentatives d'intrusion mais pas suffisant si on veut traiter les intrusions réussies. Conserver une trace des connexions qui ont traversé le firewall est indispensable. De plus, un événement pris isolement peut apparaître comme normal alors que recoupé avec d'autres, il peut traduire une anomalie. Enfin, beaucoup d'événements ou d'états normaux sont nécessaires pour analyser le contexte d'une anomalie. Ainsi, par exemple, toutes les actions de l'administrateur doivent être tracées.

En pratique, on choisira des produits offrant des possibilités de traces riches que l'on configurera en fonction des objectifs de sécurité retenus qui détermineront les évènements significatifs :

- Des traces doivent être réalisées sur les différentes machines (routeur, firewall, proxy, serveur, …) et sur ces machines à plusieurs niveaux (réseau, OS, Middleware, application).
- Outre les outils indispensables au fonctionnement, on utilisera des outils complémentaires destinés à améliorer la surveillance et enrichir les traces (Outils de contrôle d'intégrité tel Tripwire sous UNIX, outils de trace réseau tel TCPWrapper sous UNIX, outils de détection d'intrusion,...).
- On appliquera à ces traces un filtre pour détecter des événements clés devant constituer une alerte, pour éliminer les événements considérés comme peu pertinents ou pour agréger des événements étroitement corrélés.
- Plusieurs niveaux de journalisation peuvent être définis afin de ne tracer certains événements que dans certaines circonstances (voir les fiches n°13 et 14, identification et traitement d'un incident).

Sous quelle forme réaliser ces traces ?

La constitution d'une multitude de traces indépendantes est assez simple à mettre en œuvre mais la protection de ces traces est alors difficile à garantir et leur exploitation est trop complexe pour être efficace. En pratique seules quelques traces sont effectivement exploitées et cette exploitation est limitée par le caractère très local de la trace.

A l'opposé, la constitution d'un journal global et centralisé regroupant l'ensemble des événements d'origines diverses et la mise en œuvre d'outils permettant d'analyser ces événements est idéale pour une analyse efficace. En effet, on dispose alors d'une vision globale du système d'information et la possibilité de recouper des évènements en provenance de plusieurs machines ou de plusieurs niveaux d'une même machine permet une analyse riche et pointue. Il s'agit néanmoins d'une architecture coûteuse à réaliser et difficile à faire évoluer.

En pratique, on cherchera à déporter la journalisation sur un système dédié et à réaliser ainsi une « centralisation raisonnable » des traces adaptées aux infrastructures et à l'organisation que l'on peut mettre en œuvre.

Cette centralisation nécessite :

- La mise en œuvre d'une l'infrastructure de remontée et de conservation des traces : La sécurisation de cette infrastructure : sécurisation et dimensionnement de la machine centrale, gestion des droits d'accès en lecture et écriture à la trace, sécurisation de la remontée des traces
- La définition d'un format standard des traces : Chaque événement doit être horodaté et doit indiquer sa provenance (machine, process, …) et son caractère critique.
- La synchronisation des traces : les différentes sources de traces ne sont pas synchrones.

La centralisation favorise :

- La sécurisation des traces. Le déport des journaux sur une machine moins exposée rend leur compromission plus difficile.
- La corrélation entre événements issus de plusieurs sources.
- L'instrumentation de l'analyse des traces indispensable à l'exploitation effective des traces. Cette instrumentation doit permettre un premier niveau d'analyse automatique et systématique et offrir les moyens d'une analyse spécifique rapide.
- La sauvegarde et l'archivage des journaux.

Emplacement des sondes

La mise en place de sondes spécifiques - sondes réseaux autonomes ou sondes logicielles installées sur certains dispositifs - doit faire l'objet d'une expertise prenant en compte les besoins exprimés et le risque admissible. En pratique, il est fortement recommandé de suivre un principe permettant de dissocier deux types d'informations :

- **Visibilité des tentatives d'accès:**

La mise en place d'une sonde réseau au plus prés du réseau externe offre une visibilité instantanée des tentatives d'accès. Ces informations, fortement techniques et demandant une bonne connaissance des protocoles **IP** et des techniques d'attaques, permettent d'affiner les filtres amonts, voire d'anticiper les attaques.

- **Visibilité des flux établis:**

La mise en place d'une sonde réseau au plus prés de l'interface de raccordement avec les réseaux internes permet à l'exploitant d'identifier et de contrôler les flux effectivement établis à travers sa plate-forme. Une action en retour peut être initialisée afin d'affiner les filtres et les règles de sécurité. Contrairement à la sonde placée en amont, les informations collectées restent facilement exploitables car elles sont orientées « flux de services ».

Dans tous les cas, il y a lieu de considérer l'utilisation de sondes disposant de deux interfaces dissociées, l'une connectée au réseau, qui est l'objet de la surveillance, l'autre au réseau d'exploitation. L'interface d'acquisition doit impérativement être activée en mode 'transparent' et 'neutre': aucune couche protocolaire ne doit être associée à cette interface. Le raccordement de la sonde sur un port de recopie est fortement recommandée lorsqu'un tel port est disponible sur l'équipement de raccordement amont (switch, routeurs de sécurité, …).

Quand analyser une trace ?

Une analyse systématique quotidienne est indispensable. Elle peut permettre la détection d'anomalies et de réagir pour éviter un sinistre.

Cette démarche proactive reste néanmoins limitée à l'analyse d'événements ciblés et faciles à corréler d'un petit nombre de sources. Cette analyse doit pour être efficace être automatisée et générer des alertes à l'administrateur. Disposer d'alertes pertinentes nécessite un rodage qui peut être long et un travail d'analyse continu.

Au-delà, la complexité d'analyse des traces et le manque d'outils permettant d'automatiser cette analyse rend très vite cette opération très coûteuse. Des outils s'appuyant sur des technologies de datamining sont apparus récemment.

Sécurisation de journaux

- Disponibilité : archivage
- Intégrité : les traces doivent en particulier être protégées contre des actions malveillantes visant à les effacer **ou à les modifier**. L'intégrité des traces peut être assurée par l'usage de supports d'enregistrement non effaçables ou *a minima* par un transfert très fréquent, sinon temps réel, sur une machine sûre.
- Confidentialité : les traces contiennent des informations sur le fonctionnement du système, ses utilisateurs et la politique de sécurité mise en œuvre. Leur divulgation à un acteur malveillant peut donc avoir de graves conséquences. On veillera donc à ne tracer que des informations utiles (ne pas tracer les mots de passe !) et à protéger l'accès aux traces.

  Certaines traces peuvent être nominatives. Outre la déclaration à la CNIL, des règles d'accès et d'exploitation des données tracées doivent être définies. Les utilisateurs doivent être informés de l'existence de ces traces et de l'usage qui peut en être fait.

Fiche n° 2. Suivi et contrôle : centralisation de la supervision et de l'administration

Définition :

La meilleure des politiques de sécurité peut rester vaine si tous les moyens ne sont pas mis en œuvre pour que la supervision et l'administration de la sécurité (des points d'accès à l'Internet notamment) soient centralisés au niveau des équipes du RSSI.

Risques :

La dispersion des responsabilités en ce domaine, mène inéluctablement à une politique de sécurité incohérente. L'absence de supervision des éléments critiques connectés à l'Internet, laisse les coudées franches à des tentatives d'attaque du SI de l'entreprise.

Administration :

- Si une partie seulement des serveurs antivirus de l'entreprise est mise à jour, les risques d'infection subsistent.
- Si les correctifs de sécurité sur des OS serveurs ne sont pas appliqués de manière concertée à l'ensemble de l'entreprise, des trous de sécurité risquent d'exister.
- Si les filtreurs d'URL ne sont pas sous l'unique responsabilité du RSSI, alors certaines entités de l'entreprise accèderont à des sites interdits par la PSI.
- Si les filtres des firewalls interdisant certains flux IP ne sont pas cohérents sur différents points d'accès à l'Internet, des flux interdits pourront s'introduire.

Supervision :

- Si les logiciels de détection d'intrusions repèrent des attaques sans en alerter l'équipe sécurité, le risque d'attaque réussie est maximal.
- Si une passerelle antivirus détecte et rejette un document infecté, les instances de l'équipe sécurité doivent être alertées avant que l'information infectée ne suive un autre canal.
- Si un seul point d'accès échappe à la supervision centralisée du service sécurité, alors toute la sécurité du SI d'entreprise peut être compromise.

S'il est très difficile de ne rien déléguer, il s'agit de définir clairement les limites et les conditions de cette délégation, qui ne saurait être une délégation de compétences.

Un soin important doit être apporté à la protection des flux de données véhiculés entre la « console sécurité » et les éléments administrés ou supervisés par elle, pour ne pas créer un important trou de sécurité interne.

Parades :

- L'équipe sécurité doit pouvoir de manière sécurisée et fiable avoir accès aux équipements qui constituent le rempart de sécurité entre l'entreprise et l'Internet.
- Cet accès étant critique, il est parfois recommandé d'utiliser un réseau dédié à cet effet (réseau administration de la sécurité, fortement sécurisé), ou si cela est impossible, de mettre en place des mécanismes types VLAN ou chiffrement des échanges.
- Le RSSI doit pouvoir centraliser en un point unique les remontées d'alertes et les outils d'administration des équipements de sécurité du réseau d'entreprise (Antivirus, Firewall, détection d'intrusion, Filtre d'URL, détection de modification d'un serveur WEB d'entreprise…).

- Quand c'est possible, il est souhaitable que le RSSI puisse administrer de façon centralisée (via un Meta annuaire par exemple) les droits d'accès à l'Internet, voire au système d'information au travers de ce même réseau.
- Certaines anomalies récurrentes peuvent être détectées par ce service au travers de l'analyse systématique ou ponctuelle de logs de certaines de ces machines, accessibles à partir de la console sécurité. Une réponse est de prévoir des indicateurs dès la conception de l'application. Souvent, les exploitants réalisent leurs propres agents de surveillance (je ne comprends pas cette phrase), selon les événements qu'ils repèrent lors de l'exploitation.

Critères de Qualité :

- Les outils d'administration doivent être soigneusement choisis de façon à être adaptés au type de personnel en charge du suivi, ou en tout cas un soin important doit être apporté à la formation de celui-ci.

- La PSI doit définir très clairement les alertes qui doivent être « remontées » à la console sécurité, et les actions qui doivent suivre, sous peine de noyer l'administrateur sécurité sous un flot d'informations, ou au contraire de ne pas l'alerter suffisamment et de ne pas déclencher les réactions souhaitables. **Cette décision est stratégique, car il s'agit d'une gestion de risques liée à l'environnement. Les choix en la matière doivent donc se retrouver dans la PSI**. A ce propos, on consultera utilement la fiche n° 13. Identification d'un incident

- Une réelle collaboration doit s'établir entre les personnes en charge du choix des outils de sécurité, de leur installation et de leur administration/supervision, quand cela fait intervenir d'autres équipes que celles du RSSI. Sans cette coopération, la mise en place d'un système performant et facile à administrer/superviser est vouée à l'échec. La mise en place d'un tel système peut être un projet d'entreprise à part entière que doit coordonner la maîtrise d'ouvrage.

- Une bonne administration, comme une bonne supervision, nécessitent une présence 24H/24H de l'équipe sécurité : des alertes doivent déclencher les mêmes réactions à toute heure du jour et de la nuit. Une souche virale dangereuse doit pouvoir être mise à jour rapidement sur l'ensemble des serveurs anti-virus sans attendre le lendemain. On consulte, à ce propos, utilement la Fiche n° 14. Traitement de l'incident

Cette infrastructure technique et humaine nécessite des moyens importants et une organisation sans faille.

Fiche n° 3. Tests d'intrusion : règles en interne et pour la sous-traitance

Définition

Les tests d'intrusion ont pour but de mettre en évidence l'existence de failles de sécurité dans une infrastructure. La mise en œuvre de ces tests d'intrusion demande le respect d'un cadre d'intervention rigoureux. En conséquence, il s'agit de définir, d'assurer et de contrôler la légalité de l'action.

- Définir: rendre l'action conforme au droit (une action intrusive sur un système d'information est manifestement illégale si elle est accomplie à l'insu du responsable du système.
- Assurer: exécuter l'action pour qu'elle reste conforme au droit.
- Contrôler: se protéger des risques liés à l'exécution de cette action

Risques

Le risque majeur de ce type de tests est de divulguer, à l'extérieur de la société, des informations sensibles du système d'information : données sensibles, configuration de l'architecture, etc.

Par ailleurs, il est nécessaire de se prémunir contre des effets de bord (destruction de données, indisponibilité de services) qui doivent être circonscrit notamment dans un environnement de production.

Le but de ces tests est de contrer les activités malveillantes de pirates informatiques. En aucun cas, il ne doit être question de valoriser ce type d'activités. On s'interdira, de ce fait, par déontologie, d'employer ce genre d'individu de façon ponctuelle ou définitive ce qui constituerait une forme de reconnaissance.

De plus, il est nécessaire de prendre en compte le risque d'usure du service d'exploitation qui pourrait être engendré par des tests d'intrusion entrepris selon une fréquence élevée.

Parades

Concernant la fuite d'informations sensibles, il est nécessaire de mettre en place des principes déontologiques et obtenir un engagement explicite des intervenants. En particulier, ces intervenants doivent être identifiés et doivent être engagés sous contrat en bonne et due forme avec l'entreprise ou avec la société externe.

Il est nécessaire de maîtriser les fournisseurs de telles prestations. On préférera donc quelques fournisseurs privilégiés après avoir engagé avec eux une relation de confiance permettant d'obtenir des garanties s'agissant des intervenants et de méthodes employées. Certaines entreprises prestataires de tels services, s'engagent à respecter une "charte de déontologie".

La confidentialité des résultats des tests et des données recueillies au cours de ceux-ci doit être garantie. Ces informations doivent être communiquées aux seules personnes habilitées. L'ensemble des résultats doit être restitué et les éléments recueillis doivent être intégralement remis ou détruits (avec production d'un procès verbal de destruction).

Une campagne de tests d'intrusion doit être planifiée précisément : le périmètre de ces tests doit être décrit avec précision et les périodes de tests clairement définies.

Il est impératif que la campagne de tests soit explicitement autorisée par une personne habilitée et que les actions prévues soient explicitement déclarées au préalable auprès des entités pouvant être impliquées lors de la campagne de tests : organismes de contrôles compétents, exploitants de l'établissement, fournisseurs extérieurs (provider, …). L'utilisation d'une ou plusieurs adresses déclarées et dédiées aux tests est fortement recommandée.

Afin d'assurer une validation des conclusions de ces tests, il est nécessaire de mettre en place une journalisation des actions. Cette journalisation doit être assurée par la personne en charge des tests et

indiquer au moins les informations suivantes : date/heure, intervenant, action (type d'attaque, outil, etc.), adresse(s) source, adresse(s) destination, résultats/conclusions, …

Il est impératif de maîtriser les actions entreprises vis-à-vis des objectifs de la campagne et de s'interdire des actions portant sur des objets non compris dans le périmètre prévu initialement.

Il est proposé que les informations recueillies lors de tests d'intrusion soient placées sous le contrôle du responsable du système d'information qui sera seul responsable:

- de la dénonciation des infractions, crimes ou délits incidemment découverts ;
- de la gestion de l'impact sur l'entité utilisant le système d'information (plus généralement de tous les dégâts contrôlés ou incontrôlés survenus lors de l'opération d'intrusion), avec un droit d'arrêt immédiat et une possibilité de retour à l'état antérieur du système.

Critères de Qualité

Les résultats d'une campagne de tests d'intrusion ne peuvent en aucun cas constituer une preuve concernant la sécurisation du système cible, si ce n'est sur les failles détectées au cours de cette campagne. Par contre, la maîtrise du sujet par les intervenants et la méthodologie employée peuvent apporter un niveau d'assurance quant à la validité des résultats.

Dans le cas des prestations externalisées, les exigences ci-après doivent notamment être respectées :

- Existence d'une méthodologie, d'une charte déontologique (exemple : Charte FPTI).
- Certification de la société par un organisme tiers
- Utilisation de personnels habilités (dans le cas de sociétés ayant autorité pour)
- Eléments de contrôle
- Notoriété sur la place,
- Habilitation de la société et des personnels (dans le cas de sociétés « ayant le besoin d'en connaître »),
- Clauses contractuelles particulières,
- Tests menés dans les locaux de l'établissement dans la mesure du possible.

Fiche n° 4. Suivi : Diffusion des alertes de sécurité et mise à niveau des parades

Définition

La sécurité d'un système peut subir des dégradations du fait de la découverte de failles de sécurité par des utilisateurs internes ou externes. La publication des failles découvertes est une bonne pratique qui impose à tous la mise à niveau rapide des parades.

Risques

La « connectivité globale » augmente le nombre d'intervenants tant au niveau de la recherche des failles potentielles qu'au niveau de leur possible exploitation. La mise en place rapide d'un correctif est devenue une obligation.

La veille sur les failles de sécurité introduit des risques induits de désinformation (directe ou par excès de bruit), de sous-estimation des impacts potentiels, d'instabilité des correctifs appliqués, d'exposition à d'autres faiblesses lors de l'application des correctifs …

Parades

- Collecter régulièrement l'information pertinente auprès des sources connues et fiables (Constructeurs, CERT, Presse, site de veille externe, confrères, …) ou sous-traiter à un prestataire reconnu et agréé.
- Assurer la diffusion de l'information pertinente aux correspondants internes.
- Appliquer immédiatement les mesures conservatoires préconisées en attendant la disponibilité des correctifs avec éventuellement un isolement des machines concernées.
- Evaluer l'exposition réelle de chacune des situations
- Homologuer fonctionnellement et en termes de sécurité les correctifs proposés.
- Mettre en service les correctifs dans le cadre des procédures agréées (authentification, scellement, …)
- Assurer le suivi de la mise en place des parades.
- S'assurer dans les jours suivants de la non-répudiation des correctifs

Critères de Qualité

- Veille : fréquence des recherches, étendue et crédibilité des sources, croisement des informations, compétences des intervenants.
- Diffusion des alertes : liste actualisée et exhaustive des correspondants concernés, acquittement de la réception de certaines alertes, diffusion vers les services d'études et d'audit. Diffusion à la maîtrise d'ouvrage. Délai de diffusion
- Suivi du cycle des versions des logiciels
- Mise en place des correctifs : Maîtrise des procédures, vérification des correctifs, homologation des solutions corrigées

Fiche n° 5. Configuration d'un poste connecté par modem

Définition

Certains postes informatiques isolés nécessitent l'emploi d'un modem pour se connecter sur un réseau, que celui-ci soit privé soit public (Internet, TRANSPAC, …). Cet équipement est de plus en plus souvent intégré au poste informatique, notamment dans le cas de postes portables. Précisons que, bien que ce modem soit généralement adapté à un seul type de liaison (RTC, RNIS, GSM, …), celui-ci peut être utilisé pour se connecter sur de multiples réseaux. Enfin, certaines des fonctionnalités proposées par ces équipements dépendent du pays d'achat voire du pays d'utilisation : gestion des numéros brûlés, fonctionnalités de gestion de la présentation d'appel, etc.

Risques

Trois risques majeurs peuvent être identifiés :

Du point de vue du poste informatique, la présence d'un modem doit être considérée comme un moyen d'accès externe aux ressources de ce poste quand bien même l'utilisateur n'aurait pas volontairement activé la fonction modem. L'utilisation de logiciels de téléphonie (fax, répondeur automatique) conduit à autoriser les appels entrant sur le modem même si le poste ne peut être considéré comme étant à l'initiative des connexions,

Du point de vue de la ressource à laquelle on a accès, l'utilisation d'un Modem conduit à fragiliser le système en autorisant un accès susceptible d'être effectué depuis n'importe où, et tenté par n'importe qui.

Au sens large, tout poste connecté au système d'information de l'établissement par le canal d'un réseau local et disposant d'un modem peut être considéré comme une cible de choix pour qui cherchera à pénétrer dans le système d'information. La compromission de ce poste - par installation d'une porte dérobée - offrira un accès masqué distant sur le système d'information.

Parades

Les parades proposées peuvent se décliner selon 4 catégories:

• **Protections 'amont'** consistant à limiter le risque au niveau du support de communication :

- Utilisation d'une ligne téléphonique inscrite en ligne 'rouge' et sur laquelle la présentation du numéro d'appelant aura été invalidée. L'objectif est de limiter la diffusion d'information permettant à un tiers de rappeler le modem.

- Utilisation d'une ligne dédiée à cette utilisation et restreinte aux appels sortants par le biais d'un contrat de service avec l'opérateur.

• **Protections 'locales'** consistant à limiter le risque au niveau de l'équipement:

- Utilisation d'un profil d'appel stocké dans le modem lorsque cela est possible.

- Utilisation d'un modem disposant de fonctions de stockage local des fax et courrier reçus.

• **Protections 'aval'** consistant à configurer le poste de manière à limiter l'utilisation de services d'agrément:

- invalidation des mécanismes de prise de ligne automatique - fonctions de téléphonie intégrées dans les systèmes d'exploitation bureautique,

- reconfiguration des services et/ou des clients logiciels susceptibles d'accepter automatiquement un appel entrant,

- utilisation de produits de protection de type 'pare-feu personnel' sur les postes munis d'un modem, ces produits étant fournis pré-configurés par l'exploitant,

- mise à disposition de l'utilisateur d'un 'Kit de connexion' comportant l'ensemble des logiciels requis ainsi qu'une configuration sécurisée validée par l'exploitant.

• **Mesures** procédant de la politique de sécurité:

- désactivation des services non strictement utiles sur le poste de travail mais susceptibles d'être utilisés (partages réseaux, services de télémaintenance, de prise de main à distance, …),

- isolation physique des postes munis d'un modem et invalidation logique - par utilisation d'un profil dédié en environnement Windows - des modems intégrés aux portables lorsque ceux-ci sont connectés sur le réseau local

- utilisation préférentielle de lignes numériques dans les locaux afin de restreindre l'utilisation de ces lignes par les modems analogiques encore nombreux,

- gestion en inventaire du parc de modem - et des postes disposant d'un modem intégré - mais aussi des lignes utilisées avec si possible regroupement des accès informatiques externes sur un point fédérateur de type 'NAS',

- prise en compte des modems 'numériques' raccordés aux postes mobiles: GSM, DECT, …

- installation de 'brouilleurs sélectif' GSM dans les locaux à haut niveau de sécurité afin d'interdire l'utilisation de ceux-ci en tant que support de transmission numérique.

Critères de Qualité

Les critères de qualité porteront sur :

- La conformité du modem à la réglementation,

- L'étendue des fonctions de configuration proposées dont notamment les fonctions liées à la sécurité: gestion des numéros brûlés, identification de l'appelant, support de dispositifs de sécurité spécifiques.

- Les élément de contrôle

- Le contrôle de la bonne application des mesures précédentes s'inscrit dans le cadre d'une double stratégie, passive et active :

• **Stratégie passive**

- Recensement exhaustif des liaisons téléphoniques, des modems et des postes portables s'appuyant sur les éléments comptables et d'inventaire,

- Analyse statistique de la consommation des lignes téléphoniques et étude des communications établies depuis ou vers un point de présence d'un FAI,

- Analyse de la configuration des postes à partir d'outils de gestion centralisés,

- Analyse et classification en temps réel des caractéristiques des communications établies par l'intermédiaire du PABX de l'entreprise: voix, fax, données modulées analogiques ou numériques.

• **Stratégie active**

- Sondage actif des lignes téléphoniques externes et internes au moyen d'un outillage ad hoc désormais disponibles chez les éditeurs de produits de sécurité.

Fiche n° 6. Gestion des noms et adresses publiques (DNS, adressage IP)

Définition

La gestion des noms et adresses publiques, correspondance entre des noms mnémoniques alphanumériques et des adresses TCP/IP, est un domaine vital car l'arrêt de son fonctionnement a un impact direct sur la plupart si ce n'est tous les services liés à l'internet.

Risques

Une partie des risques liés à la gestion des noms et adresses publiques est d'ordre technique (détournement de nom de domaine, indisponibilité des machines, …etc), une autre partie, souvent négligée, est d'ordre administratif (renouvellement des enregistrements des noms de domaines, …etc).

Ce risque n'est pas seulement lié au DNS mais surtout à la faiblesse structurelle du protocole IP (absence de garanties de sécurité).

En cas de perte du nom, les internautes ne pourraient plus se connecter aux services proposés que par l'adresse TCP/IP des machines, ce qui ne saurait être pratiqué que par une poignée de spécialistes, éliminant ainsi tous les internautes composant la clientèle.

En cas de détournement d'adresse, les internautes seraient dirigés vers un autre site web.

En cas d'usurpation d'identité d'un site autorisé à accéder à des ressources sensibles, le risque est l'intrusion pure et simple avec tous ses aléas (perte de confidentialité, perte d'intégrité éventuelle, …etc).

En cas d'indisponibilité de la machine (par exemple pour cause d'une attaque par déni de service, aussi appelée attaque par saturation), tout ou partie des clients souhaitant accéder aux ressources sont dans l'impossibilité de le faire. Ce risque peut, dans certains cas, s'étendre aux autres sites que ceux hébergés par l'établissement privant ainsi les internautes de nombreux services internet, dont la navigation.

En cas d'hébergement de DNS à l'extérieur, l'alerte peut être longue à remonter. Il pourrait même arriver de ne pas être averti d'un dysfonctionnement.

Les risques peuvent être une baisse de trafic, une éventuelle fuite des clients vers un établissement concurrent, une impossibilité pour les clients et partenaires d'accéder aux informations et outils avec la rapidité à laquelle ils sont habitués (perte de disponibilité), une perte de crédibilité , une intrusion (perte de confidentialité), …etc.

Parades

- Avoir au moins un DNS en intranet et un DNS internet.
- Installer des machines DNS de manière redondante.
- Faire surveiller ces machines par des logiciels de supervision et de remontée d'alerte.
- Mettre en place des procédures de vérification et de renouvellement d'enregistrement de nom de domaine qui ne se reposent pas sur des alertes à l'instigation des partenaires économiques en ce domaine (fournisseur d'accès, prestataires en sécurité, …etc).
- Se renseigner sur la nature et la qualité des mesures prises par le partenaire en cas d'hébergement de DNS à l'extérieur.

Critères de Qualité

- Séparation des services de DNS intranet et internet.

- Redondance des serveurs DNS.
- Supervision automatisée des serveurs DNS et des matériels associés.
- Remontées d'alertes automatisées vers des responsables désignés.

Eléments de Contrôle

- Organisation de contrôles périodiques définis dans la Politique de Sécurité Internet de l'établissement.
- Tests d'intrusion clairement programmés.

Fiche n° 7. Filtrage IP sur un point d'accès Internet

Définition

La mise en place d'un point d'accès Internet peut être motivée par plusieurs besoins, notamment, la consultation Web pour le personnel, les échanges de messages Internet, les accès nomades (personnel en déplacement, télétravail, …), le commerce électronique (B2B, B2C, …), etc.

Les protocoles utilisés dans ce type de services connaissent des lacunes en matière de sécurité. Aussi est-il nécessaire de mettre en place un filtrage de ces échanges pour protéger les données et services internes et les échanges avec l'extérieur au niveau d'un point d'accès Internet.

Risques

Tous les services de l'Internet reposent sur l'utilisation de la suite de protocoles 'TCP/IP'. Ces protocoles, spécifiés dans les années 80, n'ont pas été conçus pour supporter les exigences de sécurité induites par les besoins actuels. Ainsi, et à titre d'exemple, bien que le protocole IP offre une excellente robustesse face aux problèmes de perte de liaisons, ce protocole n'intègre aucune protection contre la manipulation des informations contenues dans les paquets. Il revient à l'application d'assurer sa propre sécurité.

Universellement adoptés, les protocoles de la suite TCP/IP permettent d'accéder sans contrainte, en l'absence de protection ad hoc, à tout système raccordé à l'Internet sans laisser d'autres traces que l'adresse d'origine, sous réserve que celle-ci n'ait pas été manipulée. Mondialement déployés, les logiciels de gestion de ces protocoles souffrent tous de défauts inhérents à l'absence de normalisation conduisant à l'existence de 'bogues' hélas exploitables pour acquérir le contrôle du système hôte.

Il serait vain de tenter d'établir une liste exhaustive des risques encourus en interconnectant directement un quelconque système informatique sur l'Internet mais il est impensable que ce système ne fasse pas rapidement l'objet d'un sondage destiné à déterminer sa souche - système d'exploitation, version, services actifs, …- et, en conséquence, les vulnérabilités susceptibles d'être exploitées pour en prendre le contrôle, ou le cas échéant, l'inactiver (à quoi renvoie cette dernière phrase). Il est cependant possible de présenter brièvement les risques induits par les protocoles les plus connus:

IP Protocole de niveau réseau n'offrant aucune garantie quant à la fiabilité des informations transportées: le champ contenant l'adresse de la source du paquet peut être manipulé sans conséquence afin de traverser certains filtres **IP**.

ICMP Protocole de contrôle du protocole **IP** susceptible d'être utilisé par effet de bord pour obtenir la cartographie d'un réseau distant, la listes des services actifs sur un système et dans certains suffisamment d'informations pour déterminer avec précision le type, la version et les correctifs appliqués sur celui-ci. Le protocole **ICMP** est, par ailleurs, couramment utilisé comme amplificateur lors d'attaques en déni de service.

TCP Protocole de transport en mode connecté permettant d'atteindre la grande majorité des services utilisés sur Internet: messagerie, Web, … Ce protocole peut être utilisé pour déterminer ouvertement ou de manière masquée l'existence d'un service par la technique du grattage de porte.

UDP Protocole de transport en mode non connecté n'offrant aucune garantie de délivrance, l'acquittement étant réalisé si besoin par l'application. S'il est difficile d'identifier l'existence d'un service derrière un numéro de port **UDP**, ce protocole autorise, en revanche, dans certaines conditions le sondage de systèmes placés derrière certains dispositifs de filtrage. Le protocole **UDP** est couramment utilisé comme vecteur d'attaque en déni de service mais aussi comme protocole de transfert dans les outils d' « attaque distribuée ».

DNS Protocole de service assurant le lien entre le nom d'un système et son adresse. De nombreuses attaques portent sur ce protocole dont l'objet est d'usurper l'identité des sites dûment autorisés. Ce protocole, essentiel au fonctionnement d'un point d'accès, est rarement bloqué. Il peut être, dans certaines conditions, utilisé comme vecteur de transfert de l'information à travers les filtres mis en place.

Parades

Le filtrage effectué au niveau du protocole IP a pour but, non pas d'éliminer tous les risques, mais de restreindre ceux-ci à un niveau acceptable en éliminant au plus tôt toutes les tentatives non conformes à la politique de sécurité de l'établissement. Pour être efficaces, les mécanismes de filtrages doivent être positionnés aux points névralgiques du système d'information: point de raccordement sur le FAI, pivots de routages, points d'entrée sur les réseaux et enfin sur les systèmes hébergeant les applications.

Un filtrage réalisé au niveau du point d'accès Internet doit avoir pour objectifs:

- De rejeter immédiatement et au moindre coût de traitement les tentatives d'accès ne correspondant pas à un service autorisé en conservant une trace précise des conditions du rejet,
- D'assurer l'isolation et le « masquage » des systèmes hébergeant les services et applications proposés aux utilisateurs légitimes. Idéalement, aucune information qui puisse permettre l'identification des systèmes et en conséquence des vulnérabilités ne doit transpercer.
- De parer aux déficiences conceptuelles des protocoles utilisant la pile TCP/IP en rejetant tout élément protocolaire non conforme à la définition couramment acceptée.

Notons que les objectifs ainsi exprimés vont au-delà de la simple fonction de filtrage basée sur les éléments protocolaires disponibles au niveau réseau ou transport - adresses source, destination, protocole, service - et nécessitent de pouvoir assurer un filtrage portant sur les données transportées - URL, adresse de messagerie, nom de communauté SNMP, …

En pratique et pour répondre efficacement aux besoins, un système de filtrage IP doit être constitué d'un ensemble d'équipements intégrés dans une infrastructure mettant en évidence au moins trois zones distinctes: les accès externes, les accès internes, la zone de service - ou **DMZ** - accueillant divers systèmes de relayage - services **WEB**, **Mail**, … - ou de traitement spécialisés - Analyse des contenus, filtrages de URL. Le principe qui guide ce filtrage est le suivant : « tout ce qui n'est pas autorisé explicitement est interdit ».

A chaque équipement est affectée une fonction particulière:

- le routeur 'amont', placé après le routeur du **FAI**, assure, d'une part, une fonction de filtrage de premier niveau, destinée à rejeter tout ce qui peut l'être à ce niveau, et, d'autre part, un masquage de la topologie du réseau. Notons que ce routeur constitue le premier élément sous contrôle permettant d'isoler immédiatement le point d'accès.
- le pare-feu placé en rupture dans le chaîne de liaison établie entre le routeur amont et le réseau Internet assure, d'une part, un filtrage affiné car susceptible d'intégrer des conditions portant sur les données applicatives, et, d'autre part, la création de zones tampons, dites DMZ, permettant d'accueillir les systèmes de relayage. Le rôle de cet équipement est aussi de limiter la propagation des intrusions en assurant le masquage de l'architecture interne (fonction NAT). La gestion des noms est mise en œuvre dans une architecture à double DNS (DNS Internet et DNS interne) permettant encore une fois d'assurer l'intégrité du réseau interne.
- Les sondes réseaux de détection d'intrusion généralement placées de part et d'autre des équipements pare-feu dont le rôle est d'analyser en permanence les flux afin d'y rechercher des traces d'activités anormales. Ces sondes sont susceptibles de réagir en pilotant dynamiquement les règles de filtrage positionnées sur le routeur amont et le(s) pare-feu(x).

Notons, pour finir, que par conception, certains protocoles ne peuvent être partiellement ou totalement filtrés: flux chiffrés, protocoles propriétaires, …

Critères de Qualité

La politique de filtrage doit être décrite précisément et doit être régulièrement réexaminée.

Les principes généraux de la politique de filtrage doivent suivre les recommandations suivantes :

- Tout ce qui n'est pas explicitement autorisé est interdit,

- Seuls les flux strictement essentiels au fonctionnement de l'établissement sont autorisés
- les protocoles de la suite UNIX n'assurant pas une authentification forte (telnet, 'rcommande', x-windows, …) sont déconseillés,
- les protocoles nécessitant l'ouverture d'un canal en retour de la demande de connexion (ftp en mode non passif) sont refusés,
- les protocoles utilisant un numéro de service dynamiquement attribué sont limités au maximum.

Il est nécessaire d'assurer une veille technique sécurité et mettre à jour régulièrement les systèmes d'exploitation et les logiciels de protection : patches firewall, signatures d'attaque pour la détection d'intrusion, signatures anti-virales.

Eléments de contrôle

- Audit récurrent de la configuration et du paramétrage.
- Audit récurrent « en aveugle ».
- Analyse des journaux d'audit du coupe-feu,de la détection d'intrusion et du contrôle de contenu.

Fiche n° 8. La messagerie électronique en toute sécurité Service courrier électronique

Définition

La messagerie électronique est un des services les plus utilisés d'Internet et des réseaux d'entreprise. Elle est constituée d'outils permettant l'envoi et la réception de messages d'information et de fichiers via le réseau. Les outils composant un système de messagerie sont :

- un outil d'édition du message
- un agent d'envoi du message
- un réseau de relais acheminant ces messages de leur source à leur destination
- un agent de récupération des messages
- un outil de lecture du message

Certains outils permettent de remplir plusieurs de ces rôles à la fois :

- le client messagerie édite, envoie, reçoit et présente les messages,
- le serveur de messagerie reçoit, achemine et envoie au destinataire les messages.

Un message électronique est composé de différentes parties remplissant des fonctions différentes. Les parties principales sont :

- l'entête du message
- le corps du message
- les pièces jointes

A chaque outil et section d'un message électronique correspondent des risques différents.

Risques

Composée de plusieurs outils et traitant plusieurs données, la messagerie électronique expose l'établissement à une grande variété de risques. Certains sont la conséquence des technologies utilisées, d'autres sont liées au facteur humain.

Risques associés à la technologie

N'étant pas conçues dans un objectif de sécurité, les normes applicables à la messagerie électronique ne se préoccupent pas des risques. La confidentialité, l'intégrité, l'authenticité, et la non-répudiation, ne sont pas assurés par une messagerie conventionnelle.

Par conséquent, les risques sont :

- perte de confidentialité / publication de données
- perte d'intégrité / modification des données émises
- perte d'authenticité / usurpation d'identité
- perte de données / déni de service

Ces risques sont présents autant lors du transfert d'un message (confidentialité/intégrité en transit) qu'après leur réception (confidentialité/intégrité en stockage). De plus, un message électronique peut contenir un code malicieux pouvant utiliser les services d'un outil pour se faire adresser des données de façon illicite. De

la même manière, le code malicieux peut utiliser l'outil de messagerie pour diffuser d'autres données de façon tout aussi illicite.

Risques associés à l'utilisateur

L'évaluation des risques étant liée à la connaissance des produits et des circuits d'acheminement des messages, l'utilisateur peut éprouver des difficultés à les mesurer. Cela se traduit par un accroissement de la probabilité associée aux risques technologiques.

On citera par exemple :

- l'exécution de code malicieux
- perte de confidentialité
- perte de données/ déni de service
- perte d'authenticité

Détails de chacun des risques

Perte de confidentialité

La confidentialité consiste à assurer que seules les parties concernées par une donnée peuvent accéder à celle-ci. La perte de confidentialité peut résulter de plusieurs situations :

- l'interception

  Tous les échanges entre les postes clients et les serveurs, de même que le stockage des courriers reçus et émis, s'opèrent sans protection. Quiconque accédant aux liens sur lesquels circulent les messages, ou aux ordinateurs sur lesquels ils sont stockés, peut les récupérer directement.

- l'erreur d'adressage

  Tout comme pour le courrier conventionnel, le courrier électronique est adressé à son/ses récipiendaire(s).

La perte de confidentialité peut donc se produire en de nombreuses situations et de plusieurs façons bien différentes. Un utilisateur saisissant mal ce/ces nom(s), confondant deux noms, identiques ou similaires, un code malicieux envoyant lui-même un message ou une personne faisant suivre un courrier à d'autres personnes différentes des destinataires prévus.

La perte d'intégrité se produit lorsqu'un message se voit modifié après avoir été envoyé. La perte d'intégrité peut se produire en plusieurs points, au cours du transit, durant le stockage sur les serveurs ou sur le poste client. Contrairement à la perte de confidentialité, celle-ci résulte rarement d'une erreur de manipulation; elle est surtout causée par une intrusion ou par une erreur de transmission sur le réseau.

Perte d'authenticité / usurpation d'identité

Le contenu des messages électroniques étant complètement libre, chacun peut aisément s'y présenter sous un autre nom.

L'usurpation d'identité peut se faire simplement au niveau du corps du message ou en abusant de l'outil d'expédition d'un autre utilisateur.

L'usurpation d'identité est une attaque particulièrement triviale à réaliser contre une messagerie conventionnelle. Contrairement à la perte d'intégrité, la perte d'authenticité est due à l'utilisateur, rarement à la technologie.

Perte de données / déni de service

La messagerie électronique sur Internet ne garantit pas ses services. Des messages peuvent être perdus ou détruits volontairement par les serveurs pour des raisons d'administration, par exemple. Ces pertes de données surviennent le plus souvent lors d'attaques de type Déni de Service, attaque à laquelle la messagerie électronique est particulièrement vulnérable.

- surcharge d'un système

  Un système de messagerie pourra être surchargé par un surplus de messages causé par des virus qui se répliquent exponentiellement ou par des messages envoyés en très grand nombre (spamming). Des utilisateurs qui font suivre des chaînes de messages en grande quantité peuvent également saturer le système de messagerie. Dans la mesure où la passerelle de messagerie ne peut plus recevoir ou stocker les messages, elle les ignore et ils sont perdus.

- perte d'un serveur.

  Tous les messages en transit, c'est à dire en attente de routage vers les destinataires, sont dans ce cas perdus.

Par ailleurs, les données gardées par les clients risquent aussi d'être perdues en cas de problème sur leur poste.

Exécution de code malicieux

Les messages électroniques peuvent transporter non seulement des informations sous forme de texte, mais aussi des fichiers de toutes sortes. Cela inclut du code binaire exécutable ou des fichiers de commandes, qui peuvent être interprétés par l'outil de visualisation du récipiendaire.

L'authenticité n'étant pas assurée dans une messagerie de base, on ne peut garantir le code qui arrive avec le message. Ces codes, s'ils sont malicieux, peuvent produire de graves dommages :

- intrusion dans le système du client,
- intrusion dans tout le réseau du client.

Bien que quelque fois causée par la technologie, l'exécution de ces codes malicieux est souvent de la responsabilité d'utilisateurs imprudents et/ou inconscients des risques.

Parades

Les risques associés à la messagerie électronique étant de deux ordres (technologie et utilisateur), les solutions de sécurité doivent corriger ou réduire les deux types de risques.

Risques techniques

Permettant la confidentialité, l'intégrité et l'authenticité, la cryptographie, quand elle est bien utilisée, élimine plusieurs risques de la messagerie. Actuellement, la norme S/MIME est la plus utilisée.

Le déploiement d'une messagerie S/MIME demande que chaque partie possède une bi-clé et le certificat correspondant..

S/MIME permet d'atteindre trois objectifs importants : la confidentialité, l'intégrité et l'authenticité. De plus, comme les mécanismes de protection sont inclus dans le message, ils le protègent que ce soit durant le transit ou pendant le stockage.

Les codes malicieux et les Dénis de Service ne sont pas éliminés par un tel outil. Il faut coupler les services de messagerie avec des anti-virus pour le cas des codes malicieux, et faire un contrôle d'accès strict pour réduire les risques de Déni de Service.

Risques humains

La préparation et la mise en place d'une politique d'utilisation de la messagerie électronique sont essentielles. Il s'agit de rappeler ses objectifs, sensibiliser les utilisateurs aux risques des courriers et codes malicieux ainsi qu'à ceux de Déni de Service causés par des messages superflus.

La mise en place de ce type de politique peut être faite par certains outils technologiques, mais demande surtout une surveillance permanente de la messagerie en interdisant :

- la diffusion de messages vers certaines messageries publiques,
- la diffusion d'un message à plus de x (par exemple 50) personnes ou de taille supérieure à y, par exemple 5 méga-octets

Ces mécanismes permettront d'éliminer certains cas d'abus et de détecter les autres.

Les risques opérationnels correspondent à une perte de fichiers, bris de disque dur, perte d'un lien réseau ou autres pannes de ce genre. Les mesures à prendre sont :

- sauvegarde régulière des fichiers de données
- mise en place de plusieurs serveurs pour gérer un même domaine de courrier
- indépendance maximale entre les serveurs (les liens, sauvegardes et autres)
- mise en place de passerelles pour séparer la gestion du courrier interne de celle du courrier externe

Critères de qualité

Pour obtenir une solution de messagerie sécuritaire, il faut s'assurer de remplir tous les besoins de sécurité. Si les messages requièrent la confidentialité ou l'intégrité, comme des demandes de transactions la transmission de codes d'accès ou autres, un chiffrement tel celui par S/MIME est de rigueur.

Son fonctionnement dans le cadre d'un déploiement sur les postes clients présente trois inconvénients majeurs :

- il requiert une infrastructure à clef publique,
- il délocalise les contrôles de codes malicieux et antivirus sur les postes clients
- il ne permet plus le contrôles des messages émis ou reçus dans le cadre du contrôle interne.

L'ajout de S/MIME doit être complété par une sensibilisation des utilisateurs aux risques de la messagerie et une classification de l'information mettant en valeurs les données ne devant pas être transmises sans protection.

Pour régler les problèmes évoqués par une architecture S/MIME cliente, il est préférable pour les établissements de grande taille de s'orienter vers une architecture S/MIME passerelle. Dans cette configuration, le message transite en clair sur le réseau interne de l'entreprise et n'est chiffré que sur Internet. Avantages :

- il ne requiert plus une infrastructure à clef publique, un seul couple clé privée/certificat est délivré à la passerelle,
- les contrôles de codes malicieux et antivirus se font en frontal Internet après que les messages aient été déchiffrés par la passerelle,
- les messages sont accessibles pour les besoins du contrôle interne.

Une solution complète remplira donc en fonction de la politique de sécurité de l'entreprise :

- les besoins de confidentialité, intégrité et authenticité, vis à vis de l'entreprise
- la protection contre les codes malicieux qui sont très dommageables
- la disponibilité du service : sauvegarde des données, autres serveurs en cas d'urgence

- la séparation des rôles de messageries (passerelle pour traiter le courrier externe, serveurs privés pour les messages internes, divisés selon les départements ou autres)

Fiche n° 9. Charte utilisateur d'Internet

Définition

Dans les établissements bancaires, les utilisateurs des accès Internet doivent s'engager individuellement, au travers d'une charte Internet, à ne pas nuire à la réputation et la sécurité des systèmes d'Informations de leur établissement au travers de leur comportement et leurs actes sur le réseau Internet.

Cette fiche technique présente à titre d'exemple une charte Internet qu'un établissement bancaire peut demander à ses utilisateurs d'approuver et de signer avant d'accéder au réseau Internet depuis les installations de l'établissement. Chaque établissement peut établir en fonction de sa culture d'entreprise, de sa problématique technique et des ses contraintes sa propre charte utilisateur Internet. Les services juridiques pourront être utilement associés à l'élaboration du document.

Exemple d'éléments constitutifs d'une charte Internet

ARTICLE 1 - UTILISATEUR

a - La présente déclaration est applicable à toute personne (ci-après « Utilisateur ») autorisée à faire usage des moyens informatiques (ci-après les « Moyens Informatiques ») de la Banque et qui accède ou utilise le réseau Internet. Par « Moyens Informatiques », il faut notamment entendre le matériel (hardware), les fichiers, programmes, logiciels, progiciels (software), ainsi que l'ensemble des moyens d'accès, internes et externes et systèmes de communication (réseaux).

Entrent ainsi dans cette définition tous les services et messageries accessibles par le réseau Internet, grâce au matériel et/ou aux programmes, fichiers, logiciels et progiciels, mis à la disposition de l'Utilisateur par l'établissement.

b - Tout Utilisateur est responsable de l'utilisation qu'il fait des Moyens Informatiques mis à sa disposition par l'établissement.

c - Tout Utilisateur s'engage à respecter les dispositions de la présente déclaration.

ARTICLE 2 - USAGE DES MOYENS INFORMATIQUES

a - L'Utilisateur ne doit employer les Moyens Informatiques de l'établissement que dans le cadre exclusif de son activité professionnelle, et conformément aux procédures et recommandations en vigueur dans l'établissement.
Il lui est interdit d'utiliser ou de charger tout logiciel ou toute donnée qui n'est pas destinée à lui permettre d'exercer son activité.

b - L'usage des messageries Internet mises à disposition par l'établissement est limité aux besoins professionnels.

c - L'accès Internet mis à disposition des Utilisateurs de l'établissement fait l'objet de mesures de protection et de surveillance. Il appartient à chacun de respecter les procédures de connexion mises à sa disposition.
Du fait des dispositifs de protection mis en place par l'établissement pour contrôler tout accès Internet, des traces de toutes les transactions, voire une analyse du contenu des messages échangés, peuvent être utilisées, à des fins de contrôle, en cas d'incident ou de malveillance.

d - N'étant pas un moyen de communication sécurisé, Internet n'offre aucune garantie de bon acheminement, d'intégrité ni de confidentialité des messages transportés. Il importe donc d'utiliser ce vecteur de communication à bon escient.
Il est interdit d'utiliser ce canal pour transmettre des programmes de l'établissement. Il est

également interdit, pour des raisons d'intégrité et de confidentialité, d'utiliser Internet pour transmettre des fichiers sans avoir auparavant mis en œuvre des moyens adaptés : chiffrement, signature électronique.
L'Utilisateur doit être conscient qu'il ne peut avoir la certitude qu'un message reçu provient bien de l'émetteur mentionné dans le message.

e - L'Utilisateur cessant, même provisoirement, d'exercer ses fonctions à l'établissement, ne doit plus utiliser les moyens, ressources et réseaux informatiques qui étaient mis à sa disposition, sauf accord écrit de l'établissement, ceux-ci incluant les boites aux lettres des messageries mises à sa disposition par l'établissement.

f - Toute cessation définitive de ses activités au sein de l'établissement oblige l'Utilisateur à restituer les copies de sauvegarde de données, fichiers et logiciels de l'établissement ainsi que les codes d'accès à ses messageries.

ARTICLE 3 - OBLIGATION DE LOYAUTE, RESPECT DE LA CONFIDENTIALITE ET DE L'INTEGRITE DES DONNEES

a - L'Utilisateur ne devra ni accéder ni tenter d'accéder ni aider un tiers à accéder à tout ou partie des Moyens Informatiques, sans y avoir été expressément et préalablement autorisé.

ARTICLE 4 - OBLIGATION DE VIGILANCE

a - L'Utilisateur est soumis à une obligation de vigilance à l'égard des Moyens Informatiques mis à sa disposition et notamment à l'égard des fichiers contenant des informations nominatives et/ou sensibles. Il doit respecter la confidentialité et l'intégrité des Moyens Informatiques mis à sa disposition, et notamment les fichiers et les programmes placés sous sa responsabilité.
A cette fin, il est notamment tenu de ne pas quitter son poste de travail en laissant une session en cours, sans avoir au préalable activé un contrôle d'accès de son poste de travail protégé par mot de passe.

b - Sont formellement interdits, même temporairement :
- le fait d'émettre sur Internet des informations confidentielles;
- le fait de communiquer ses codes d'accès personnels à d'autres utilisateurs ou à des tiers, sauf dans le cadre de la procédure de cessation définitive d'activité;
- l'utilisation des codes d'accès d'un tiers, même avec son consentement.

c - Tout fichier en provenance d'Internet, y compris les fichiers attachés à un message électronique, peut être porteur de virus ou autre code dangereux.
L'Utilisateur doit prendre toutes les précautions qui s'imposent et ne traiter ce type de fichier qu'en connaissance de cause.
Il ne doit pas ouvrir de document joint à un message non sollicité ou de nature non professionnelle.

d - L'Utilisateur n'a pas la certitude que les informations consultées sur Internet soient exactes. Il ne doit les diffuser, le cas échéant, sans s'être assuré au préalable de leur véracité.

ARTICLE 5- RESPECT DES DROITS D'AUTEURS

a - Sauf autorisation explicite de l'établissement, il est interdit à tout utilisateur, toute copie de documents, normes, méthodes, logiciels et polices, images, séquences, etc., hors du cadre de ses fonctions ou à destination d'un utilisateur non autorisé.
L'utilisation de toute copie enfreignant les lois sur le droit d'Auteur est également interdite.

b - L'Utilisateur reconnaît que les Moyens Informatiques, conçus ou réalisés dans le cadre de ses activités professionnelles, ne sont pas sa propriété, sauf autorisation expresse de l'établissement,

c - L'acquisition de progiciels au moyen d' Internet est soumis :

- au respect des Lois actuelles et à venir, et notamment :
  Loi 57-298 : propriété des œuvres de l'esprit
  Loi 85-660 : protection des logiciels
  Loi 94-361 : protection juridique des programmes d'ordinateur
- au code de la propriété intellectuelle et,
- au respect des directives et règlements intérieurs actuels et à venir.

ARTICLE 6 - SECRET BANCAIRE :

La mise à disposition des Moyens Informatiques par l'établissement, ne dispense pas l'Utilisateur de devoir respecter les règles de déontologie et le secret professionnel, auxquels il reste tenu.

ARTICLE 7 - SANCTIONS :

L'Utilisateur qui ne respecte pas ces règles sera sanctionné conformément au règlement intérieur de l'établissement et susceptible d'être poursuivi devant les juridictions pénales.

.

Fiche n° 10. Service navigation WEB

Définition

Souvent confondu avec l'Internet, le Web consiste en une grande quantité de serveurs publiant des données de toutes sortes. Le Web est aujourd'hui omniprésent, incontournable, multifonctions, si bien que les risques liés à la navigation ne sont plus négligeables. Le but de la sécurité est de permettre des accès licites et sécurisés à cette ressource.

Risques

Composés de plusieurs outils et traitant plusieurs types de données, les mécanismes de la navigation Web présentent une grande variété de risques. Certains sont dus aux technologies, d'autres à des facteurs humains.

Risques associés à la technologie

Le but premier du Web étant de publier des données, il a été conçu pour permettre un maximum de possibilités à ses utilisateurs.

Le principal risque technologique provient de la forme sous laquelle sont transportées les données. Elle peut être malicieuse et conduire à une intrusion dans le système client et dans tout le réseau qui l'entoure.

Chaque jour, les sites Web contiennent davantage de code actif. Un code actif est un programme exécuté par le client, à la demande du serveur et présentant des fonctions avancées. Ainsi, un serveur malicieux peut faire exécuter un code compromettant à ses visiteurs. Parmi les codes actifs, on trouve ActiveX, Java, VBScript, JavaScript …

Développé par Microsoft, ActiveX et VBScript représentent un risque majeur pour le client puisqu'ils ont été intégrés à même le système d'exploitation Windows et peuvent faire sans limite tout ce que Windows peut faire : formater un disque, lire des données, expédier des données …

Java a été développé par Sun et est particulièrement utilisé sur Internet. Contrairement à ActiveX, Java est exécuté dans un environnement restreint et contrôlé. Un programme Java ne pourra pas formater un disque dur, par exemple, sans la permission explicite de l'utilisateur. JavaScript, développé par Netscape, est aussi un code actif à faible risque, exécuté dans un environnement restreint et contrôlé.

Un autre risque de la navigation Web intervient lors du téléchargement de fichiers. Les fichiers exécutables téléchargés peuvent être infectés par des virus.

Pour naviguer sur le Web, d'autres services sont requis, comme DNS, permettant de traduire les noms des sites Web en adresse IP. Dans la situation où un serveur DNS est compromis, le logiciel de navigation de l'utilisateur accédera à des ressources autres que celles demandées. L'utilisateur peut ainsi recevoir de fausses données, accéder à des ressources d'un tout autre type ou même envoyer des données à une mauvaise adresse..

Un troisième risque vient de ce que l'on ne peut pas être sûr que l'on est bien sur le site recherché (ne serait-ce que par une attaque sur le DNS -voir fiche 6). Les informations recueillies sur Internet doivent donc être vérifiées.

En résumé, les risques techniques de navigation sur le Web sont :

- l'exécution de code actif, conduisant à
  - l'intrusion dans le système du client et son réseau
  - la perte de confidentialité sur le poste local ou en émission
  - la perte d'intégrité sur le poste local ou en émission

  - la perte d'authenticité / usurpation d'identité
  - la perte de données / déni de service
- les virus
- la connexion à une fausse adresse et l'émission de données vers cette fausse adresse ou la réception de fausses données

Risques associés aux utilisateurs

Le Web publiant des données de toutes sortes, les utilisateurs peuvent être tentés d'accéder à certaines données, peu recommandables, soit sans lien avec leur activité professionnelle, soit illégales... Bien que certains de ces accès soient délibérés, ils ne le sont pas toujours (faute de frappe dans une adresse, lien annonçant autre chose que ce sur quoi il dirige…)

Les clients sont identifiés auprès des serveurs visités par leur adresse IP. Ces accès au nom de l'entreprise (avec les adresses IP de l'entreprise) peuvent conduire à des situations embarrassantes.

Pour ces deux raisons il est nécessaire de contrôler les ressources accédées.

Les utilisateurs peuvent également télécharger des fichiers de grande taille (audio, vidéo …) sans rapport avec leur activité professionnelle et ainsi accaparer à eux seuls une grande partie de la bande passante.

Les codes actifs sont omniprésents et offrent plusieurs services utiles. Cependant, leur exécution n'est pas toujours sécurisée. Aussi le navigateur doit-il demander à l'utilisateur l'autorisation d'exécuter le code en question. Pourtant,, cette précaution est peu utile. Même si les utilisateurs sont interrogés par leur navigateur avant l'exécution du code, ceux-ci répondent le plus souvent par l'affirmative sans comprendre les risques encourus. Or, le plus souvent, chaque permission accordée correspond à un accès potentiel sans limite à tout l'ordinateur et son réseau. Les utilisateurs doivent donc être formés aux risques encourus pour éviter que de telles permissions soient accordées de façon précipitée.

Parades

Le premier outil d'un accès Web sécurisé est le serveur proxy. Placé entre le client et le serveur, il prend le plein contrôle sur l'accès en cours. Sa présence est pratiquement essentielle puisqu'il est le seul outil qui puisse filtrer une connexion au Web. Une fois en place, le serveur proxy pourra :

- contrôler quelles ressources sont accessibles ou non aux utilisateurs en se fondant sur les adresses IP des serveurs distants ou les noms de domaines (listes noires),
- retirer les codes actifs dangereux,
- retirer les virus,
- contrôler le type des fichiers téléchargés,
- filtrer sur mot clé.

Un serveur proxy sera cependant incapable de filtrer les données échangées via SSL puisque celles-ci sont chiffrées au moment où il tente de les contrôler. C'est pour cette raison qu'une bonne configuration du poste client est de rigueur.

Commençant par utiliser un navigateur de qualité suffisante, le poste client doit être configuré pour refuser sans question tous les codes actifs dangereux, notamment ActiveX. Les autres codes devront demander une permission explicite avant de s'exécuter. Mais, comme décrit plus haut, l'utilisateur doit être formé pour que ce contrôle soit valable.

Les utilisateurs doivent donc prendre conscience des risques encourus par leurs faits et gestes.. Ils doivent comprendre ce qu'ils font en acceptant un certificat SSL, en chargeant une nouvelle clé racine ou encore en permettant l'exécution d'un code actif. Ils doivent de plus comprendre les limites dans lesquelles s'inscrit leur accès Internet. La signature d'une charte ou d'un additif au règlement intérieur, l'authentification (forte) et le suivi de leurs connexions peut leur faire prendre conscience de leur responsabilité.

Le poste client devra également être muni d'un anti-virus à jour complétant celui du serveur proxy.

Critères de Qualité

Pour obtenir un accès au Web sécuritaire, il faut s'assurer de remplir tous les besoins de sécurité. Le serveur proxy est essentiel et il faut ensuite définir la granularité avec laquelle on souhaite appliquer les règles.

Utilisant un navigateur de qualité, les clients doivent être configurés pour réduire les risques, surtout ceux associés au code actif. Les postes clients doivent aussi être muni d'un logiciel anti-virus pour accroître la protection contre ce risque. En dernier lieu, les clients doivent comprendre les risques de la navigation sur le Web.

Une solution complète remplira donc dans l'ordre :

- la mise en place d'un serveur proxy qui limitera les accès autant que nécessaire (listes noires),
- la protection contre les codes actifs autant sur le serveur proxy que sur les postes clients,
- la configuration des postes clients (anti-virus, codes actifs, navigateur de qualité),
- la mise en place de l'authentification et le suivi des logs sur l'utilisation du Web par les collaborateurs,
- la formation des utilisateurs,
- l'utilisation conjointe d'autres outils sur le serveur proxy (anti-virus, filtre sur le type de fichiers, filtre sur mots clés …).

Fiche n° 11. Architecture d'un point d'interconnexion Internet

Définition

La mise en place d'un point d'accès Internet peut être motivée par plusieurs besoins, notamment la consultation Web pour le personnel, les échanges de messages Internet, les accès nomades (personnel en déplacement, télétravail, …), le commerce électronique (B2B, B2C, …), etc.

L'architecture à mettre en place dépend des types de services à assurer. Cette fiche prend en compte la problématique engendrée par l'ensemble de ces services.

Risques

Un des principaux risques est celui d'intrusion du système d'information interne depuis l'Internet. Une intrusion peut engendrer :

- une perte de confidentialité des données sensibles de l'organisme
- une perte d'intégrité (données, détournement de sites Web, postes de travail),
- une perte de disponibilité (Déni de service)

Si le point de raccordement avec Internet permet un accès à distance pour une certaine catégorie de personnel, le risque majeur est l'usurpation d'identité. De la même façon, une application de commerce électronique doit assurer vis-à-vis de clients ou de fournisseurs une sécurisation des échanges (authentification des interlocuteurs, des données échangées, non-répudiation…).

Par ailleurs, les données transitant sur Internet sont susceptibles d'être écoutées à des fins de piratage ou d'espionnage économique. Les données sensibles transmises par ce canal doivent donc être protégées (en intégrité, en confidentialité). Enfin, une fonction de non-répudiation peut être requise pour certains types d'échanges.

Du fait du grand nombre d'internautes et de la diffusion de codes ou techniques d'attaques, la probabilité d'occurrence des attaques doit être considérée comme très importante.

Parades

La définition de l'architecture d'un point d'interconnexion Internet doit impérativement respecter un ensemble de règles fondamentales en partant d'un constat simple : la sécurité absolue n'existe pas. Il est en effet impossible, à coût et délai contraint, de définir une architecture n'offrant aucun point faible.

En conséquence, il est fondamental de définir une architecture optimale, c'est à dire, une activité qui offre, d'une part, une capacité de résistance calculée au regard des risques et des attaques réputés connus, et, qui offre, d'autre part, un environnement de supervision permettant de réagir en temps et heure en cas d'alerte de sécurité.

Une isolation maximale doit être recherchée entre le domaine non contrôlé (accès externes) et les ressources de l'entreprise. L'interface entre ces deux domaines constitue le périmètre de sécurité. Cette isolation doit, autant que possible, prendre en compte la nature et la dynamique des flux traversant l'interface.

Le réseau interne de l'entreprise peut présenter une sensibilité variable et il peut être nécessaire par ailleurs de différencier des sous-réseaux internes selon leur de la sensibilité du réseau interne.

Les fonctionnalités offertes doivent être logiquement et physiquement regroupées afin de minimiser la propagation d'une menace induite par la vulnérabilité d'un des composants à l'intérieur du périmètre de sécurité. La logique de regroupement retenue doit prendre en compte le principe du maillon le plus faible : les fonctions les plus vulnérables doivent être circonscrites dans une zone dédié (Zone Tampon ou DMZ).

La mesure de la vulnérabilité doit prendre en compte non seulement la fonctionnalité mais aussi l'environnement supportant celle-ci : système d'exploitation, services connexes,...

La résistance et la robustesse du point d'accès sont des qualités évolutives et dynamiques devant faire l'objet d'un contrôle régulier. L'architecture technique doit en conséquence être évolutive et adaptative, c'est à dire modulaire et non monolithique.

Afin de faciliter l'analyse de l'architecture fonctionnelle du point d'interconnexion Internet, les fonctionnalités génériques seront regroupées en 5 catégories :

Services techniques. Cette catégorie regroupera l'ensemble des fonctionnalités permettant d'offrir les services techniques élémentaires du point d'accès à l'exception des fonctionnalités spécifiques de sécurité,

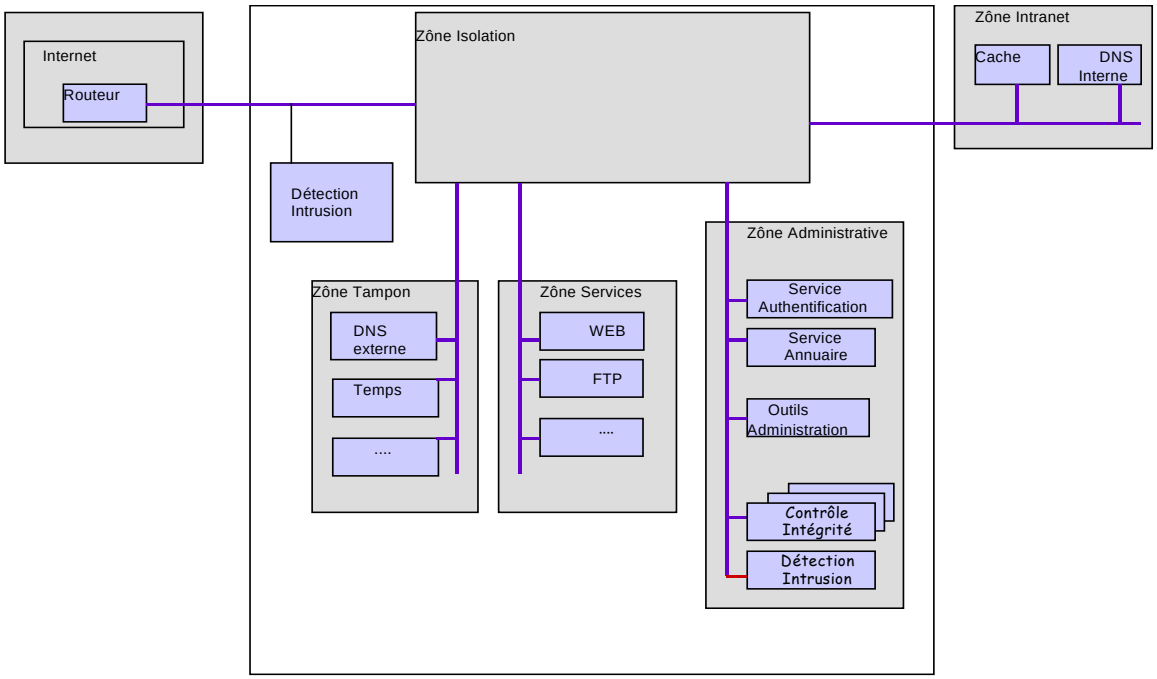
Services hébergés. Cette catégorie regroupera l'ensemble des fonctionnalités permettant d'offrir un ensemble de services à valeur ajouté offerts à l'utilisateur du point d'accès et directement hébergés sur la plate-forme technique constituant celui-ci,

Services sécurité. Cette catégorie regroupera l'ensemble des fonctionnalités participant directement à la sécurisation logique et physique du point d'accès et de l'infrastructure de service associée,

Services Administration. Cette catégorie regroupera l'ensemble des fonctionnalités, sécurité comprise, permettant d'assurer l'administration et l'exploitation des différents composants logiques ou physiques constituant le point d'accès,

Services Supervision. Cette catégorie regroupera l'ensemble des fonctionnalités, sécurité comprise, permettant d'assurer la surveillance du bon fonctionnement du point d'accès et de l'infrastructure de service associée.

Le schéma synoptique suivant présente une architecture susceptible de répondre à l'ensemble des besoins précédemment exprimés.



Point d'interconnexion Internet

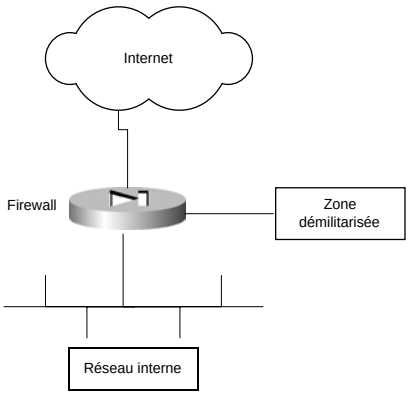
Le système de détection d'intrusions est divisée en deux composants :

- Une sonde placée en amont de la zone d'isolation

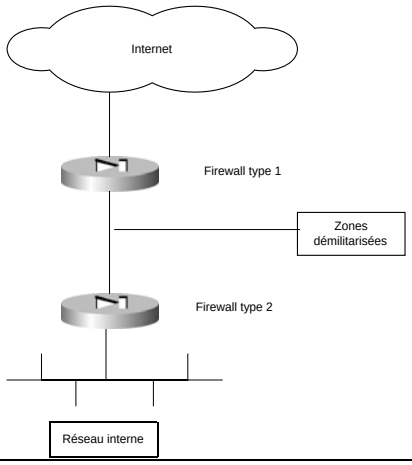
- Une sonde supervisant le trafic dans la zone d'isolation ou en aval de celle-ci.

Pour des raisons de coûts, ces deux composants sont parfois regroupés. Cette architecture n'est pas conseillée car elle induit une vulnérabilité potentielle de contournement de la zone d'isolation via la sonde elle-même.

La zone d'isolation est construite en fonction des objectifs pesant sur le point d'interconnexion.



Architecture à un FireWall



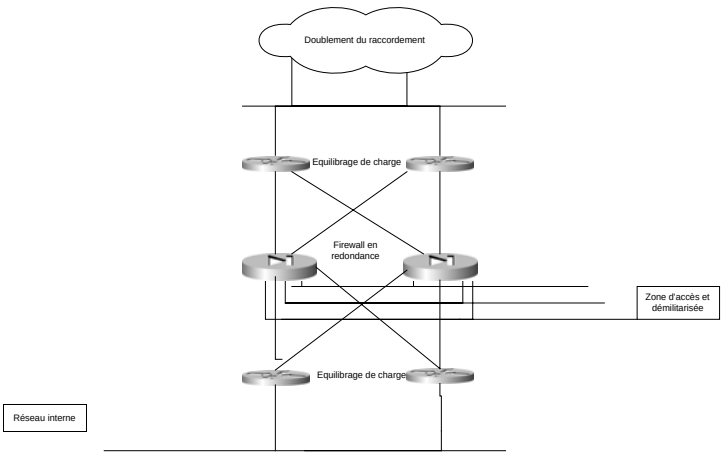
Architecture 3 tiers : 2 firewalls de technologies différentes

L'architecture est construite avec un sas assuré par deux coupe-feux de deux technologies différentes, permettant ainsi une complémentarité fonctionnelle de sécurité.

Le coupe-feu avant travaille plus spécialement sur les trames réseaux reçues d'Internet.

Le deuxième firewall est un firewall de technologie proxy-relay permettant de tester plus finement les commandes dans les différents protocoles. De plus, le mode relayage, permet, à la réception d'un flux, d'analyser la requête, puis de la relayer en la ré-émettant vers la cible.

Architecture à redondance : haute disponibilité



La montée en charge de ce type d'architecture ne doit pas remettre en cause les principes de conception.

La haute disponibilité d'une architecture se bâtit à l'aide de commutateurs à équilibrage de charges. Ces commutateurs sont eux-mêmes redondants. Cette configuration permet de dupliquer les moyens de filtrage ou de services de façon simple.

Critères de Qualité

Utilisation d'une approche méthodologique pour déterminer les objectifs de sécurité.

Définition d'une architecture modulaire et évolutive.

Elément de contrôle

- Supervision de la sécurité.
- Audit de la configuration
- Audit des procédures de suivi des incidents.
- Tests d'intrusions.

Fiche n° 12. Configuration, contrôle et surveillance d'un serveur exposé à l'Internet

Définition

Un serveur exposé à l'Internet permet l'échange d'information avec l'extérieur. Il peut offrir des services tels que la messagerie, la consultation Web (publishing), l'échange de fichiers, le commerce électronique (B2B, B2C, etc.).

Qu'il s'agisse de l'architecture d'accès à ces services ou des moyens de protection amont (pare-feu, DMZ, …), la sécurité repose également sur la qualité de l'architecture et sur la configuration des serveurs. En effet, le filtrage d'un protocole comme http par un équipement coupe-feu ne permet pas de se protéger contre une vulnérabilité induite par une erreur de codage dans un script CGI.

Risques

Un serveur exposé à l'Internet doit être et rester dans une configuration sécurisée.

Les principaux risques sont :

- Une mise en place dans une configuration non sécurisée,
- Une perte de sécurité liée à la publication de nouvelles vulnérabilités sur ses différents composants,
- Une régression suite à une opération de maintenance.

Bien que le serveur soit dans une configuration sécurisée, des vulnérabilités dans des applications qu'il héberge peuvent provoquer des failles de sécurité, il est donc indispensable de vérifier régulièrement la sécurité du serveur.

Parades

Un serveur ne doit pas être directement accessible depuis Internet. Aussi le place-t-on en général derrière un équipement de filtrage (voir la fiche 8), dans une zone démilitarisée (DMZ).

De plus, il est nécessaire d'assurer une configuration sécurisée de ce serveur en prenant en compte :

- La configuration de cet OS (fermeture des services non nécessaires, gestion des comptes et groupes utilisateurs, ne pas installer de compilateur (gcc, etc.) ou d'interpréteurs de commandes (Perl), choix de protocoles qui peuvent être sécurisés).
- Le choix des logiciels installés : serveurs Web, serveurs de mail, serveur FTP, DNS, etc.
- Le choix des outils et protocoles de supervision,
- La configuration de ces logiciels.

Le maintien du paramétrage sécurisé des serveurs doit être assuré dans la durée. Aussi, la configuration doit être réexaminée tout au long de la vie du serveur, en particulier, lors des phases de maintenance, suite à une panne HardWare, une mise à jour du système d'exploitation ou une mise à jour de logiciels ou middleware.

Il est donc impératif de documenter les paramétrages systèmes et logiciels dans une fiche. Cette fiche doit être mise à jour en fonction de l'évolution du serveur. Cette fiche permet le référencement de la politique de sécurité système mise en œuvre qui doit être vérifiée périodiquement et à chaque modification. Les mises à jour logicielles et matérielles doivent re-qualifiées avant mise en exploitation sur une plate-forme dédiée.

Une supervision sécurité de ce serveur doit être assurée de façon récurrente

Mise à jour des versions en fonction des attaques publiées : une veille technologique est assurée sur les différentes annonces sécurité

Audit récurrent de configuration : cet audit peut se faire « à la main » mais peut être assisté par des outils d'audit de politique de sécurité. Ces audits peuvent être sous-traités à des sociétés spécialisées sous condition de mettre en place un cadre d'intervention rigoureux (voir fiche 3).

Audit des événements journalisés : cela se fait par l'analyse des différents outils de journalisation. Certains outils permettent une centralisation de ces journaux et une analyse de corrélations entre différents événements.

Contrôle d'intégrité : il est nécessaire de vérifier l'intégrité des objets sensibles hébergés sur le serveurs : données, pages Web, etc.

Il s'agit de mettre en place une détection d'intrusion sur des logiciels installés sur le serveur (Host IDS).

Par ailleurs, il faut s'assurer de pouvoir le restaurer de manière satisfaisante (qualité, temps de réaction, etc.), ce qui implique un système de sauvegarde.

Cette supervision doit être documentée dans le cadre de procédures. En particulier, le traitement des incidents et les procédures d'escalade doivent être documentées.

Critères de Qualité

Documentation détaillée de la politique sécurité système.

Surveillance automatique du respect de cette politique.

Détection d'intrusion système.

Surveillance automatique de l'intégrité des logiciels et données stockés.

Elément de contrôle

Tests récurrents d'intrusion.

Audit des procédures de suivi d'incidents.

Fiche n° 13. Identification d'un incident

Définition

Il existe plusieurs façon d'identifier les incidents en fonction de l'analyse que l'on souhaite en faire.

La présente fiche a pour objectif de définir des axes, - qui ne se veulent pas exhaustifs - en matière d'identification des incidents afin de mettre en place une organisation et des moyens pour détecter et identifier un incident de Sécurité Internet.

Plus précisément, dans le cadre de la Sécurité Internet, un incident peut se définir selon trois approches :

- Par constat, comme un dysfonctionnement par rapport à une situation stable connue et définie comme « normale »

- Par référencement ; comme correspond à un élément d'une liste de référencement des incidents (historique d'entreprise et veille technologique)

- Par concept : Comme une violation de la Politique de Sécurité Internet

Différentes catégories peuvent être établies :

- Déni de service

- Intrusion

- Virus (réel)

- Hoax (faux virus)

- Vol d'identifiants

- Vol de mots de passe

- Vol d'information

- Modification d'information

- Destruction d'information

- Détournement de site

- Usurpation d'identité

- Détournement de la puissance de calcul

- … etc

Pour chacune de ces catégories (voire pour des sous-catégories plus précises ou des incidents déjà référencés), il s'agit de définir les critères DICP affectés, la gravité potentielle, l'urgence de l'intervention, les responsables à contacter, les actions de "premier secours" et leur ordre d'application, en fonction de différents critères (géographiques, horaires et autres)...

Risques

Les risques associés sont nombreux en cas de non-identification d'un incident:

- Subir des dommages sans en avoir conscience
- Etre dans l'incapacité de déceler un incident
- Véhiculer une image négative auprès de tiers (partenaires, clients, … etc)
- Ne pas réagir efficacement ou assez rapidement par manque de préparation, d'information, de moyens ou de ressources

- Créer des effets de panique injustifiés par une communication non-contrôlée et/ou un manque d'analyse des évènements
- Désinformer (diffusion de mauvaises informations)
- … etc

Parades

Chaînes de traitement

Des listes de contacts et de leurs suppléants, éventuellement par type d'incident, seront établies par l'établissement à l'intention des équipes de détection.

Les chaînes de traitement définies comporteront au moins un point de contrôle humain (on évitera la diffusion entièrement automatisée d'alertes généralisées afin d'éviter les effets de panique injustifiés).

Cinématique de remontées d'alertes

Un schéma des canaux de communication pourra être établi montrant les intervenants, leurs modes de remontées d'information, les délais minima et maxima de ces transferts, mettant ainsi en évidence les éventuels oublis et le délai minimum global avant traitement.

Compétence

Le personnel sera suffisamment formé à la réaction en cas de détection et informé sur les suites à donner à une détection avérée.

Sensibilisation des utilisateurs

Les utilisateurs devront être sensibilisés à la nécessité de remonter toute anomalie qu'ils constateraient dans leurs environnements à leur responsable définis dans la chaîne de contact.

Adaptation des systèmes réalisés par des tiers

Les recommandations et mises en place réalisées par les prestataires devront être suffisamment claires et adaptables pour pouvoir faire systématiquement l'objet de légères modifications, lors de leur mise en place finale en production. On rendra ainsi insuffisante la connaissance que ces acteurs extérieurs ont du projet pour permettre un contournement direct des systèmes de sécurité mis en place

Critères de Qualité

Types des incidents

Il s'agit de distinguer trois types de détection, selon qu'elle intervient a priori, immédiatement et a posteriori.

Détection	Constat	Importance	Urgence
A priori	- Potentiel - L'incident n'est pas encore survenu, sa détection s'est fait à l'occasion d'un contrôle de révision des systèmes ou de l'analyse des protections actuelles par rapport à une nouvelle menace déclarée	Casuistique	Casuistique
Immédiate	- En temps réel - De nombreux outils proposent	Vraisemblablement forte	Vraisemblablement forte

	aujourd'hui ce type de service, le plus souvent dans les domaines de déni de service, d'intrusion et de détection de virus		
A posteriori	- Historique - Il est utile d'alimenter une base de connaissance avec ces constats afin de mieux se prémunir contre des types de risques similaires qui pourraient survenir	Vraisemblablement faible	Vraisemblablement faible

La détection devra déclencher immédiatement un processus d'identification le plus précis possible afin:

- d'alerter les compétences les plus adaptées pour la résolution du type d'incident
- de circonscrire l'incident géographiquement (si son mode de propagation, s'il existe, est connu)
- de circonscrire l'incident fonctionnellement (si le mode de fonctionnement de sa cause est déterminé)
- de mettre en place une éventuelle cellule de crise.

Description d'un incident

Les incidents seront répertoriés par types.

Exemple de contenu

- Horodatage
- Qualification de l'incident
- Sens de l'agression : entrante ou sortante
- Statut de la menace : potentielle, tentative ou avérée
- Codification DICP
- Gravité
- Urgence
- Priorité
- Estimation de l'étendue des dommages
- Personnes à contacter
- Signature des intervenants, visa des responsables

Agression entrante ou sortante ?

On prendra soin d'opérer une première distinction, souvent négligée. L'agression est-elle entrante (phénomène le plus souvent constaté), ou bien sortante (la menace provient de l'établissement aux dépens du monde extérieur) ? Ce deuxième cas de figure, bien que rare, est à considérer car il peut entraîner des conséquences graves :

- Détérioration de l'image de l'établissement
- Perte de crédibilité
- Réactions – souvent violentes - des victimes extérieures touchées
- …etc.

Tentative ou réalité de la menace ?

Une autre distinction, à effectuer, est de déterminer s'il s'agit d'une tentative d'attaque ou bien d'une attaque avérée et plus généralement si la menace reste potentielle ou bien si elle est ou a été active. Bien évidemment, les mesures curatives s'avéreront très différentes, qu'il s'agisse du degré d'urgence de leur mise en place et des les chemins de diffusion qu'elles emprunteront.

Intoxication ou réalité ?

Les fausses alertes étant très consommatrices de ressources (c'est même là le principe des virus de type "canular") et très démotivantes pour les personnels sensibilisés, il est important que les remontées d'alertes subissent une phase de validation avant d'être diffusée hors des services techniques spécialisés.

Portée des incidents

Il sera utile de définir des priorités sur les incidents afin de pouvoir organiser les réactions en fonction:

- D'importance des dégâts potentiels
- De la rapidité de propagation des dommages
- De la quantité et qualité des resources disponibles au moment de l'incident pour le traiter avec efficacité
- D'un éventuel coefficient de sensibilité de la zone touchée qui pourra varier en fonction non seulement de l'estimation qui en sera faite à l'origine mais également en fonction d'actions commercialles ou marketing ponctuelles.

Codification DICP

On pourra judicieusement utiliser la méthode d'évaluation DICP.

Pour rappel, les quatre facteurs de sécurité définis par DICP sont :

Disponibilité	Aptitude des systèmes à remplir une fonction dans des conditions prédéfinies d'horaires, de délais et de performances.
Intégrité	Propriété qui assure que des informations sont identiques en deux points, dans le temps et dans l'espace.
Confidentialité	Propriété qui assure la tenue secrète des informations avec accès aux seules entités autorisées.
Preuve	(et contrôle). Faculté de vérifier le bon déroulement d'une fonction.

Eléments de Contrôle

Révisions

Les risques et les outils de prévention, détection et éradication évoluant très rapidement en ce domaine, l'établissement devra réviser ses procédures de réaction aux incidents de façon régulière.

Simulations d'alertes

Il pourra être organisé des simulations d'alertes afin de tester la réactivité de la chaîne de traitement et son bon déroulement.

Validation

Compte tenu de l'importance stratégique de ces procédures et de leurs répercussions sur l'établissement, un système de validation des procédures définies devra être organisé.

Exemples de questions auxquelles répondre :

- Qui déclenche la procédure de gestion d'un incident, c'est à dire, qui décide que l'on est en présence d'un incident ?
- Quels sont les éléments de décision ?

.

Fiche n° 14. Traitement de l'incident

Définition

Mettre en place une organisation et des moyens pour traiter un incident de Sécurité Internet.

Voir également la fiche technique N° 13 "Identification d'un incident".

Risques

Les risques associés sont nombreux en cas de non-traitement d'un incident :

- Subir des pertes de confidentialité, de disponibilité, d'intégrité, …etc
- Etre dans l'incapacité de contingenter un incident
- Véhiculer une image négative auprès de tiers (partenaires, clients, … etc)
- … etc

Parades

Organisation des équipes

Les équipes de traitement d'incidents informatiques de sécurité pourront être organisées a minima de deux niveaux. Le premier niveau est composé personnel pourvu de compétences de base en matière de sécurité. Son rôle principal est un rôle de surveillance, d'identification, de vérification et de remontée d'alerte. Ce premier niveau doit être hautement disponible et réactif. Le deuxième niveau, composé de personnel aux compétences pointues en matière de sécurité, sera chargé, pour sa part, de confirmer l'identification et le niveau de gravité ainsi que de la résolution du problème.

Les équipes de traitement d'incidents informatiques de sécurité pourront être distinctes des équipes qui ont travaillé sur la définition et la mise en place des systèmes de protection, bien que ces dernières seront le plus souvent sollicitées, si ce n'est pour leur connaissance approfondie des systèmes, du moins pour la modification de ces systèmes afin de procéder à la résolution et/ou la non-reproduction de l'incident.

En fonction de la gravité, peut être constituée une "cellule de crise" pour gérer l'incident.

Compétence d'intervention

Le personnel sera suffisamment formé au traitement des incidents et informé sur les constantes évolutions en ce domaine. En cas d'incertitude, il sera fait appel à une expertise externe sous la supervision d'un responsable de l'établissement.

Estimation des dégâts et de leur étendue avant résolution

Les processus d'éradication, en particlier peuvent se révéler longs. Aussi, il sera utile de procéder à une estimation de l'étendue des dommages par un moyen différent de celui qui a servi au processus d'identification.

Il s'agit ici de constats à effectuer sur le terrain, même à distance, et c'est également souvent l'occasion d'obtenir quelques premières informations sur ce qu'ont ressenti les victimes des dégâts.

Recueil et analyse d'informations

Il s'agit d'obtenir un maximum d'informations sur les différentes actions possibles face à l'incident. Un compromis devant être trouvé entre la rapidité de réponse et la pertinence de la réponse.

Typologie

Pour un traitement plus rapide des incidents référencés, ceux-ci seront répertoriés par types. (voir fiche n°13 Identification des incidents)

Protection des preuves et des enregistrements de l'activité

Afin de constituer :

- une base de connaissance sur les incidents
- une collecte d'éléments pouvant servir dans un dossier de justice

Il s'agit de collecter un maximum d'information sur l'incident dans son état "actif" (avant neutralisation). Néanmoins ici aussi, un compromis devra être trouvé entre l'accumulation de connaissance sur la menace et la rapidité de son traitement.

Pour cela, en fonction du type d'incident, la mise en place d'un « pot de miel » (serveur leurre) peut faciliter la collecte d'information sur l'incident sans porter préjudice au système d'information.

Communication

Les régles et principes de communication doivent être établis préalablement par grandes catégories d'incident, en fonction de la cible, afin de n'avoir à s'attacher qu'au contenu descriptif de l'incident lorsque celui survient.

- ➢ Communication interne
- ❖ Le traitement d'un incident relatif à la sécurité étant que très rarement sans incidence sur la qualité de service normalement délivré, on veillera à inclure très tôt dans la chaîne d'information de cet incident les responsables des directions susceptibles d'en ressentir les effets.
- ❖ On distinguera les comptes rendus techniques, qui devront être le plus précis et détaillés possible, et dont le stockage sera naturellement soumis aux règles en vigueur dans l'établissement concernant les documents hautement confidentiels, des documents d'information diffusés en interne, plus synthétiques, qui pour leur part ne devront jamais contenir d'informations explicites ou implicites, qui puissent fournir des indications sur le caractère secret des systèmes de protection en place, fussent-ils été défaillants ou non.
- ➢ Communication externe
- ❖ Instances légales
- ❖ Si l'incident est de nature à appeler l'application de la loi (domaines du pénal, du commercial ou du civil), les autorités concernées devront naturellement être alertées au plus vite en présence d'un responsable de l'établissement habilité à traiter les problèmes de cette nature.
- ❖ Partenaires extérieurs
  - Organisations nationales : Police.
  - Organisations internationales: CERT, Interpol, … etc
  - Fournisseurs de solutions antivirales
  - Fournisseurs de solutions de détection d'intrusions
  - Fournisseurs de solutions de protection contre les intrusions
  - Partenaires économiques privilégiés
  - … etc

- Relations publiques - Communiqués de presse

  La diffusion publique de commentaires sur un incident devra se faire en accord avec le service Communication de l'entreprise qui apportera son concours.

Tests

Afin d'en mesurer l'efficacité et les éventuels effets secondaires, il est sage, lorsque le cas le permet, d'exécuter des tests avant de procéder massivement au déploiement d'actions d'endiguement et d'éradication.

Endiguement

Il est souvent plus facile et parfois rapide d'endiguer un incident que de l'éradiquer. Aussi est-il conseillé de procéder à un arrêt de la propagation le plus rapidement possible. Cela ne gêne que rarement l'étude de l'incident, qui peut être menée parallèlement.

Le but en cas de propagation, sera d'isoler la ou les zones touchées par l'incident.

On distinguera deux stratégies majeures:

- soit en isolant chaque zone touchée par l'incident des zones saines
- soit en isolant globalement des ensembles de zones contenant des sous-zones infectées et saines de la source de l'incident. Cette approche peut s'avérer plus facile à mettre en œuvre, surtout dans le cas de propagations rapides (intrusions, virus, …etc)

Eradication

Une fois l'incident correctement identifié et ses comportements et dommages caractérisés, un processus d'éradication pourra être mis au point et déployé après un minimum de tests.

Reprise de l'activité

Une fois les dommages subis étudiés, les processus de reprise d'activité pourront être mis en œ, dans la mesure où cet état a pu être déterminé, sont autant de mesures dont la complexité de mise en œuvre est, au cas par cas, variable.

Critères de Qualité

Préparation

Il est important de préparer des réponses types - du moins les premières réactions à avoir en fonction des types d'incidents répertoriés (voir fiche 13). Cette préparation est validée, d'une part, au cours de tests d'autre part enrichie après chaque incident (voir fiche 15)

Dans cette préparation, il est nécessaire d'identifier par type d'incident, les éléments pertinents permettant :

- de reconnaître le type d'incident,

- de mesurer son impact (voir fiche 15)

Tests

Les tests avant déploiement seront un gage de réussite et de satisfaction de la population touchée par l'incident après traitement.

Suivi

L'établissement déterminera dans ses procédures les modalités de suivi de cet incident et de ses variantes si elles peuvent exister.

On peut envisager, si les ressources le permettent, la mise en place pour une durée déterminée d'une veille technique proactive visant à prévenir des éventuelles variantes de cet incident.

Organisation des traitements

Le traitement sera organisé en fonction des priorités définies par la politique de sécurité de l'établissement et du type d'incident identifié, notamment en fonction:

- de l'importance des dégâts potentiels
- de la rapidité de propagation des dommages
- de la quantité et de la qualité des resources disponibles au moment de l'incident pour le traiter avec efficacité
- d'un éventuel coefficient de sensibilité de la zone touchée qui pourra varier en fonction non seulement de l'estimation qui en sera faite à l'origine mais également en fonction d'actions commercialles ou marketing ponctuelles.
- et, naturellement, de la codification DICP.

Eléments de Contrôle

Simulations d'alertes

Il pourra être organisé des simulations d'alertes afin de tester la réactivité de la chaîne de traitement et son bon déroulement.

Exemples de questions auxquelles répondre :

En préparation

- Qui prévient qui ?
- Quels sont les décideurs ? Leurs suppléants ?
- Qui est en mesure de connaître les implications d'une réponse à un incident ?
- Qui doit être prévenu ?
- En combien de temps l'intervenant X peut-il être contacté ?
- Quel sont les moyens de savoir qu'une remontée d'information n'a pas atteint son destinataire ?
- Quel est le délai supplémentaire en cas d'absence du contact principal ?
- … etc.

En traitement de l'incident

- Les responsables ont-ils été contactés ?
- L'étendue des dommages est-elle connue ?
- L'incident est-il déjà répertorié ?
- L'efficacité de la solution déployée a-t-elle été testée ?

.

Fiche n° 15. Evaluation des dommages post-incident : historisation

Définition

Mettre en place une organisation et des moyens pour évaluer les conséquences d'un incident de Sécurité Internet après son traitement.

Voir également la fiche technique N° 13 "Identification d'un incident".

Risques

Les risques associés sont nombreux en cas de non-évaluation postérieure au traitement d'un incident:

- Avoir déployé un traitement inefficace
- Avoir mal contingenté un incident
- Véhiculer une image négative auprès de tiers (collaborateurs, partenaires, clients, …etc)

Parades

Estimation des dégâts et de leur étendue après résolution

Outre la vérification de la pertinence de la solution mise en œuvre, ces constats seront également l'occasion d'obtenir des informations sur ce qu'ont ressenti l a posteriori les victimes. On pourra parfois en déduire l'efficacité de méthodes de prévention actuelles et futures.

Enrichissement de la base de connaissance

L'établissement gagnera à stocker de manière systématique et organisée l'historique de ses incidents et de leurs résolutions.

Partage d'expérience

Il est recommandé de partager les retours d'expérience avec les organisations nationales et internationales qui collectent ces informations et en publient gratuitement les synthèses, ainsi qu'avec tous les autres partenaires privilégiés que l'établissement aura pris soin de déterminer.

L'établissement prendra naturellement soin de rendre génériques les informations véhiculées par ses retours d'expérience afin de ne pas faire de ces partages d'expérience une source de fuite d'informations confidentielles.

Recherche active d'éventuelles variantes futures

Les attaques largement diffusées répondant souvent à des phénomènes de "mode", il sera dans l'intérêt de l'établissement d'avoir une démarche préventive à l'encontre de variantes potentielles de l'incident subi.

Mise en place de méthodes et outils actualisés et/ou nouveaux

La synthèse de l'incident devra déboucher sur une série de décisions et vraisemblablement d'actions visant à améliorer les défenses de l'établissement.

- Mises à jour des matériels et logiciels
- Acquisition de nouveaux systèmes
- Révision des méthodes et procédures

- Création d'équipes dédiées
- Campagnes d'information
- … etc

Historisation: Exemple de contenu

- Horodatage
- Etendue de l'étude
- Etendue des dommages
- Eventuelles fiches de témoignage
- Statistiques
- Personnes à contacter
- Signature des responsables

Critères de Qualité

Tests

Les tests avant déploiement seront un gage de réussite et de satisfaction de la population touchée par l'incident après traitement.

Suivi

L'établissement déterminera, dans ses procédures, une durée de suivi de cet incident et de ses variantes si elles peuvent exister.

On peut envisager si les ressources le permettent la mise en place pour une durée déterminée d'une veille technique proactive visant à prévenir des éventuelles variantes de cet incident.

Eléments de Contrôle

Qualité des recueils d'informations

Des contrôles croisés entre différents recueils d'informations permettront de vérifier la qualité de ces recueils.

Comparaisons

Il pourra être effectué des comparaisons avec les expériences enregistrées dans la base de connaissance.

Fiche n° 16. Hébergement extérieur d'un Site Web

Définition

Un établissement bancaire ou financier peut être amené à confier à un prestataire externe l'hébergement d'un ou plusieurs de ses sites Web.

Cette fiche technique présente un ensemble de mesures qu'il est souhaitable de vérifier et / ou d'imposer avant même de prendre tout engagement avec un prestataire externe. L'objectif de ces mesures étant de procurer au(x) site(s) hébergé(s), un niveau de sécurité acceptable.

L'établissement bancaire doit mettre par écrit ses exigences et les mesures requises dans un cahier des charges référencé par un contrat.

Une condition préalable avant la signature de tout contrat, est que l'hébergeur accepte les audits commandités par l'établissement bancaire ou financier, exigence réglementaire au titre du contrôle interne. La réglementation bancaire et financière, et en particulier la décision n° 99-07 du Conseil des marchés financiers, doit être respectée.

Ces mesures sont à sélectionner et à adapter en fonction du contexte précis de mise en œuvre (site web transactionnel par exemple).

La protection des équipements de l'établissement

● Toutes les mesures de sécurité physique du site (accès, protection des équipements…) doivent être prises, ce qui inclut des tests de contrôle et leur périodicité.

● Les droits d'accès aux locaux font l'objet d'une gestion rigoureuse (organisationnelle et technique) : cohérence des droits et privilèges par rapport aux fonctions exercées, gestion des mouvements de personnels, gestion des mots de passe, désactivation des badges périmés, volés ou perdus…

● Les équipements dédiés à l'établissement, actifs et de secours, sont situés dans des locaux différents alimentés en énergie par des dispositifs séparés.

● Les équipements dédiés à l'établissement, actifs et de secours, sont situés dans de sites différents.

● Les équipements dédiés à l'établissement sont placés dans des locaux à accès restreint, réservés à l'établissement.

● Les armoires « matériel » et baies techniques sont fermées à clé et les clés sont conservées dans des locaux adaptés et uniquement accessibles via une procédure d'obtention.

● L'établissement a connaissance des droits d'accès sur les machines constituant son dispositif.

Accès aux systèmes et aux informations de l'établissement

● Les droits d'accès aux systèmes font l'objet d'une gestion rigoureuse (organisationnelle et technique) : cohérence des droits et privilèges par rapport aux fonctions exercées, gestion des mouvements de personnels, gestion des mots de passe…

● L'établissement a connaissance des droits d'accès sur les systèmes constituant son dispositif.

● Le personnel sensible ayant accès à des informations relevant du secret bancaire devra faire partie du personnel de l'établissement ou être dûment habilité par l'établissement. Son rôle sera clairement défini. Il devra s'engager par écrit au respect des règles, édictées par l'établissement, se rapportant à son domaine de compétence.

● Le nombre des intervenants sur un composant du système est limité aux seules personnes susceptibles d'intervenir. L'établissement est informé de leur identité.

● Des moyens de cryptographie (chiffrement) sont utilisés de façon à garantir la confidentialité des informations stockées. La clé de chiffrement devra être sécurisée.

● La mise en place de tous les moyens de création d'un espace de confiance de type PKI (Public Key Infrastructure), permet de garantir la non-répudiation des transactions.

● L'utilisateur dispose d'une authentification forte pour prouver son identité.

● Le client a la possibilité de changer lui-même son mot de passe.

● Les mots de passe triviaux sont refusés par le logiciel.

● Les logiciels refusent un mot de passe identique à l'ancien à la demande de renouvellement.

● Le changement de mot de passe périodique est fortement recommandé.

● Des moyens de scellement sont utilisés de façon à garantir l'intégrité des informations stockées et transmises.

● Des moyens de chiffrement sont utilisés de façon à garantir la confidentialité des informations transmises.

● Partage des rôles : le programmeur du *token* (objet physique permettant l'authentification forte) n'a pas connaissance de l'identité du client.

● Partage des rôles : l'administrateur système n'a pas accès à la base de données.

● Les intervenants ont les connaissances requises en matière de sécurité des systèmes et les responsabilités sont clairement définies.

● Le prestataire externe doit mettre en place les moyens garantissant l'intégrité des personnels occupant des fonctions sensibles (confidentialité, discrétion, etc.) tels que notamment des procédures strictes lors de l'embauche, contrat avec clauses spécifiques de déontologie y compris pour les intervenants externes (maintenance, sous-traitance, prestataires de services, intérimaires, stagiaires…).

● Tout intervenant sur des données sensibles doit garantir la confidentialité de ces dernières, lors des processus de transformation, de transport et de stockage quel que soit le type de support d'exploitation, de sauvegarde, d'archivage...

● Les modalités d'intervention en production sur des données sensibles sont décrites dans une note circulaire contenant les procédures ad hoc. Ce mode opératoire sera publié pour l'ensemble du personnel concerné et devra être scrupuleusement respecté. Ces procédures devront répondre aux exigences propres du domaine de production en terme de confidentialité, d'intégrité des données et de piste d'audit.

L'infrastructure

● Un site web public passif est créé. Il ne contient ni code transactionnel ni code de création de pages dynamiques.

● Le site web public est abrité par un serveur Web public qui ne contient aucun outil dont la nécessité n'est pas absolue. Le serveur Web public ne contient que des données statiques.

● Un serveur http invisible de l'Internet : le *Web Application Server* (WAS) construit les requêtes envoyées aux systèmes back-end et produit les pages HTML dynamiques sollicitées par le serveur web public.

● La mise à jour de pages HTML directement sur le serveur public n'est pas possible.

● Un premier coupe-feu, appelé *bastion,* n'autorise l'accès au serveur web public, depuis l'Internet, que par le seul protocole HTTP ou HTTPS.

● Un second coupe-feu dont la technologie diffère du bastion, de part la marque et l'origine du « moteur », protège :

- Le segment de réseau dédié à l'établissement où se trouve le site web public, de tout accès non autorisé depuis le réseau interne de l'hébergeur,

- Le segment de réseau où se trouvent les serveurs dédiés à l'établissement (serveur de données, WAS…).

● Une passerelle de niveau application analyse les commandes passées au serveur web public.

● Un système détecteur d'intrusion (IDS) réseau, indétectable, doit être placé sur chaque segment du réseau où se trouve un serveur de l'établissement.

● Une rupture de protocole intervient avant l'accès au système *back end.*

● La base d'authentification ne doit pas être chez l'hébergeur prestataire de services.

● L'hébergeur doit mettre en place les moyens garantissant l'intégrité des configurations et informations des éléments actifs de l'architecture de sécurité au moyen d'une technique de scellement par exemple.

● Les infrastructures destinées à la clientèle de l'hébergeur sont découplées du réseau interne de l'hébergeur pour tout accès à l'Internet, de façon à strictement réserver la bande passante nécessaire au bon fonctionnement des applications de sa clientèle. De cette manière et à titre d'exemple, tout comportement abusif du personnel de l'hébergeur en regard de l'Internet (téléchargement de fichiers volumineux) n'aura aucun effet néfaste sur le trafic de sa clientèle.

● L'hébergeur doit être relié à l'Internet par deux fournisseurs d'accès (un opérationnel et un en secours).

● Les fournisseurs d'accès doivent garantir une qualité de service en rapport avec les objectifs de disponibilité du projet :

➢ Taux de disponibilité.

➢ Les modalités de calcul du taux de disponibilité seront précisées.

➢ Le fournisseur doit fournir un tableau de bord de suivi de la disponibilité et justifier les incidents.

➢ Débit réservé au client (l'établissement).

➢ Les fournisseurs d'accès Internet doivent doubler les points d'accès.

● Les matériels sont redondants et un dispositif assure une copie en temps réel sur la machine dite « miroir ».

● Les matériels sont choisis dans la gamme « haute disponibilité ».

● Les matériels actifs et de secours sont placés sur des réseaux locaux dépendants d'infrastructures différentes.

● Les serveurs s'identifient mutuellement.

Les systèmes dédiés à l'établissement

● Les systèmes ont subi une opération de durcissement logiciel conforme aux meilleures pratiques dans le domaine de la sécurité des systèmes d'information.

● Les systèmes ont subi un test de résistance aux attaques avant sa mise en relation avec l'Internet.

● L'intégrité des serveurs est régulièrement vérifiée par un système automatique capable de donner l'alerte.

● Les outils de détection d'intrusion système sont installés et activés dans la ou les machines considérées, les traces doivent être conservées pour être produites à l'établissement selon requête ou en cas d'alerte, laquelle doit être signalée et traitée en temps réel.

● Un journal de connexions (succès, connexion, déconnexion, échec) est produit et analysé par du personnel compétent.

● Le journal des connexions est transmis à l'établissement.

● Un plan de sauvegarde/récupération des données doit exister et les procédures de récupération des systèmes et données sont documentées et testées.

● Le contenu des systèmes bénéficie des techniques de *disaster recovery*.

● L'administrateur du système est secondé par une personne compétente disponible en cas de besoin.

● Le taux d'utilisation des systèmes (CPU, mémoire, nombres de processus…) fait l'objet d'un suivi.

● Les systèmes bénéficient des mises à jour nécessaires au maintien de leur résistance aux intrusions et de leur disponibilité.

● L'hébergeur assure la veille technologique des logiciels systèmes.

● L'hébergeur assure la veille sécuritaire et identifie les mises à jour à appliquer aux systèmes dédiés à l'établissement ainsi qu'à ceux utilisés pour sécuriser l'architecture réseaux (Firewall, IDS…).

● L'administrateur système contrôle les équipements logiciel régulièrement.

● Toute intervention sur un ou des systèmes sensibles devra être journalisée.

● Toute intervention sur des données sensibles devra être journalisée.

● Les machines supportant les logiciels applicatifs, de supervision ou de sécurité de l'établissement sont dédiés à l'établissement.

L'applicatif

● L'établissement est informé des évolutions de code applicatif.

● Une procédure de qualification de code applicatif est rédigée selon trois axes : fonctions, performances et sécurité, impliquant l'établissement et une personne compétente en sécurité des systèmes d'information.

● Le code en cours de qualification n'est pas testé sur un serveur accessible au public.

● Le fournisseur du code applicatif s'appuie sur une gestion rigoureuse de la qualité et une procédure de vérification de la non-régression des modules.

● La production de code est normalisée de manière à ce que les initiatives des développeurs ne mettent pas en jeu la sécurité du dispositif.

● La production de code, les tests, la recette et la production doivent être dans des environnements séparés et le passage de l'un à l'autre doit être strictement contrôlé.

● Le logiciel transactionnel de l'hébergeur détecte les doublons.

● Le logiciel transactionnel du conservateur détecte les doublons.

● L'état général du site est contrôlé automatiquement par l'établissement, au moins toutes les deux heures sur les heures de bourse.

● Le logiciel assure une vérification automatique de la cohérence de l'ordre passé, notamment de la limite de prix dont il est assorti avec les conditions du marché. Si le système constate une incohérence, un mécanisme de blocage automatique d'entrée des ordres est activé. Le client est avisé par un message à l'écran des raisons du blocage. ● Chaque ordre est référencé d'une manière unique.

● Un ordre conditionnel (vente des titres à un prix fixé par exemple) doit être confirmé quotidiennement (ou autre périodicité) Une fenêtre dédiée s'affichant sur la page Web pourra rappeler au client l'enregistrement de son ordre conditionnel.

● La réglementation fiscale en matière de produits boursiers est scrupuleusement respectée.

● Le logiciel assure un suivi statistique des transactions du client pour pouvoir déceler les transactions atypiques et permettre d'en aviser automatiquement le responsable opérationnel de manière à ce que ce dernier puisse le cas échéant, contacter son client pour s'assurer de la validité de l'ordre ou des ordres passés.

● Des contrôles programmés doivent être mis en œuvre s'agissant de la gestion des interdictions, des limites, des cohérences, des seuils, des quantités, des montants…

● Un rapprochement est possible entre les ordres émis par l'hébergeur et les ordres traités par le Conservateur des Titres.

● Un journal des ordres est produit et transmis à l'établissement.

● Les journaux de suivi des ordres sont extérieurs aux serveurs de gestion des ordres.

● L'hébergeur ne stocke et ne reçoit (de la part des établissements bancaires) aucune donnée nominative.

● L'hébergeur ne connaît pas l'identité des clients.

● La page d'accueil du service invite le client à signaler tout incident.

● Le système permet un suivi des encours sur l'interface WEB présentée au client.

● Le système permet de faire des simulations de phénomènes boursiers afin de pouvoir anticiper les risques.

● Les traitements concourant au fonctionnement de l'ensemble du processus informatisé ne doivent pas être désynchronisés par rapport aux exigences fonctionnelles de métier.

● Le carnet d'ordre doit permettre aux différents acteurs impliqués dans le processus de suivre les différents états de l'ordre depuis la saisie jusqu'à la mise à disposition sur le Web de l'avis d'exécution.

● Il doit y avoir une parfaite cohérence des informations de type WEB avec celles dont dispose le responsable opérationnel hors contexte Internet, de manière à ce que ce dernier puisse avoir tous les éléments nécessaires lui permettant de gérer une situation en mode dégradé avec son client (passage d'ordres par téléphone si Internet non disponible).

● L'hébergeur doit, en liaison avec l'établissement, mettre en œuvre un système automatisé de vérification de compte. En cas d'insuffisance des provisions et des couvertures, le système doit assurer le blocage de l'entrée de l'ordre. Le client est avisé, à la lecture de l'écran, des raisons du blocage et il est appelé à régulariser sa situation.

● Deux connexions simultanées avec le même compte sont rendues techniquement impossible.

Les incidents

● Une procédure de traitement des incidents est établie entre l'établissement et son sous-traitant.

● Un dispositif permet d'alerter une personne compétente qui soit en mesure d'agir de jour comme de nuit en cas d'alerte sur l'un des maillons du dispositif.

● Toutes les mesures de continuité de service doivent être prises incluant des tests de contrôle et leur périodicité.

● Un centre d'appel permanent reçoit les demandes de renseignements des clients, y compris celles concernant les incidents.

● Le centre d'appel destiné aux clients doit avoir une vue de l'état de l'ensemble des systèmes impliqués (hébergeur, ISP, Conservation des Titres, back office banque).

● Le centre d'appel doit être en mesure de gérer une surcharge suite à une indisponibilité de longue durée.

● Une procédure dégradée prévoit le passage des ordres par téléphone ou fax.

● Une ou plusieurs personnes à l'établissement, aptes à comprendre les comptes-rendus, les messages d'alerte et à proposer un plan d'action, sont nommées.

● Le client a tous les moyens à sa disposition pour faire opposition sur son contrat Internet de manière à pouvoir faire bloquer dans les meilleurs délais l'accès à son compte en cas de besoin (perte de son token, vol de son ordinateur portable, suspicion d'usurpation d'identité…).

Choix et obligations de l'hébergeur

● Un Cahier des Charges relatif au choix du sous-traitant (l'hébergeur) doit exister.

● Le choix de l'hébergeur s'est appuyé sur le cahier des charges « CHOIX D'UN SOUS-TRAITANT » faisant partie de la POLITIQUE DE SECURITE DE L'ÉTABLISSEMENT.

● Les sous-traitants doivent garantir que toutes les mesures de sécurité ont été prises.

● L'établissement peut faire auditer les infrastructures techniques du prestataire externe impliquées dans son activité, ainsi que l'organisation qui permet de garantir le bon fonctionnement de ces infrastructures.

● Lors de l'établissement contractuel de la relation avec un prestataire externe, le PLAN QUALITE ET SECURITE doit être formalisé d'un commun accord.

● Tous les systèmes impliqués dans le processus doivent être auditables et en mesure de fournir les alertes sur leurs dysfonctionnements (en particulier pour le centre d'appel).

● La maintenance des matériels et des logiciels de fournisseurs doit faire l'objet d'un contrat détaillé incluant le respect de mesures de sécurité adéquates.

● Le personnel est informé par un code de « bonne conduite » sur les dispositions à prendre en cas de saturation possible du réseau, en termes de respect de la confidentialité des informations et de devoir d'alerte en cas de dysfonctionnement…

● Les processus sensibles (exploitation des ordinateurs, supervision du réseau, développement…) sont mis en œuvre par du personnel suffisant et compétent.

● Chaque responsable de fonctions doit mettre en place les moyens et mesures pour garantir :

➢ La continuité de service de ses fonctions (accès aux biens et informations, systèmes, équipements, nécessaires à l'accomplissement de la fonction).

➢ La confidentialité des informations et la protection des accès aux ressources sensibles.

● La couverture des services de support aux clients et de surveillance des infrastructures techniques (logicielles et matérielles) doit être adaptée à la disponibilité requise par le métier.

.

Fiche n° 17. Poste Itinérant : Soumission aux règles de Sécurité applicables aux postes fixes

Définition

Les postes itinérants sont très fréquemment utilisés pour le télé-travail, la télémaintenance, les astreintes, les accès en extranet, le nomadisme…

Ces postes présentent des risques pour les systèmes d'informations avec lesquels ils sont en relation. Aussi, est-il nécessaire de les soumettre aux règles de sécurité applicables aux postes fixes.

Voir aussi la fiche N°5 configuration d'un poste avec modem.

Risques

Un poste itinérant peut être utilisé à des fins personnelles (téléchargement de logiciels, consultation de sites internet douteux…) ce qui peut mettre en péril l'intégrité du poste itinérant ainsi que l'image de marque de l'établissement.

Le vol d'un poste itinérant peut engendrer la perte de la confidentialité des informations stockées.

Le poste itinérant peut être utilisé pour s'introduire dans le réseau interne de l'établissement à des fins malveillantes.
Par exemple, la connexion directe du poste itinérant à l'internet peut aboutir à sa contamination (Cheval de Troie, virus, ver…) et lorsque le poste itinérant est relié au réseau local de l'entreprise, il compromet la sécurité du système d'informations.

Parades

Les postes itinérants doivent respecter les standards techniques de l'établissement et ce, en matière d'équipements logiciels de protection (antivirus…).

Tout poste itinérant doit accéder à l'Internet via le réseau interne et ses équipements de protection (pare feux, proxys…).

Le disque dur du poste itinérant doit être chiffré au niveau secteur. Sont ainsi protégés :

- Les fichiers confidentiels qui auraient pu être stockés localement (répliques de bases courrier, bases de données clientèle, contrats…).
- Les réglages favorisant l'intrusion dans le réseau interne de l'établissement : numéros de téléphone du serveur d'accès distant avec identifiants et mots de passe, fichiers éventuellement créés par l'utilisateur et contenant des mots de passe…

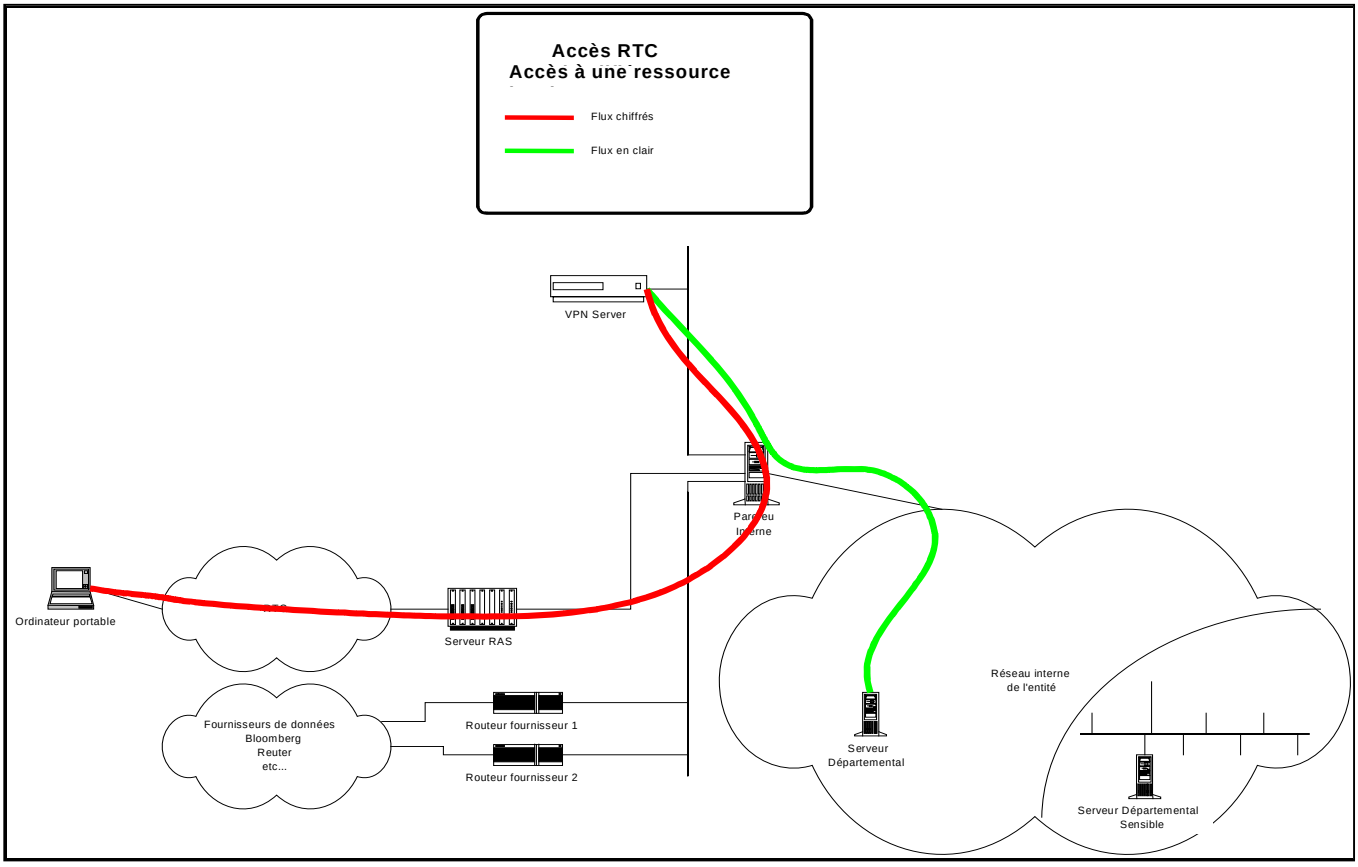
L'accès au réseau interne est soumis à une phase d'authentification forte.

Tout accès à des données confidentielles non chiffrées ou à des systèmes avec des privilèges élevés doit se faire au travers d'un canal chiffré.

Les utilisateurs des postes itinérants doivent être sensibilisés aux risques encourus.

L'utilisateur ne doit pas avoir la possibilité de désactiver les protections mises en œuvres au niveau du poste itinérant.

Exemple


Accès RTC
Accès à une ressource
Flux chiffrés
Flux en clair
VPN Server
Pare-feu
Interne
Ordinateur portable
Serveur RAS
Fournisseurs de données
Bloomberg
Reuter
etc...
Routeur fournisseur 1
Routeur fournisseur 2
Réseau interne
de l'entité
Serveur
Départemental
Serveur Départemental
Sensible

Glossaire

CERT	Computer Emergency Response Team : Organisations mises en place un peu partout dans le monde pour assister leurs adhérents en matière de sécurité des réseaux. Regroupés au sein de la structure FIRST
CGI	Common Gateway Interface : Spécification concernant l'interfaçage d'un serveur Web avec une application.
Cookie:	Elément de donnée stocké sur le poste de travail par un serveur WEB et contenant l'identification du serveur, de la page ainsi que tout autre donnée utile au concepteur du site ou de l'application.
DDOS	Distributed Denial Of Service : Technique d'attaque répartie cherchant à obtenir un déni de service.
DMZ	DeMilitarized Zone : Zone démilitarisée ; zone d'échange entre deux réseaux de sensibilités différentes. Le contrôle des échanges est assuré par un dispositif de coupe-feu.
DNS	Domain Name Server : Service permettant la traduction de l'adresse IP d'un ordinateur en son nom et inversement. Le nom constitue un moyen mnémotechnique pour faciliter l'accès aux informations et l'envoi de messages.
DOS	Denial Of Service : déni de service
FAI	Fournisseur d'Accès Internet : en anglais "ISP" Internet Service Provider et " Provider " fournisseur.
FPTI	Fédération des Professionnels des Tests Intrusifs.
FTP	File Transfer Protocol : Protocole internet permettant transférer des fichiers. Il fonctionne en mode connecté. Généralement, l'accès est anonyme.
GSM	Global System for Mobile communications : Le GSM est la norme européenne utilisée en France et partout dans le monde par les réseaux de téléphonie cellulaire.
HTTP	Hypertext Transfer Protocol : Protocole qui sert à naviguer dans World Wide Web. Un serveur WWW est un ordinateur qui utilise le protocole HTTP.
ICMP	Internet Control Message Protocol : Le protocole ICMP est un protocole qui permet de gérer les informations relatives aux erreurs des machines connectées. Etant donné le peu de contrôles que le protocole IP réalise, il permet non pas de corriger ces erreurs mais de faire part de ces erreurs aux protocoles des couches voisines. Ainsi, le protocole ICMP est utilisé par tous les routeurs, qui l'utilisent pour reporter une erreur (appelé *Delivery Problem*).
IP	C'est un des protocoles les plus importants d'Internet car il permet l'élaboration et le transport des datagrammes IP (les paquets de données), sans toutefois en assurer la "livraison": le protocole IP traite les datagrammes IP indépendamment les uns des autres en définissant leur représentation, leur routage et leur expédition.
NAS	Network Access Serveur : Serveur d'accès distant, Routeur équipé de modems permettant l'interconnexion entre le système d'information et les équipements distants raccordés via une ligne téléphonique (analogique ou numérique).
NAT	Network Translation Adress : Translation d'adresse, Mécanisme permettant de masquer le plan d'adressage utilisé par la translation dynamique des adresses d'un plan d'adressage vers un autre.
Numéro brûlé	Mécanisme imposé par la législation française ayant pour objectif de limiter les appels nuisants. Le numéro appelé est enregistré dans une liste interne au modem au-delà d'un certain nombre d'appels infructueux.

Proxy	Programme qui tourne sur un pont ou une passerelle et qui bloque le passage direct des paquets entre le client et le serveur et n'autorise le passage que de certains paquets.
RNIS:	Réseau Numérique à Intégration de Services : réseau téléphonique numérique.
RTC:	Réseau Téléphonique Commuté : réseau de téléphone analogique
SMTP	Simple Mail Transfer Protocol : Protocole d'échange de message selon le principe stockage puis transmission. Il est utilisé essentiellement entre deux passerelles de messagerie, éventuellement pour une remise locale.
SSL	Secure Socket Layer : Protocole de transport assurant un service d'authentification, d'intégrité et de confidentialité en mode point à point indépendamment des caractéristiques du réseau sous-jacent.
TCP	*Transmission Control Protocol* : *Protocole de Contrôle de Transmission* est un des principaux protocoles de la couche transport du modèle TCP/IP. Il permet, au niveau des applications, de gérer les données en provenance (ou à destination) de la couche inférieure du modèle (c'est-à-dire le protocole IP). TCP est un protocole orienté connexion, c'est-à-dire qu'il permet à deux machines qui communiquent de contrôler l'état de la transmission.
TCP/IP	Transmission Control Protocol/Internet Protocol : Protocole de communication de niveau 4 entre les différents ordinateurs connectés à Internet. Il assure la commutation des paquets sur le réseau et contrôle l'intégrité des informations au départ et à l'arrivée. Il est utilisé pour des applications telles que HTTP, FTP, SMTP.
TLS	Transport Layer Security : Normalisation par l'IETF du protocole SSL (Netscape)
UDP	User Datagram Protocol : Protocole de communication de niveau 4 en mode non connecté. Les datagrammes sont acheminés vers des ports UDP, repérés par une adresse IP (32 bits) et un numéro de port local (16 bits). Les applications prennent en charge les problèmes de correction d'erreurs et de contrôle de congestion. Il est utilisé pour des applications telles que SNMP (Simple Network Management Protocol) ou DNS.
URL	Universal Resource Locator : Chemin universel de ressources qui indique où se trouvent les informations WWW et quel est le protocole utilisé. Nom normalisé pour identifier un objet sur Internet.
VLAN	Virtual Local Area Network : Réseau local virtuel
VPN	Virtual Private Network : Réseau Privé Virtuel, concept recouvrant tout réseau privatif construit sur un réseau public. Par extension, un VPN dispose généralement de son propre plan d'adressage et de fonctions de sécurité visant à protéger la confidentialité des données transportées.

GLOSSAIRE

AUDIOTEL

Système **audiotex** français.

AUDIOTEX

L'audiotex correspond à la notion de service téléphonique automatisé. L'audiotex se définit par la conjonction de trois éléments : un usager qui utilise son poste téléphonique, une machine vocale (capable de gérer des informations sonores) porteuse d'un service d'information ou de transaction, une ligne téléphonique qui relie les deux.

AUTORITÉ D'ATTRIBUTION

Elle émet des **certificats** avec des attributs spécifiques, qui sont généralement à valeur ajoutée : capacité administrative à exercer un métier, état civil certifié, comptabilité certifiée, acte notarié. Voir **PSC.**

AUTORITÉ D'ENREGISTREMENT

Elle effectue la vérification d'un certain nombre d'informations concernant la personne (physique ou morale) demandant l'octroi d'un **certificat** de clé publique, notamment son identité mais aussi par exemple la nature de ses moyens de signature et de conservation de la clé privée et adresse un message normalisé à **l'opérateur de certification** en vue de la fabrication du **certificat** dont elle assure également la distribution**.** Voir **PSC.**

AUTORITÉ DE CERTIFICATION

Une autorité de certification intervient en tant que tiers de confiance entre utilisateurs du réseau **internet** pour sécuriser les échanges. Elle est le donneur d'ordre des **opérateurs de certification** et des **autorités d'enregistrement**. Elle assume la responsabilité finale vis à vis des tiers et définit la politique de certification : ensemble des procédures et règles de sécurité appliquées par une autorité de certification ou exigées de ses prestataires pour une catégorie donnée de certificats. L'autorité de certification conserve la clé secrète servant à signer les **certificats**. Elle gère éventuellement la marque associée à son activité ainsi que les problèmes d'**interopérabilité**. Voir **PSC.**

BROWSER

Butineur, **interface** logicielle qui permet de naviguer sur le web. Les plus connues de ces interfaces sont Communicator de Netscape et Internet Explorer de Microsoft.

CERT

Computer Emergency Response Team : organisations mises en place un peu partout dans le monde pour assister leurs adhérents en matière de sécurité des réseaux. Regroupement au sein de la structure FIRST.

CERTIFICAT

Un certificat est une attestation électronique qui lie les données afférentes à la vérification de signature à une personne et confirme l'identité de cette personne.

CERTIFICAT QUALIFIÉ

Un certificat qualifié est un certificat qui satisfait aux exigences visées à l'annexe I de la directive signature électronique : identification du **PSC**, nom du signataire, code d'identité du certificat, possibilité d'inclure une qualité spécifique du signataire en fonction de l'usage auquel le certificat est destiné, date de validité, limites à l'utilisation du certificat, limites à la valeur des transactions pour lesquelles le certificat peut être utilisé… En outre, il est fourni par un prestataire de service de certification satisfaisant aux exigences visées à l'annexe II : faire la preuve qu'ils sont suffisamment fiables, assurer le fonctionnement d'un service de révocation sûr et immédiat, vérifier par des moyens appropriés et conformes au droit national l'identité et le cas échéant les qualités spécifiques de la personne à laquelle un certificat qualifié est délivré, ne pas stocker ni copier les données afférentes à la création de signature de la personne à laquelle le PSC a fourni des services de gestion de clés…

CHEVAL DE TROIE

Logiciel qui se place sur une machine cible, à l'insu du propriétaire. Il permet de communiquer avec la machine cible pour exécuter des opérations malveillantes.

CONFIDENTIALITÉ

Propriété qui assure la tenue secrète des informations avec accès aux seules entités autorisées.

COOKIE

Elément de donnée stocké sur le poste de travail par un serveur WEB et contenant l'identification du serveur, de la page ainsi que tout autre donnée utile au concepteur du site ou de l'application.

CRITÈRES COMMUNS

Les Critères communs (pour la sécurité des systèmes d'information) sont une norme internationale. Cette norme définit de façon standardisée, d'une part, des exigences fonctionnelles de sécurité visant des produits ou des systèmes tilisant les technologies de l'information et d'autre part des exigences d'assurance de sécurité, c'est à dire les moyens que l'on se donne pour vérifier la conformité de ces produits ou systèmes aux exigences fonctionnelles de sécurité. Fondés par la France, le Royaume-Uni, l'Allemagne, les États-Unis et le Canada, les Critères

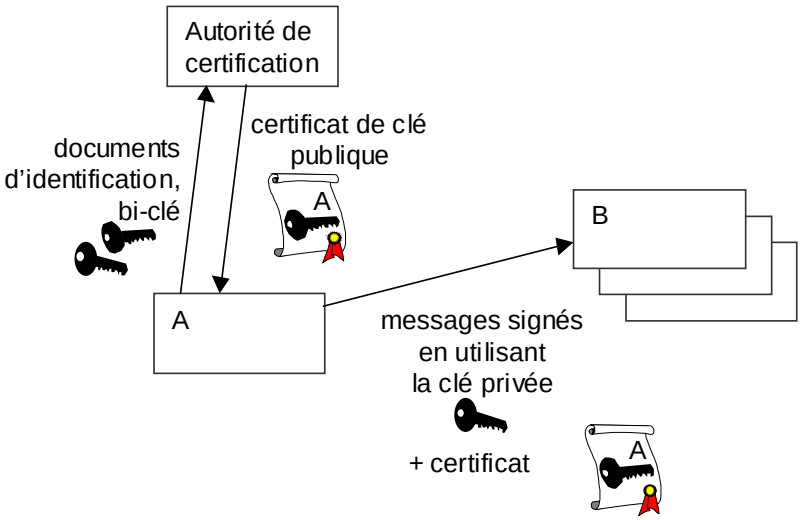
communs sont devenus une norme ISO (ISO 15408) depuis juin 1999. Les Critères communs fournissent également un outil appelé " **profil de protection** " permettant aux utilisateurs de préciser de façon générique leurs exigences de sécurité relatives à une famille de produits ou de systèmes.

CRYPTOGRAPHIE A CLÉ PUBLIQUE

Mode de chiffrement permettant à deux correspondants de s'affranchir de l'échange préalable de clés secrètes.

OU

CRYPTOGRAPHIE ASYMETRIQUE



Comme l'illustre le schéma ci-dessus, on génère pour chaque internaute (personne physique ou morale) un couple de clés indissociables :

- la première clé (clé privée) est un secret connu seulement par son détenteur, l'internaute.
- la seconde clé (clé publique), au contraire, est une donnée publique qui peut être diffusée à tous les interlocuteurs.

L'algorithme de génération des clés est tel qu'il est impossible de retrouver la clé privée à partir de la clé publique correspondante. En outre, ce couple de clés ou bi-clé est conçu de telle sorte qu'un message crypté en utilisant l'une des clés peut être décrypté en utilisant l'autre, et seulement l'autre.

Deux cas de figure peuvent être imaginés : soit l'internaute génère son bi-clé, en utilisant un dispositif considéré par l'autorité de certification comme étant de confiance, soit l'autorité le génère pour lui. Le premier cas présente l'avantage de ne pas requérir la distribution de la clé privée générée par l'utilisateur. Des procédures doivent cependant être mises en place pour s'assurer de l'unicité de la clé privée de l'utilisateur. Le second cas met en œuvre des procédures de création et de distribution de bi-clé, ainsi que de suppression de la clé privée chez l'autorité de

certification. Toutes ces procédures doivent être hautement sécurisées si on veut in fine pouvoir garantir que la clé privée n'est pas compromise.

Pour s'identifier lors de l'envoi d'un message, A va crypter ce message en utilisant sa clé privée. Tout détenteur B de la clé publique de A saura décrypter le message envoyé par A et le lui attribuer.

Pour ce faire, il faut que B puisse faire le lien de façon sûre entre la clé publique de A et l'identité de A. C'est le rôle d'une tierce partie de confiance que d'apporter cette assurance à B en délivrant un **certificat** établissant le lien entre la clé publique de A et son identité. On parle **d'autorité de certification** pour qualifier ce service rendu à la communauté des internautes.

CYBER-COMM

Lancée en juin 1998, cyber-Comm, société anonyme, fonde sa solution de paiement sécurisé sur internet sur la carte bancaire à puce et commercialise un lecteur, qui a fait l'objet d'un profil de protection. La solution du lecteur de cartes à puces a été lancée en avril 2000 et est soutenue par la place (Crédit agricole, BNP-Paribas, Société générale, Banques populaires, Crédit commercial de France, Crédit lyonnais et Crédit mutuel). Cette protection est la condition pour que les banques puissent accorder leur garantie aux commerçants comme aux utilisateurs de carte. Au tour de table, figurent également La Poste, ParisBourse, le Groupement CB, Europay International (Eurocard, Mastercard) et Visa, ainsi que les industriels Alcatel, Bull et Cap Gemini. En France, les 2 % de transactions réalisées par des canaux de vente à distance (VPC, minitel, téléphone, Internet) totalisent 50 % des litiges de l'ensemble des paiements par carte bancaire.

DCSSI

Direction centrale de la sécurité des systèmes d'information du Secrétariat général de la défense nationale. La DCSSI est organisme de certification. À ce titre, il a compétence pour délivrer des agréments aux centres d'évaluation de la sécurité des technologies de l'information (CESTI).

DDOS

Distributed Denial Of Service. Technique d'attaque répartie cherchant à obtenir un déni de service.

DMZ

DeMilitarized Zone : zone démilitarisée. Zone d'échange entre deux réseaux de sensibilités différentes. Le contrôle des échanges est assuré par un dispositif de pare-feu.

DNS

Domain Name Server : service permettant la traduction

	de l'adresse IP d'un ordinateur en son nom et inversement. Le nom constitue un moyen mnémotechnique pour faciliter l'accès aux informations et l'envoi de messages.
DOS	Denial Of Service : déni de service
EDI	Echange de données informatisées. Dialogue entre applications informatiques (achats, commandes, facturations…) de partenaires économiques (banques, entreprises…).
ETEBAC 5	**Protocole** sécurisé de transfert de fichiers banques-entreprises, utilisé en particulier pour les opérations de gestion de trésorerie. Ce protocole, normalisé sur le plan domestique, assure grâce à l'usage de la **cryptographie asymétrique** et des cartes à puces un ensemble de fonctions de sécurité : **authentification** réciproque, **intégrité, confidentialité** et surtout **non-répudiation**.
FAI	Fournisseur d'Accès Internet : en anglais «ISP» Internet Service Provider.
FIREWALL	Pare-feu. Solution hardware ou software, qui permet de contrôler les entrées et sorties sur une liste de port. Un port est désigné par un numéro. Ces numéros de port sont utilisés par les programmes pour se connecter au réseau **TCP/IP**. Certains programmes disposent d'un numéro de port bien connu pour être facilement utilisables. Ces programmes sont alors plus vulnérables et il est nécessaire d'empêcher leur utilisation depuis l'extérieur. Un pare-feu permet de filtrer ces messages **TCP/IP**.
FPTI	Fédération des Professionnels des Tests Intrusifs.
FTP	File Transfer Protocol : protocole Internet permettant de transférer des fichiers. Il fonctionne en mode connecté. Généralement, l'accès est anonyme.
GAFI	Groupe d'action financière mis en place au sommet de l'Arche en 1989 par le G7, avec pour mission d'une part d'élaborer des recommandations pour lutter contre le blanchiment de l'argent " sale " que les États membres pouvaient intégrer dans leurs droits nationaux respectifs, d'autre part de prendre les dispositions nécessaires pour évaluer l'efficacité de ces réglementations nationales et proposer des mesures complémentaires. Le GAFI est composé de 26 membres, dont les 15 pays de l'Union européenne.
GSM	Global System for Mobile communications : le GSM est la norme européenne utilisée en France et partout dans le monde par les réseaux de téléphonie cellulaire. Le système numérique GSM,

déployé en France en 1993, permet un accès très large au réseau téléphonique à partir de terminaux portables standardisés et largement diffusés dans le public. En dehors des services de téléphonie classique et de télécopie, les GSM permettent l'envoi de messages courts (**SMS** pour Short message services).

GTA

L'autorité de confiance mondiale, Global Trust authority, GTA, à laquelle sont affiliées plus de huit cent banques ainsi que différentes associations professionnelles, a été lancée le 6 septembre 1999. Ses membres fondateurs sont la NATWEST, la ROYAL BANK of CANADA, la SAKURA BANK, la SERMEPA (Espagne), la SIA (Italie), le SIBS (Portugal), la SOCIETE GENERALE, SWISSKEY, l'ABI (Italie), la BANK of IRELAND, la BNP, les CARTES BANCAIRES, INTERPAY (Pays-Bas), ISABEL (Belgique) et LA CAIXA. GTA, structure à but non lucratif, a pour objectif, en tant qu'autorité racine, de faciliter les échanges électroniques **interopérables** transfrontaliers en définissant des règles fonctionnelles et sécuritaires communes, et en s'assurant de la sécurité, de la garantie et de la confiance dans le système.

HACKERS

Les hackers sont des pirates informatiques.

HBCI

HomeBanking Computer Interface. Avec la loi multimédia d'août 1997, l'Allemagne a mis en place une infrastructure de sécurité ayant pour objet de créer la base juridique garantissant la sûreté des signatures électroniques. Afin d'harmoniser les différents systèmes de sécurité et construire une plate-forme commune pour les échanges de données entre le client et ses banques un standard unitaire a été notamment établi au sein du Conseil central du crédit. Signé en octobre 1997, l'accord invitait l'ensemble des établissements de crédit à respecter avant octobre 1998 le standard HBCI. D'autres standards existent : OFX et IFX. Open financial Exchange résulte de la fusion des standards OFC (de Microsoft, Open exchange, d'Induit) et des protocoles pour les opérations bancaires et les paiements électroniques de Chekfree. Cette fusion a été opérée pour constituer un standard technique et de communication unique de banque sur internet.

HTTP

HyperText Transfer Protocol : protocole qui sert à naviguer dans World Wide Web. Un serveur www est un ordinateur qui utilise le protocole HTTP.

HYPERTEXTE

Texte comportant des liens à partir de mots ou d'images affichées par le **browser**, permettant l'affichage instantané d'un autre texte (ou d'une autre partie du texte) quelle que

soit sa localisation. Un système hypertexte est un logiciel capable d'afficher un tel document et de supporter le parcours non linéaire. Voir **(http**, hypertext transfer protocol).

ICMP

Internet Control Message Protocol. Le protocole ICMP est un protocole qui permet de gérer les informations relatives aux erreurs des machines connectées. Étant donné le peu de contrôles que le protocole IP réalise, il permet non pas de corriger ces erreurs mais de faire part de ces erreurs aux protocoles des couches voisines. Ainsi, le protocole ICMP est utilisé par tous les routeurs, qui l'utilisent pour reporter une erreur (appelé Delivery Problem).

IDENTRUS

IDENTRUS est un club fermé entre grands établissements de crédit, à but lucratif ; contrairement à **GTA** qui est ouvert et à but non lucratif. IDENTRUS offre un service de certification à valeur ajoutée. D'une part, son service de certification interentreprise est doublé d'un scoring d'entreprises, sur le modèle du service offert par WEBTRUST, qui a développé une fonction complémentaire d'audit comptable. D'autre part, si un litige relatif à la garantie identitaire fournie par IDENTRUS est levé, IDENTRUS fournit un processus de résolution du litige.

IDENTRUS a été créée et est détenue par des banques essentiellement américaines et allemandes, sous la forme d'une société commerciale. Sa mission est de développer une infrastructure de confiance intégrée. Sa structure repose sur des contrats noués avec des banques, qui elles seules entretiennent des relations avec leurs clients à travers les différentes applications qu'elles mettent en oeuvre. Il revient aux institutions financières de développer leurs propres applications qui doivent répondre aux normes d'IDENTRUS, qui ne fournit in fine qu'une plate-forme d'identité.

INTERFACE

Dispositif grâce auquel s'effectuent les échanges d'informations entre deux systèmes. Interface utilisateur : ensemble des moyens de dialogue entre l'utilisateur et l'ordinateur, regroupant l'usage des commandes.

INTERNET

Interconnected networks. Réseau mondial de fait formé par l'interconnexion de l'ensemble des réseaux IP (Internet protocol), c'est à dire fonctionnant sous le protocole de transmission **TCP/IP.** Sur ces réseaux sont connectés particuliers, entreprises, administrations, universités, **hackers**… Le principe d'Internet repose sur le fait que chacun des ordinateurs connectés (appelés host) coopère au bon acheminement des messages. Les messages contiennent l'adresse de leur destination.

L'intranet se dit d'un réseau utilisant les technologies Internet (protocoles et applications **TCP/IP**) à l'intérieur d'une

organisation (au niveau du réseau local, mais aussi au niveau d'un réseau grande distance privé).

L'Internet Architecture Board IAB est le comité scientifique qui décide des normes essentielles pour le réseau, en agissant au nom d'une association à but non lucratif, l'Internet Society, juridiquement responsable en cas de litige. L'IAB s'appuie sur les conclusions des groupes de travail réunis au sein de l'IETF (Internet Engineering Task Force) et coordonnés par un IESG (Internet Engineering Steering Group). L'IANA est l'organisme mondial qui gère l'adressage IP, adresses de chaque ordinateur connecté à internet.

INTEROPÉRABILITÉ

Sens technique : capacité des dispositifs à échanger des informations entre eux ou à intégrer les mêmes interfaces.

IP

C'est un des protocoles les plus importants d'Internet car il permet l'élaboration et le transport des datagrammes IP (les paquets de données), sans toutefois en assurer la «livraison»: le protocole IP traite les datagrammes IP indépendamment les uns des autres en définissant leur représentation, leur routage et leur expédition.

IRRÉVOCABILITÉ

Impossibilité pour l'utilisateur ou le prestataire de refuser de payer une transaction qu'il reconnaît avoir faite. Il ne peut notamment pas changer d'avis en raison d'un différend l'opposant au commerçant sur la qualité du bien acheté par exemple. La loi n° 91-1382 du 30 décembre 1991 dispose à ce titre que " l'ordre ou l'engagement de payer donné au moyen d'une carte de paiement est irrévocable ; il ne peut être fait opposition au paiement qu'en cas de perte ou de vol de la carte, de redressement ou de liquidation judiciaire du bénéficiaire ".

KIOSQUE

Système de paiement dans lequel un opérateur de télécommunication est mandaté par un ou plusieurs prestataires de services pour assurer le recouvrement et le versement des sommes dues par les utilisateurs de ces services au fournisseur du service.

MONNAIE ÉLECTRONIQUE

La monnaie électronique est définie, d'après la directive " monnaie électronique " comme une valeur monétaire représentant une créance sur l'émetteur, qui est stockée sur un support électronique, émise contre la remise de fonds d'un montant dont la valeur n'est pas inférieure à la valeur monétaire émise, acceptée comme moyen de paiement par des entreprises autres que l'émetteur.

Lorsque le support dans lequel est incorporé le pouvoir d'achat (la créance sur l'émetteur) est une carte à microprocesseur, on parle de porte-monnaie électronique

(PME). Lorsqu'il s'agit d'un PC ou d'un serveur accessible par l'intermédiaire d'un PC connecté à l'internet, on parle généralement de porte-monnaie virtuel (PMV).

MOTEUR DE RECHERCHE Logiciel qui permet de retrouver des fichiers de diverses natures notamment des **pages** html à partir de mots-clés ou d'expressions.

NAS Network Access Serveur : serveur d'accès distant. Routeur équipé de modems permettant l'interconnexion entre le système d'information et les équipements distants raccordés via une ligne téléphonique (analogique ou numérique).

NAT Network Translation Adress : translation d'adresse. Mécanisme permettant de masquer le plan d'adressage utilisé par la translation dynamique des adresses d'un plan d'adressage vers un autre.

NON-RÉPUDIATION Impossibilité pour l'utilisateur ou le prestataire de nier qu'il est l'auteur de la transaction et que celle-ci existe bien. A distinguer de **l'irrévocabilité.**

NUMÉRIQUE Digital en anglais. Se dit d'un signal qui ne peut prendre qu'un nombre fini de valeurs. La transmission numérique ne prend que deux valeurs : 0 ou 1. Signal binaire utilisé d'abord pour l'informatique et qui s'étend à présent à l'ensemble des communications.

NUMÉRO BRÛLÉ Mécanisme imposé par la législation française ayant pour objectif de limiter les appels nuisants. Le numéro appelé est enregistré dans une liste interne au modem au-delà d'un certain nombre d'appels infructueux.

OPÉRATEUR DE CERTIFICATION Il fabrique le certificat à clé publique à partir du message envoyé par **l'autorité d'enregistrement**. Il le signe, en assure la publication et gère sa révocation éventuelle.

PAGE HTML Une page html (HyperText Markup Language) est un fichier contenant des marques html utilisés par le **browser** pour afficher correctement du texte, des images, de la vidéo… Parmi les marques html, certaines marques -marques **hypertextes**- permettent de faire le lien avec d'autres pages quelle que soit leur localisation. Ces marques hypertextes contiennent la localisation des pages liées sous la forme d'une adresse **URL**. Le **protocole** de diffusion des pages html est http.

PORTE-MONNAIE ELECTRONIQUE Voir **monnaie électronique**

PORTE-MONNAIE VIRTUEL Voir **monnaie électronique**

PROFIL DE PROTECTION

Un profil de protection (PP) est un cahier des charges en matière de sécurité visant une famille de produits et rédigé dans le formalisme des **Critères Communs**. Il décrit la cible d'évaluation (appelée TOE, pour target of evaluation), son environnement sécuritaire, ainsi que les objectifs de sécurité et les exigences de sécurité liées à la cible. Un PP est évalué et enregistré par l'organisme de certification (**DCSSI**). Différents PP existent : PP cartes à puce, PP échange de données informatisées, PP Billétique, PP **firewalls,** PP messagerie électronique, PP site web institutionnels, PP porte monnaie électronique…

PROTOCOLES

Un protocole est une convention précisant des règles et des spécifications techniques à respecter dans le domaine des télécommunications afin d'assurer l'interopérabilité des systèmes. Il existe différentes couches de protocoles répondant à des besoins différents : protocoles de transport de données, protocoles applicatifs, etc. De nombreux protocoles sont normalisés, ce qui leur assure une reconnaissance nationale ou internationale.

PROXY

Programme qui tourne sur un pont ou une passerelle et qui bloque le passage direct des paquets entre le client et le serveur et n'autorise le passage que de certains paquets.

PSC

Prestataires de services de certification. Ce terme générique visé par la directive " signature électronique " recoupe les différents métiers de la certification : **opérateurs de certification, autorités d'enregistrement, de certification et d'attribution.** En France, la Poste en partenariat avec la SAGEM et en accord avec les Chambres de commerce et d'industrie a créé CERTINOMIS. CERTPLUS, opérateur de certification créée par GEMPLUS, VERISIGN, France TELECOM et MATRA HAUTES TECHNOLOGIES a été retenu par **CYBER-Comm** pour émettre les certificats SET dont auront besoin les commerçants pour être reconnus dans l'univers du commerce électronique. GEMPLUS propose avec GEMSAFE une solution organisée autour d'un lecteur de carte et d'une carte à puce sur laquelle sont stockés un couple clé privée / clé publique et le certificat qui aura été signé par CERTPLUS. Aux États-Unis, l'ABA (American bankers association) en partenariat avec DIGITAL SIGNATURE TRUST Cie a l'intention de devenir autorité de certification pour l'industrie de services financiers. En outre, VERISIGN a sa propre hiérarchie et VISA, MASTERCARD, AMEX et DINER'S ont développé une hiérarchie de type **SET**. Deux projets d'autorités mondiales dans le secteur financier ont été développés : **GTA** et **IDENTRUS**.

RNIS	Réseau Numérique à Intégration de Services : réseau téléphonique numérique.
RSA	Système algorithme de **cryptage** asymétrique mis au point au MIT en 1977. Une clé publique permet de coder le message que le destinataire pourra déchiffrer à l'aide d'une clé privée qu'il est seul à détenir. Voir **cryptographie à clé publique**.
RTC	Réseau Téléphonique Commuté : réseau de téléphone analogique
SET	Le **protocole** SET (Secure Electronic Transactions) repose sur l'identification des parties en présence et la saisie des références de la carte du client hors connexion. SET permet la confidentialité de la transmission, la conservation de l'intégrité des instructions de paiement par signature électronique et l'authentification mutuelle du client et du commerçant. SET s'oriente vers la combinaison des sécurités logicielle et matérielle, avec l'utilisation de la carte à puce (voir **CYBER-Comm**) afin d'assurer la non-répudiation des transactions. La transaction n'est pas répudiable et le serveur du commerçant ne peut interférer dans la transmission de l'ordre de paiement à la différence de **SSL**.
SIM	La carte SIM est une carte à micro-processeur. En dehors de ses fonctions de stockage de données et de sécurité, elle peut également exécuter des applications. La carte SIM est ainsi une plate-forme intelligente permettant de fournir des services à forte valeur ajoutée.
SITES PORTAILS	Un portail rassemble autour d'une **page** de nature informative un ensemble de liens **hypertextes** vers les sites de prestataires partenaires. Yahoo, AOL sont les portails généralistes grand public les plus connus. En matière bancaire et financière, différents projets se développent sur la place. Le plus avancé est Ze Project, partenariat entre Europaweb et DEXIA. En permettant une grande liberté de choix entre différentes offres, les portails vont aviver la concurrence.
SMS	Short message service. Voir **GSM**
SMTP	Simple Mail Transfer Protocol : protocole d'échange de message selon le principe stockage puis transmission. Il est utilisé essentiellement entre deux passerelles de messagerie, éventuellement pour une remise locale.
SSL	Secure Socket Layer : protocole de transport assurant un service d'authentification, d'intégrité et de confidentialité en mode point à point indépendamment des caractéristiques du réseau sous-jacent.

SWIFT

Society for *worldwide interbank financial telecommunication*, réseau international pour le traitement des opérations financières transfrontalières entre institutions financières.

TCP

Transmission Control Protocol : le Protocole de Contrôle de Transmission est un des principaux protocoles de la couche transport du modèle TCP/IP. Il permet, au niveau des applications, de gérer les données en provenance (ou à destination) de la couche inférieure du modèle (c'est-à-dire le protocole IP). TCP est un protocole orienté connexion, c'est-à-dire qu'il permet à deux machines qui communiquent de contrôler l'état de la transmission.

TCP/IP

Transmission Control Protocol/Internet Protocol : protocole de communication entre les différents ordinateurs connectés à Internet. Il assure la commutation des paquets sur le réseau et contrôle l'intégrité des informations au départ et à l'arrivée. Il est utilisé pour des applications telles que HTTP, FTP, SMTP.

TEST D'INTRUSION

Appelé également " analyse de pénétration ". Un test d'intrusion est un essai d'intrusion prévu, conçu pour estimer la sécurité d'un réseau et identifier ses vulnérabilités.

TLS

Transport Layer Security. Normalisation par l'IETF du protocole **SSL** (Netscape)

TRANSPAC

Réseau mis en place à partir de 1975 par la France pour permettre les échanges entre les ordinateurs selon la norme **X 25**. Transpac est une filiale de France Télecom.

UDP

User Datagram Protocol : protocole de communication de niveau 4 en mode non connecté. Les datagrammes sont acheminés vers des ports UDP, repérés par une adresse IP (32 bits) et un numéro de port local (16 bits). Les applications prennent en charge les problèmes de correction d'erreurs et de contrôle de congestion. Il est utilisé pour des applications telles que SNMP (Simple Network Management Protocol) ou DNS.

URL

Universal Resource Locator : chemin universel de ressources qui indique où se trouvent les informations WWW et quel est le protocole utilisé. Nom normalisé pour identifier un objet sur Internet.

VIRUS

Partie d'un programme d'ordinateur qui se duplique lui-même en s'incrustant dans d'autres programmes. Quand ces programmes sont exécutés, le virus est encore appelé et peut se propager davantage.

VPN

Virtual Private Network : réseau privé virtuel, concept recouvrant tout réseau privatif construit sur un réseau public. Par extension, un VPN dispose généralement de son propre plan d'adressage et de fonctions de sécurité visant à protéger la confidentialité des données transportées.

WAP

La technologie WAP permet d'accéder directement à l'Internet à partir d'un téléphone portable. Le débit des données sur les réseaux GSM et les formats des écrans des téléphones portables contraignent encore fortement cette technologie qui devra attendre les nouveaux réseaux haut débit et les nouvelles générations de téléphones portables pour trouver les conditions de son développement. Dans l'univers des portables WAP, un langage spécifique, Wireless markup Language (WML) se substitue au protocole HTML (voir **page**). Une passerelle à la jonction des réseaux internet et GSM fait la transcription en WML des pages HTML. Un **browser** spécifique est inclus dans la carte SIM et permet de se déplacer de site en site.

WEB

Toile d'araignée mondiale, World wide web (WWW). Fondé sur une architecture client-serveur, ce système hypermédia intègre des fonctions de l'Internet (courriers électroniques, forums, téléchargement de fichiers et consultation de serveurs d'informations) en ajoutant des dimensions **hypertexte** et multimédia.

X 25

Protocole de communication à commutation de paquets en mode connecté. Cette technologie optimise l'utilisation de la bande passante du réseau par un partage des ressources disponibles.

BIBLIOGRAPHIE INDICATIVE

■ TEXTES DE REFERENCE DES AUTORITES FRANCAISES

- **COMITÉ DES ÉTABLISSEMENTS DE CRÉDIT ET DES ENTREPRISES D'INVESTISSEMENT** (Rapport au), *La libre prestation de services en matière de services d'investissement*, novembre 1998, rapport disponible sur www.banque-france.fr/ informations bancaires et financières.

- **COMMISSION BANCAIRE**, Rapport annuel 1999, *Les nouvelles technologies de la banque à distance, quelles conséquences pour les établissements financiers et leurs autorités de contrôle ?*, juillet 2000.

- **COMMISSION BANCAIRE**, *Livre blanc sur la sécurité des systèmes d'information*, 1996.

- **CONSEIL D'ÉTAT, section du rapport et des études**, *Internet et les réseaux numériques*, juillet 1998, rapport disponible sur le site www.internet.gouv.fr.

- **COMMISSION DES OPÉRATIONS DE BOURSE**, *Les marchés financiers à l'heure d'Internet, VIIIème entretiens de la COB*, Bulletin COB n° 329 novembre 1998, disponible sur le site de la COB, www.cob.fr.

- **COMMISSION DES OPÉRATIONS DE BOURSE**, *recommandation n° 99-02 relative à la promotion ou la vente de produits de placement collectif ou de services de gestion sous mandat via Internet*, 3 septembre 1999 et *recommandation n° 2000-02 relative à la diffusion d'informations financières sur les forums de discussion et les sites Internet dédiés à l'information ou au conseil financier* disponibles sur www.cob.fr.

- **CONSEIL DES MARCHES FINANCIERS**, *décision n° 99-07 relative aux prescriptions et recommandations pour les prestataires de services d'investissement offrant un service de réception-transmission ou d'exécution d'ordres de bourse comportant une réception des ordres via Internet*, septembre 1999. Cette recommandation est disponible sur le site du CMF, www.cmf-France.org.

- **CONSEIL NATIONAL DU CRÉDIT ET DU TITRE**, *La banque électronique*, août 1997.

■ TEXTES DE REFERENCE D'AUTORITES ETRANGERES

- **OFFICE OF THE COMPTROLLER OF THE CURRENCY**, *the report of the consumer electronic payments task force,* avril 1998.

- **OCC ALERT 2000-14**, *Infrastructure threats – intrusion risks,* 15 mai 2000.

- **OCC ALERT 2000-1,** *Internet security : distributed denial of service attacks. 11 février 2000.* Ces recommandations sont disponibles sur le site www.occ.treas.gov.

- **OCC,** *Internet banking, Comptroller's handbook,* octobre 1999.

- **FEDERAL DEPOSIT INSURANCE CORPORATION (FDIC),** *risk assessment tools and practices for information system security,* FIL-68-99, juillet 1999.

- **FDIC,** *Electronic banking examination procedures,* février 1997. Ces documents sont disponibles sur le site www.fdic.gov.

- **SECURITIES AND EXCHANGE COMMISSION,** *Use of Internet web sites to offer securities, solicit securities transactions or advertise investment services offshore, 23 mars 1998.* Cette recommandation est disponible sur le site de la SEC à www.sec.gov. De nombreuses décisions y sont également publiées.

- **BANK OF JAPAN,** *The importance of information security for financial institutions and proposed countermeasures,* avril 2000, disponible sur le site www.boj.or.jp.

■ RAPPORTS

- **ORGANISATION INTERNATIONALE DES COMMISSIONS DE VALEURS,** *Internet et les services financiers,* septembre 1998.

- **EUROPEAN CENTRAL BANK,** *The effects of technology on the EU banking system,* juillet 1999. Rapport disponible sur le site www.ecb.int.

- **EUROPEAN COMMITTEE FOR BANKING STANDARDS,** *Technical report on electronic banking,* TR 600, octobre 1999. Rapport disponible sur www.ecbs.org.

- **EUROPEAN COMMITTEE FOR BANKING STANDARDS,** *Certification authorities,* TR 402 juillet 1999.

- **BASLE COMMITTEE FOR BANKING SUPERVISION,** *risk management for electronic banking and electronic money activities,* mars 1998, disponible sur www.bis.org et *Electronic Banking Group Initiatives and White Papers,* octobre 2000

SECRÉTARIAT GÉNÉRAL DE LA COMMISSION BANCAIRE

Réalisation et mise en page à l'atelier de reprographie du SGCB

Directeur de la publication : Jean-Louis FORT,
Secrétaire général de la Commission bancaire