Fondation internet nouvelle génération

# « Confiance et sécurité sur les réseaux »
# Document de synthèse

Arnaud Belleil et Daniel Kaplan
12 octobre 2004

# SOMMAIRE

# 1. Confiance et sécurité sur les réseaux : la problématique

## *1.1. Confiance : une notion ambiguë*

La confiance est une notion ambiguë qui entretient des relations complexes avec la sécurité. Il est donc intéressant, pour introduire la réflexion, d'oublier les aspects techniques pour procéder à un croisement des approches[1] anthropologiques, sociologiques, économiques, juridiques de la confiance et de son existence sur les réseaux.

### 1.1.1. A chacun sa confiance

La confiance peut se définir comme « *Une espérance ferme en une personne ou une chose* » (Dictionnaire universel francophone, Hachette). Les approches de la confiance et la mise en valeur des ses caractéristiques essentiels varient pourtant selon les disciplines et les auteurs.

- Le juriste (Eric Caprioli, Avocat au Barreau de Nice) distinguera trois dimensions. D'abord, la croyance en la bonne foi, loyauté, sincérité et fidélité d'autrui ou en ses capacités, compétence et qualification professionnelles ; ensuite l'action de se fier à autrui, ou plus précisément de lui confier une mission (mandat, dépôt, …) ; enfin la manifestation de cette confiance (« la question de confiance »).

- Pour l'économiste (Eric Brousseau, Université Paris X), la confiance représentera un moyen de diminuer les coûts associés aux règles, contrats et institutions. Elle pourra être aussi considérée (Laurent Gille, ENST) comme une valeur propre à l'économie pré marchande.

- Selon l'anthropologue (Dominique Boullier, Université Technologique de Compiègne) pour comprendre la confiance, il faut accepter qu'elle se fonde sur une fiction admise, sur une convention juridique pour pallier l'absence de certitude. C'est ainsi que l'état-civil peut devenir une « preuve » de la généalogie.

- Le professionnel du marketing (Georges Fischer, CCIP) considère simplement que la confiance est un actif immatériel.

- L'approche sémantique (Youval Eched, La Poste, faisant état des travaux de Louis Quéré, EHESS) proposera de retenir « *la présomption d'un retour d'expérience positif dans la relation à un référent* ».

[1] http://www.fing.org/ref/confiance/FING_Confiance_26022004_CR_V1.pdf

- Le scientifique des technologies de sécurité (Michel Riguidel, ESNT), pourra de son côté définir[2] la confiance comme « *une relation non réflexive, non symétrique et non transitive* ». « Non réflexive » signifie qu'on ne se fait pas nécessairement confiance à soi-même. « Non transitive » signifie que la confiance ne se transfère pas. « Non symétrique » signifie que la confiance n'est pas nécessairement réciproque.

- Il est enfin possible d'envisager la confiance comme le produit (au sens multiplication) d'une réputation et de pratiques (Arnaud Belleil, Fing). Cette vision permet de saisir en quoi la confiance est longue à établir – l'influence de l'évolution des bonnes pratiques sur la réputation – et très rapide à détruire – l'impact d'une mauvaise pratique révélée sur la réputation.

### 1.1.2. La confiance en qui ? En quoi ?

La confiance peut-être accordée à une personne physique, à une personne morale, à une institution ou à un système. La langue anglaise rend bien compte de cette particularité avec la distinction entre «*trust*», la confiance dans les partenaires, et «*confidence* », la confiance dans un système (Eric Brousseau).

Selon Laurent Gille, on peut avoir confiance en un dispositif technique qu'on pourra tenir pour fiable, en une personne (tenir pour bienveillant), ou dans une institution (tenir pour juste).

D'un point de vue plus opérationnel, Cédric Nicolas[3], Bouygues Telecom, indique qu'il faut prendre en considération les « *cercles concentriques de la confiance* » auquel chacun se réfère naturellement : moi, mes proches, mes services quotidiens, mes services occasionnels.

Le manque de confiance peut aussi être adressé à des cibles distinctes. Georges Fischer explique que l'on peut manquer de confiance à autrui, surtout quand il est dématérialisé. On peut également manquer de confiance dans l'environnement car on ne comprend pas les règles et/ou on ne connaît pas les arbitres. On peut enfin manquer de confiance en soi-même, avoir des doutes sur sa propre maîtrise ou sa compréhension.

Enfin, on peut avoir confiance en la capacité de quelqu'un, en son comportement ou en ses intentions (Eric Brousseau). Lucky Luke peut faire confiance à Rantanplan pour retrouver les Dalton en prenant en compte son comportement et non sa compétence : il indique systématiquement la direction opposée.

[2] http://www.fing.org/confiance/IMG/pdf/Michel_Riguidel_juin_2003.pdf - page 27

[3] http://www.fing.org/confiance/IMG/pdf/Fing.org_Confiance_27042004_-_Bouygues_Tel_-_C._Nicolas.pdf - page 11

### 1.1.3. Les fondements de la confiance

La confiance étant une espérance, sur quels éléments tangibles peut-on se fonder pour accorder sa confiance ? Trois fondements peuvent être identifiés :

- L'historique des relations ; « *cela s'est bien passé avant, donc cela se passera bien la prochaine fois* » ;
- Les recommandations des tiers ; « *cela s'est bien passé avec d'autres, donc cela se passera bien avec moi* » ;
- La capacité à exercer des représailles ; « *cela va bien se passer car il a plus à perdre que moi si cela se passe mal* ».

Cette dernière dimension est plus particulièrement étudiée par les économistes qui cherchent à expliquer pourquoi les agents n'adoptent pas un comportement opportuniste, c'est-à-dire, en langage grand public, pourquoi les gens ne se comportent pas comme des escrocs alors qu'ils pourraient, à première vue, y avoir objectivement intérêt. Eric Brousseau[4] parle en la matière « *d'équilibre de la terreur* » et « *d'équilibre de la terreur mutualisé* ». Dans le premier cas, on décide de ne plus travailler à l'avenir avec un agent qui n'a pas été « de confiance ». Dans le second, il s'agit de lui nuire en portant atteinte à sa réputation, voire en obtenant son exclusion d'un marché. C'est efficace mais peut-on encore parler de relation de confiance ?

## *1.2. Confiance et sécurité : des univers différents*

### 1.2.1. Une perception et des technologies

La confiance et la sécurité ne se situent pas dans le même registre. La confiance est du ressort de la perception, avec une forte dimension psychologique, alors que la sécurité renvoi à un univers plus scientifique, notamment celui de la technologie. C'est ce que résume parfaitement Laurent Gille : « *La sécurité a trait à des dispositifs techniques destinés à « se sentir à l'abri du «danger» (en fonction de son évaluation du risque) ; la confiance est donnée à une «personne», elle est de l'ordre de la relation, elle englobe l'absence de danger (la sécurité) et la bonne fin, la satisfaction* ».

La confiance peut ainsi être objectivement irrationnelle comme on a pu le constater avec la question de la transmission des numéros de carte bancaire sur Internet. Les consommateurs étaient très nombreux à ne pas vouloir communiquer leur numéro de carte bancaire en ligne alors que, d'une part, le commerçant était le seul à assumer la totalité du risque de fraude et que, d'autre part, leurs comptes bancaires pouvaient être prélevés sans leur autorisation en l'absence de transmission du numéro sur le réseau (« captation » du numéro dans un échange physique, générateur automatique de numéros de carte bancaire). Cette perception du public était

[4] http://www.fing.org/ref/confiance/Confiance_Brousseau_26022004.pdf - page 5

tellement forte que les acteurs du paiement sécurisé l'ont intégré comme une donnée incontournable plutôt que de chercher à éduquer le public sur la réalité.

Dans le même ordre d'idée, Christophe Mourtel, Gemplus, indique[5] que les technologies de communication sans contact entraînent des réactions de défiance de la part des utilisateurs alors que les vulnérabilités connues sont les mêmes que pour les cartes à contact.

### 1.2.2. Un capital et des coûts

La confiance accordée à une marque correspond à un actif immatériel dont la valeur est jugée encore plus importante dans l'économie numérique. Inversement, la sécurité est perçue comme un coût. Les décideurs savent ce qu'elle coûte et ne savent pas ce qu'elle rapporte. Dominique Boullier indique que la demande de sécurité dans les entreprises ou les organisations n'existe pas car elle est toujours jugée « suffisante ». C'est dans ce contexte que s'inscrivent les réflexions récentes du Clusif (Club de la sécurité des systèmes d'information français) sur la notion de RoSI[6] (Retour Sur Investissement de sécurité). Cela devrait être un outil pour tenter de justifier les budgets auprès des directions.

## *1.3. La confiance et la sécurité : des relations complexes*

### 1.3.1. La sécurité composante de la confiance

L'approche la plus fréquente consiste à considérer la sécurité comme une méthode, ou même un préalable indispensable, pour construire la confiance. La confiance représente alors l'objectif et la sécurité le moyen. C'est dans cet esprit qu'il faut comprendre la juxtaposition fréquente des deux termes dans les travaux et programmes initiés par les grandes institutions publiques.

Cette vision est tout à fait fondée et il n'est pas nécessaire de s'y attarder compte tenu de l'abondance de la littérature disponible. Mais il importe de prendre en considération que d'autres relations sont envisageables.

### 1.3.2. La confiance substitut à la sécurité

La confiance peut-être un substitut efficace à la sécurité, une méthode par laquelle le social (ou le marketing) impose sa loi à la technologie. Si le consommateur est persuadé que le système est sûr, même si ce n'est pas objectivement le cas, tout peut fonctionner parfaitement. Cette approche présente en outre l'intérêt de permettre une réduction drastique des investissements en matière de sécurité.

[5] http://www.fing.org/confiance/IMG/pdf/Fing.org-27042004-Confiance_Gemplus-v0.3.pdf - page 8

[6] https://www.clusif.asso.fr/fr/clusif/commission/gt02.asp

Dans le même ordre d'idée, la confiance peut aussi être un substitut économique à la sécurité juridique. C'est ce qu'explique Eric Brousseau pour qui la confiance représente un moyen de diminuer les coûts associés aux règles, contrats et institutions. Les partenaires qui se font confiance avancent plus vite, sans solliciter les avocats, et ils conservent une liberté d'adaptation que n'autorisent pas les contrats qui tendent à ficeler les relations. De façon provocatrice, il est possible de dire que dès qu'il y a contrats, avec la sécurité juridique qui en découle, ou encore sécurisation par la technique, c'est que la confiance n'existe plus.

### 1.3.3. La sécurité génératrice de défiance

La sécurité peut enfin être un moyen très efficace pour engendrer de la défiance. La première raison résulte de ce que Dominique Boullier appelle « *l'illisibilité de la grammaire de la sécurité* ». A titre d'exemple, pour un néophyte de la signature électronique, la découverte des sigles obscurs - PKI[7] (ou IGC), AE[8,] AC[9], PSC[10], classe 3+ - forment un ensemble rebutant qui n'est guère en mesure de susciter la confiance dans les technologies de confiance.

La seconde raison est que la confiance n'est pas nécessairement symétrique. La sécurité de l'un peut ainsi éroder ou même détruire la confiance de l'autre. Les banquiers et les commerçants en ligne seront désireux d'identifier et d'authentifier les acheteurs pour éviter la fraude et garantir leur confiance. Ce faisant, ils développeront des solutions qui, en portant atteinte à l'anonymat du consommateur, susciteront en retour un éventuel phénomène de défiance. Les diffuseurs de contenus numériques semblent ne pouvoir accorder leur confiance aux internautes qu'en utilisant des dispositifs techniques de protection pouvant aller jusqu'à la surveillance, à des fins de gestion des droits, des pratiques culturelles. A l'évidence, ce n'est pas forcément la méthode la plus facile pour obtenir en retour la confiance du public.

---

En février 2001, Jean-François Abramatic[11], président du W3C, présentait les étapes selon-lui nécessaires pour que l'on puisse passer de la sécurité à la confiance : « *un : il faut que la technique soit disponible ; deux : que les outils soient déployés ; trois : que les gens soient conscients que les outils servent à résoudre les problèmes de sécurité qu'ils souhaitent voir résoudre. Et c'est à ce prix seulement qu'on acquiert la confiance* ». Cette analyse reste d'actualité.

[7] Public Key Infrastructure ou Infrastructure de Gestion des Clés

[8] Autorité d'Enregistrement

[9] Autorité de Certification

[10] Prestataires de Service de Certification

[11] http://www.fing.org/index.php?num=827,4

## Encadré : la confiance en équation ?

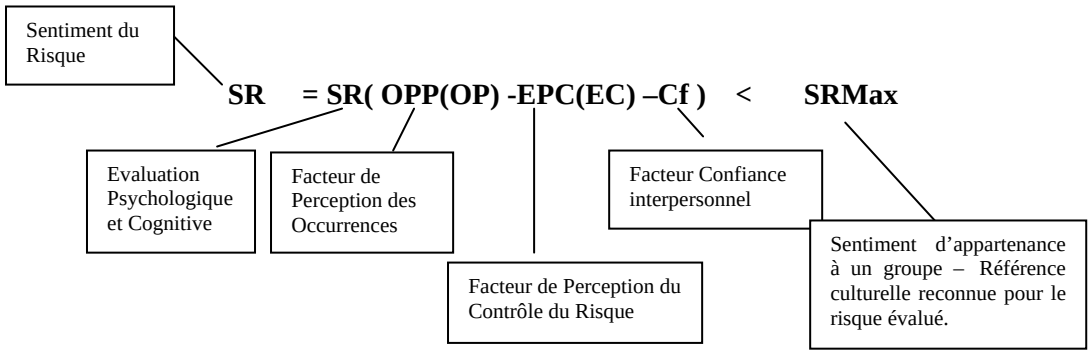
La confiance n'est qu'un élément de la chaîne de la perception du risque et intervient comme facteur motivant l'action (minorant du risque perçu) ou l'inhibant (majorant). De même la sécurité n'a d'efficacité que si elle est mise en scène pour que le risque soit perçu comme contrôlé donc minoré.

Henri Prévôt[12] se fonde sur les travaux menés par le Conseil Général des Mines (CGM) pour tenter de résumer la relation complexe dans le processus cognitif de la perception de la confiance.

Pour que soit possible une coopération fructueuse entre deux parties, le sentiment du risque *SR* doit être inférieur à un maximum *SRMax*. *SRMax* étant le sentiment du risque considéré comme limite acceptable pour la communauté et le sujet en référence.

Le sentiment de risque dépend de la perception du risque (*OPP* : occurrences perçues possibles) ; la perception du risque est diminuée par l'efficacité, telle qu'on la perçoit, des contrôles que l'on peut exercer, soit *EPC* ; la perception du risque est également diminuée par ce que nous appelons ici la confiance, *Cf*.

La perception des occurrences possibles et celle de l'efficacité du contrôle dépendent l'une des occurrences possibles, *OP*, et l'autre de l'efficacité du contrôle, *EC*. Ce qui donne la formule suivante :




Cette analyse rend compte de situations très diverses.

Ainsi, la confiance et le sentiment de risque peuvent coexister : *Cf* n'annule pas forcément *SR*. En cas de défiance, on dira que *Cf* est négatif, ce qui augmente la perception « nette » de risque, pour un même risque objectif et une même perception « brute », c'est à dire une perception dont on sait rendre compte. Là où l'incertitude brute perçue est nulle, il n'y a pas besoin de recourir à la confiance pour expliquer l'absence de sentiment de risque. Cela ne veut pas dire que la confiance n'est pas présente, mais elle n'est pas nécessaire. A l'inverse la défiance vient augmenter la perception du risque.

*Youval Eched*

[12] Henri Prévôt - L'Etat et la Confiance – Conférence à L'EHESS – Mai 2004

## *1.4. La confiance dans les dispositifs de confiance : une question essentielle*

La confiance peut se construire sur des dispositifs de confiance, qu'il s'agisse de technologies ou des services. Mais peut-on faire confiance à ces dispositifs ? La question n'est pas simple, mais elle est essentielle.

### 1.4.1. La qualité et l'éthique des développements

Les technologies et services de confiance intègrent souvent une forte composante logicielle. Or, ce secteur d'activé possède une spécificité forte en matière de qualité, notamment par rapport aux biens industriels : les *bugs* y sont considérés comme des éléments inévitables qu'il conviendra de corriger, au fil du temps, après la mise en service du produit.

Jacques Stern, ENS, démontre[13] ainsi que dans un secteur fortement lié à la sécurité, la cryptologie, il existe de nombreux exemples où des erreurs, facteurs de vulnérabilités, ont pu être repérées.
Les méthodes formelles constituent une approche pour améliorer la qualité des développements dans le domaine de la sécurité et de la confiance mais, Jean-Louis Lanet[14], Inria & Everest Team, précise qu'elles ne peuvent s'appliquer qu'à certains types de programmes de taille restreinte comme ceux qui figurent sur les cartes à mémoire.

En outre, précise Michel Riguidel, ENST, si les méthodes formelles peuvent apporter des améliorations quant au respect des spécifications, elles ne sont d'aucun secours pour se prémunir contre les attaques provoquées par le spécificateur. Cela pose la question à ses yeux essentielle de « *l'éthique des calculs* » ou comment interroger un programme sur ce qu'il fait réellement. Dans un futur proche, prédit-il, il y aura des programmes illégaux qui prendront une forme nouvelle et qui sauront disposer d'une puissance de calcul considérable. Le développement éthiquement incorrect sera très puissant.

### 1.4.2. La question de la souveraineté

Certaines technologies sont censées participer à la confiance, mais si elles sont achetées à des ennemis, ou à des faux amis, il est légitime de s'inquiéter. Cette interrogation renvoie notamment aux questions de souveraineté qui ont été particulièrement d'actualité au cours de l'année 2004 dans le domaine de la sécurité informatique et des infrastructures de confiance.

[13] http://www.fing.org/confiance/IMG/pdf/28-06-2004-J_Stern-FING-confiance.pdf

[14] http://www.fing.org/confiance/IMG/pdf/lanet_inria_Fing_Confiance_securite_250504.pdf

Diffusé en juin 2004, le rapport[15] du député Bernard Carayon consacré à la stratégie de sécurité économique nationale prône la création d'un Commissariat aux technologies de l'information, de la communication et de la sécurité. Il détaille, pour en souligner l'efficacité, l'importance du dispositif américain en matière de soutien à l'innovation.

Par ailleurs, depuis le début de l'année 2004, est annoncée la création d'Infrasec qui va conduire à une recomposition du paysage français de la PKI et de la certification électronique. La fusion entre deux fournisseurs français de certificats électroniques, Certplus et PK7, bénéficie de la bienveillance des pouvoirs publics et semble avoir pour conséquence, ou pour motivation, la marginalisation de Verisign. La société américaine, souvent critiquée pour sa position dominante dans le domaine des certificats électroniques, disposait de 20% du capital de Certplus. Elle n'apparaît plus dans le tour de table du nouvel ensemble qui proposera des offres reposant sur des technologies nationales.

En matière de souveraineté, l'un des enjeux principaux est en effet celui de la position quasi-hégémonique de certaines sociétés américaines dans des domaines ayant trait à la confiance et la sécurité : Verisign mais aussi Microsoft, Cisco, Intel... La question n'est pas tant celle du quasi-monopole dont ils disposent, que de leur relation, qu'ils ne choisissent pas nécessairement, avec les pouvoirs publics de leur pays d'origine – avec un double potentiel de surveillance, voire de blocage en cas de crise. Cette préoccupation ne porte plus uniquement sur les vendeurs de matériels informatiques, de « hard », comme à l'époque du Plan Calcul mais aussi, et surtout, les fournisseurs de « soft ».

Dans un domaine où il est difficile d'avoir des informations fiables et où la rumeur domine, Eric Schmidt[16], CEIS, cite un exemple précis et documenté : l'accord conclu entre Lotus et les autorités américaines en 1996 garantissant à ces dernières l'accès à 24 bits sur les fonctionnalités cryptographiques de 56 bits. Cet accord a provoqué de vives critiques au sein du gouvernement suédois qui s'était équipé du logiciel pour son département de la défense, le ministère des finances et le parlement.

Parmi les domaines où la question de l'hégémonie américaine est particulièrement sensible figurent notamment les plateformes de confiance ou les travaux de normalisation en matière de RFID.

### 1.4.3. Les tiers de confiance

Si l'on ne peut accorder totalement sa confiance à des dispositifs ou des technologies, pourquoi ne pas l'accorder à des acteurs spécialisés – les tiers de confiance – dont ce serait la vocation, a fortiori si cela cadre avec leur mission historique ?

[15] http://www.assemblee-nat.fr/12/rap-info/i1664.asp

[16] http://www.fing.org/confiance/IMG/pdf/FING_Confiance_28062004_CR_ABL.pdf

Pour Eric Caprioli[17], l'activité des tiers de confiance permet d'associer la question de la confiance à celle de la sécurité technique : « *la confiance doit donc s'entendre ici comme le sentiment de sécurité dans le marché numérique, qui recouvre à la fois les usages de la confiance, et l'industrie de la confiance qui les supporte* ».

De son côté, Laurent Gille souligne que le tiers de confiance ne crée pas la confiance, il supplée au manque de confiance en introduisant un rapport de force et une fonction d'assurance.

Youval Ched[18] explique que les tiers de confiance doivent disposer, par ordre d'importance, d'un statut, d'une image et, en dernier lieu, d'une compétence. Pour imager sa thèse, il fait un parallèle avec l'arbitre de foot qui doit en premier lieu être inscrit sur la liste officielle des arbitres, ensuite disposer des attributs visuels de sa fonction (tenue noire, sifflet, cartons jaune et rouge) et enfin - on pourrait presque dire accessoirement - bien arbitrer.

L'importance du statut et de l'image qui favorise les acteurs institutionnels et/ou historiques peut être une des explications de l'échec relatif des systèmes de paiement de type *escrow services* développés pour les sites d'enchères sur Internet. Ces jeunes sociétés, comme Tradescure ou escrow.com, se proposent moyennant une commission, de jouer le rôle de tiers de confiance entre le vendeur et l'acheteur. Le vendeur n'expédie son bien que lorsque l'acheteur a envoyé l'argent à *l'escrow service.* Il ne touche l'argent que lorsque l'acheteur a notifié à l'intermédiaire qu'il a bien reçu le bien, conforme et en bon état. Le concept est séduisant mais ces jeunes sociétés ne disposent ni d'une image, ni d'un statut sauf à disparaître au sein d'une véritable institution comme eBay[19].

Le modèle du tiers de confiance n'est pas unanimement accepté. Christian Huitema[20], architecte du groupe « *Windows Networking & Communications* » de Microsoft, s'est livré, à Autrans en janvier 2004, à une vive critique de cette vision centralisatrice de la confiance. Selon lui, l'avenir d'Internet est dans l'accentuation de la décentralisation, pour laisser faire inventeurs et commerçants. Il y a une technologie qui permet d'y parvenir : le pair à pair. Dès lors, il faut concevoir sur cette base des réseaux de confiance, notamment pour assurer la gestion des clefs publiques. Dans ce contexte, les tiers de confiance n'apportent rien à la sécurité.

[17] http://www.fing.org/ref/confiance/Fing_Confiance_ECaprioli_260204.pdf

[18] http://www.fing.org/universite/IMG/pdf/confiance-fing-190603-v3.pdf

[19] http://pages.ebay.com/help/community/escrow.html

[20] http://www.fing.org/index.php?num=4654,4

# 2. Typologie des technologies et services de confiance

Pour appréhender le paysage de la R&D dans le domaine de la confiance et de la sécurité sur les réseaux, il convient dans un premier temps de délimiter le champ couvert en établissant une typologie des technologies et services de confiance.

L'exercice est loin d'être trivial et il n'est guère possible d'aboutir à une typologie incontestable répondant aux deux critères d'exhaustivité et de non redondance, tant les domaines sont imbriqués et mouvants, notamment grâce aux avancées de la recherche.

Nous proposons dans les paragraphes qui suivent une typologie fondée en priorité sur les fonctionnalités assurées. Cette typologie permet de disposer d'une vue d'ensemble intégrant les domaines classiques et les approches les plus novatrices. D'autres typologies étaient envisageables comme celles fondées en priorité sur les disciplines scientifiques (cryptographie, statistiques, etc.) ou celles privilégiant les secteurs industriels (carte à mémoire, biométrie, etc.). Il convient également de préciser que les technologies et services qui appartiennent à l'univers de la « pure » sécurité informatique (*firewall*, antivirus, etc.) n'ont pas été pris en compte.

Enfin certaines approches reposent sur des trucs et astuces, rustiques et efficaces. Patrice Plessis, Gemplus, évoque[21] ainsi très sérieusement la feuille de papier aluminium qui enveloppe la carte sans contact pour éviter la lecture à distance à l'insu du porteur. Ce type de solution de confiance ne figure pas dans la typologie proposée.

## *2.1. Authentification et identification*

Un grand nombre de technologies et services de confiance ont pour finalité première de proposer des solutions en matière d'identification et/ou d'authentification. Encore faut-il avoir conscience que les définitions peuvent varier selon les secteurs. Cette confusion n'est pas volontaire mais elle conduit à rendre les débats plus complexes. Classiquement, une approche consiste à dire que l'identification correspond à la phase « je déclare que je suis moi » alors que l'authentification serait celle de « je prouve que je suis moi ». Le couple *login/password* en est une bonne illustration. Pour une deuxième école, l'identification correspond à la même phase – « je déclare que je suis moi » – mais l'authentification est perçue de façon bien différente : « je prouve que j'ai des droits, sans forcément avoir à m'identifier ». Le monde de la biométrie travaille sur des notions différentes en distinguant l'identification et la vérification. Identifier, c'est reconnaître une personne parmi une population nombreuse, une foule. Plus simplement la vérification consiste à s'assurer que l'identité qu'une personne a annoncée est vraie ou fausse par comparaison à des données préalablement stockées. D'autres auteurs, comme Charles Copin, proposent de s'en tenir aux définitions du dictionnaire pour constater qu'on identifie

[21] http://www.fing.org/confiance/IMG/pdf/Fing.org-27042004-Confiance_Gemplus-v0.3.pdf - page 5

une personne et qu'on authentifie un tableau ; le terme identification suffirait et la confusion ambiante proviendrait d'une mauvaise traduction du terme anglais *authentication*. Enfin, citons l'approche proposée dès 1998 par le RNRT pour lequel l'identification renvoie à trois problématiques associées : l'authentification (sécurité), le nommage (désignation) et la personnalisation (adaptation) ; l'authentification consistant dans ce contexte soit à vérifier l'identité d'une personne, soit à vérifier l'origine d'un contenu.

### 2.1.1. Carte à mémoire

La carte à mémoire a été popularisé en France par la Carte Bancaire, utilisée pour les fonctions paiement et retrait et par la Carte Vitale dans le domaine de la santé. Dans les deux cas, la carte assure une fonction d'authentification. Depuis ces dernières années, une distinction fondamentale s'opère entre les cartes avec contact et les cartes sans contact. Ces dernières sont proches des outils de mobilité et de traçabilité abordés au paragraphe 2.4 de ce document.

Les cartes à mémoire peuvent être classées selon des grandes familles auxquelles correspondent des fonctionnalités systématiques ou fréquentes :

| | Identification | Authentification, signature | Contrôle de droits et d'accès (physique ou non) | Stockage d'informations, de valeurs |
|---|---|---|---|---|
| Cartes d'identité | X | X | | |
| Cartes bancaires | X | X | X | |
| Porte-monnaie électronique | | X | | X |
| Cartes santé | X | | | X |
| Cartes SIM | X | | X | X |
| Cartes professionnelles | X | | X | |
| Cartes de transport | | | X | |
| Cartes multiservices | Parfois | | X | X |

On citera également pour mémoire la carte anonyme porteuse de droits comme le fût à l'époque la télécarte. Bien des observateurs pronostiquent l'essor prochain des cartes multi applications rendues possibles par de nouveaux standards comme EMV. La notion même de carte multi applications tend à rendre caduque la classification sectorielle opérée ci-dessus. Les cartes ville – ou « cartes de vie quotidienne » – quand elles associent les dimensions paiement, transport, accès sécurisé à des services en ligne, etc., appartiennent à cette catégorie.

En ce qui concerne les tokens ou clés USB, il est possible de considérer soit qu'il s'agit d'une technologie concurrente de celle de la carte à puce, soit qu'il s'agit d'un design particulier de celle-ci la destinant au porte-clé plutôt qu'au portefeuille. Nous retiendrons ici cette deuxième vision à un moment où les clés se démocratisent pour devenir, au-delà des fonctions sécuritaires d'identification et d'authentification, des disques durs amovibles, voire des lecteur de fichiers MP3. L'un des intérêts des clés USB par rapport aux cartes à mémoire classiques est qu'elles se branchent directement sur l'ordinateur sans nécessiter un lecteur spécifique.

### 2.1.2. Biométrie

Pour reprendre la définition proposée par Bernadette Dorizzi[22], INT Evry, La biométrie consiste à vérifier l'identité d'une personne à l'aide d'une ou plusieurs modalités qui lui sont propres.

Il convient de distinguer deux types de biométrie. En premier lieu, celle qui repose sur les caractéristiques physiques : empreintes digitales, iris de l'œil, forme du visage, forme de la main, voix ; en second lieu, celle qui se fonde sur les comportements : démarche, frappe du clavier, dynamique de la signature manuscrite, …

Les données génétiques, comme l'ADN, doivent est-elles considérées comme des données biométriques ? Oui, pour le ministère de l'intérieur pour qui le Fichier National Automatisé d'Empreintes Génétiques[23] (FNAEG) se situe dans la continuité des fichiers d'empreintes digitales. Non, pour un récent rapport[24] de l'OCDE dans la mesure où le code ADN peut être utilisé pour des finalités autres que l'identification, principalement pour l'analyse du risque médical. Toujours selon ce rapport, la question des vrais jumeaux – une naissance sur 250 – rend impossible l'utilisation de l'ADN comme dispositif unique d'identification. La nouvelle loi informatique et libertés[25] adoptée le 15 juillet 2004 semble considérer que les « données génétiques » et les « données biométriques » appartiennent à deux catégories différentes (Article 25 alinéas 2 et 8).

[22] http://www.fing.org/confiance/IMG/pdf/FING_30032004_MmeDorizzi_INT-Evry_Biometrie.pdf

[23] http://www.interieur.gouv.fr/rubriques/b/b7_aide_aux_victimes/fiche_fnaeg

[24] http://appli1.oecd.org/olis/2003doc.nsf/43bb6130e5e86e5fc12569fa005d004c/d15c6d3ea769bc64c1256e84004c42fc/$FILE/JT00166988.PDF

[25] http://www.cnil.fr/fileadmin/documents/approfondir/textes/CNIL-Loi78-17_Senat2.pdf

Deux autres distinctions sont très importantes à prendre en considération car elles fondent la doctrine de la Cnil en matière de biométrie :

- Nous laissons dans l'environnement, sans nous en rendre compte, des traces comme nos empreintes digitales ou notre ADN. Inversement, nous ne pouvons pas oublier un peu partout dans la nature la forme de notre main ou les caractéristiques de notre Iris. La Cnil fait donc une distinction entre la biométrie « avec traces » et la biométrie « sans traces ». La Cnil est réticente vis-à-vis des technologies avec traces car elles sont susceptibles de favoriser un « détournement de finalité » : l'empreinte digitale est collectée pour le contrôle d'accès, puis elle est utilisée pour une enquête policière. Il n'est pas anodin de souligner que l'industrie française est particulièrement en pointe dans le domaine des empreintes digitales, une biométrie « à trace ».

- Certaines solutions biométriques supposent l'existence de bases de données centralisées alors que d'autres opèrent une comparaison avec une information qui est uniquement en possession de l'usager.

Les avantages de la biométrie – ce « qu'on est » – par rapport aux autres écoles de type « ce qu'on sait » (les codes secrets) et « ce qu'on possède » (les cartes ou clés) sont bien connus. Elle permet d'éviter les vols, pertes, oublis … ou les prêts.

La biométrie, souvent associée à l'univers des cartes à mémoire, repose en réalité sur une approche probabiliste. Il s'agit d'optimiser deux taux critiques : le taux de faux rejets (FRR - *False Rejection Rate*) le taux de fausse acceptation (FFA - *False Acceptance Rate*) en fonction des caractéristiques de l'application (nécessitant plutôt un fort degré de sécurité ou plutôt une utilisation conviviale).

Au-delà des seules considérations techniques, il apparaît que l'acceptation sociale est aussi un facteur d'efficacité d'une solution biométrique. Longtemps cantonnée au seul domaine de la sécurité, la biométrie est appelée à se développer avec les nouvelles générations de titre d'identité et/ou de voyage. La « personnalisation d'environnement » pour les ordinateurs, les assistants numériques ou les téléphones Mobiles devrait aussi concourir à la démocratisation de la biométrie.

Devant cet engouement, des spécialistes, comme Philippe Wolf[26] de la DCSSI, soulignent que la biométrie ne saurait être suffisante pour valider, à elle seule, une authentification. Dans bien des cas, il conviendrait de l'utiliser en complément d'autres dispositifs comme le traditionnel mot de passe.

### 2.1.3. Certificats électroniques

Le certificat électronique est très souvent assimilé – à tort – à la signature électronique. Pour reprendre la définition pédagogique proposée par François-Xavier

[26] http://www.cnrs.fr/Infosecu/num46.pdf

Marquis[27] sur le site web de Chambersign, « *il s'agit d'une carte d'identité qui permet de savoir qui a signé un document. Le certificat authentifie la clé publique, comme une carte d'identité authentifie un exemplaire de la signature en y apportant des renseignements complémentaires* ».

Le certificat électronique répond bien à une logique d'identification/authentification. Il peut être purement logiciel – c'est le cas des 1,2 millions de certificats qui identifient les ménages fiscaux ayant eu recours au service TéléIR en 2004 - ou sur un support physique de type carte à puce ou clé USB. Dans le jargon de la profession, il est alors question de certificat de « classe 3+ ».

#### 2.1.4. Approches mixtes

Si elle a une certaine vertu pédagogique et technique, la présentation qui consiste à distinguer la carte à mémoire, la biométrie et le certificat électronique a dans la pratique un intérêt limité compte tenu des multiples applications qui associent deux, voire trois dimensions.

Les certificats de classe 3+ évoqués ci-dessus en fournissent une première illustration. Par ailleurs, la future carte d'identité électronique française, qui pourrait être opérationnelle en 2006[28], devrait être, selon toute vraisemblance, une carte à mémoire, intégrant un certificat numérique et des informations biométriques.

Ces approches mixtes constituent un domaine privilégié pour le développement d'innovations. Ainsi, une société californienne, Beepcard, vient de créer un prototype de carte bancaire munie d'une puce capable de reconnaître la voix de son propriétaire. Le code confidentiel est donc dicté à la carte qui vérifie qu'il n'y a pas fraude.

Autre exemple très différent, l'usage de la biométrie sur des appareils électroniques permet à la fois d'en sécuriser l'accès, d'accélérer la reconnaissance de l'utilisateur (plus de PIN) et de personnaliser la machine : la biométrie apporte ici de la commodité en même temps que de la sécurité.

### *2.2. Confidentialité*

#### 2.2.1. Cryptographie par algorithme

Pour Jacques Stern[29], ENS, la cryptologie est la science des messages secrets. Elle repose sur une trilogie fondamentale :

[27] http://www.chambersign.tm.fr/alaune/une.html

[28] http://www.interieur.gouv.fr/rubriques/c/c1_le_ministre/c13_discours/2003_09_26_idemocratie

[29] http://www.fing.org/confiance/IMG/pdf/28-06-2004-J_Stern-FING-confiance.pdf

- L'intégrité ; elle permet de prouver qu'un message n'a pas subi de modification ;
- L'authenticité ; elle sert à démontrer une identité à un interlocuteur, à prouver l'origine d'un message ;
- La confidentialité ; la cryptologie autorise la transmission d'une information sur un canal non sécurisé, ou l'archivage des données sur un média non sécurisé, de façon à ce qu'un tiers non autorisé ne puisse pas en prendre connaissance.

Même si c'est une approche réductrice, c'est ce dernier point qui est souvent, le plus spontanément associé en priorité à la cryptologie et à sa discipline sœur, la cryptanalyse, la science du « cassage » des codes secrets.

On ne reviendra pas ici en détail sur la description des méthodes et techniques utilisées. Les sources qui abordent ce sujet sont déjà largement disponibles. Rappelons uniquement que la cryptographie moderne repose sur le mécanisme des paires de « clés » publiques et privées dont les fondements théoriques et les premières applications sont apparues dans les années 70. En 1976, Whitfield Diffie et Martin Hellman publient les premiers travaux publics sur les systèmes de cryptographie asymétrique, à base de paires de clés publiques et privées. En 1978, Ronald Rivest, Adi Shamir et Leonard Adleman publient l'algorithme RSA, première application pratique des systèmes à clés publiques.

La cryptographie « moderne » est donc une discipline relativement ancienne, dont l'usage, à des fins d'authentification notamment, est largement diffusée via les téléphones mobiles ou les cartes bancaires, sans que le grand public en ait fortement connaissance. L'usage de la cryptologie pour assurer la confidentialité des messages reste en revanche relativement marginal au regard de la vivacité du débat politique sur la libéralisation de la cryptologie à la fin des années 90. L'un des enjeux importants autour de la cryptologie, et l'une des principales difficultés, concerne la question de la gestion des clés. Comment assurer efficacement la diffusion des informations à jour sur les clés publiques ? Comment créer les clés privées pour eux qui en ont besoin tout en maintenant le secret ? Les réponses à ces questions ne sont pas simples.

En matière de confidentialité, la cryptologie peut-être associée à la stéganographie qui consiste schématiquement à dissimuler sciemment une aiguille dans une botte de foin, par exemple une courte phrase chiffrée dans un faux spam[30].

### 2.2.2. Cryptographie quantique, cryptographie par le chaos

Si la cryptologie par algorithme est aujourd'hui une discipline mature, ce n'est pas le cas des nouvelles approches fondées sur la cryptographie quantique ou la cryptographie par le chaos. Dans les deux cas, la démarche consiste à faire reposer

[30] http://www.spammimic.com/index_fr.shtml

la sécurité sur les propriétés physiques - énergie optique, ondes - de l'information transmise.

Pour Laurent Larger[31], GTL-CNRS Telecom, ces technologies se donnent pour objectifs de compléter les méthodes classiques reposant sur des algorithmes de cryptage, et d'en dépasser certaines limites : le niveau théorique de confidentialité d'une part et le débit de transmission d'autre part.

L'une des grandes particularités de ces nouvelles cryptologies et de faire en sorte que toute « écoute » opérée entre les deux points d'une communication modifie le signal (clé ou données) et rend donc impossible le décryptage.

Les premières applications et les premières entreprises privées sont apparues dans le domaine de la cryptologie quantique alors que la cryptologie par chaos en est encore au stade du laboratoire.

Pour bien des spécialistes, il s'agit d'un domaine particulièrement important sur lequel de nombreux travaux de recherche sont actuellement menés (voir paragraphe 3.3.1 ci-après). Michel Riguidel[32], ENST, considère ainsi que le XXI$^{ème}$ siècle, à l'horizon 2020, sera quantique.

## *2.3. Preuves électroniques*

On peut classer sous le vocable générique de « preuves électroniques », un ensemble de technologies associé à la PKI (ou IGC pour Infrastructures à Gestion de Clés). Elles sont mises en œuvre dans le contexte de la dématérialisation des procédures.

La signature électronique, l'horodatage et l'archivage à valeur probante sont des éléments importants de la confiance sur les réseaux et au-delà d'une véritable économie de la confiance en cours de constitution.

Ces domaines sont ici cités ici pour mémoire, avec une reprise des définitions proposées par la FNTC[33] (Fédération Nationale des Tiers de Confiance), sans être développés. Ces questions ont été en effet peu abordés en tant que telles par le groupe de travail de la FING. En effet, d'autres organismes ou associations se livrent à un important travail en la matière (ADAE, Mission pour l'Economie Numérique, Forum des droits sur l'internet, FNTC, …).

Avec un cadre juridique désormais très complet, la priorité du secteur est sans doute moins celle de la R&D que celle du déploiement à grande échelle via le développement des usages.

[31] http://www.fing.org/confiance/IMG/pdf/FING_30032004_MrLarger_UMR-CNRS_crypto_Chaos.pdf

[32] http://www.fing.org/confiance/IMG/pdf/Michel_Riguidel_juin_2003.pdf - page 59

[33] http://www.fntc.org/articles/IMG/pdf/DP_fntc_juin2004.pdf

### 2.3.1. Signature électronique

La signature électronique peut se définir à un premier niveau comme une donnée ajoutée à une autre donnée ou à un ensemble de données et garantissant l'origine de cette ou de ces données, c'est-à-dire certifiant l'authenticité de l'émetteur. Elle serait dans l'univers du numérique la transposition de la signature manuscrite.

A un niveau plus complet, la signature électronique représente l'action de chiffrer, à l'aide de la clé privée d'une bi-clé, afin de garantir l'authenticité, l'intégrité et la non répudiation d'un document électronique.

Pour la FTNC dans le premier cas il s'agit d'*electronic non handwritten signature* et dans le second d'*electronic signature.* Cette distinction est à ce jour peu usitée.

### 2.3.2. Horodatage

Toujours selon la définition proposée par la FNTC, l'horodatage est un ensemble de techniques utilisant des algorithmes cryptographiques permettant de s'assurer si un document électronique a été créé ou signé à (ou avant) une certaine date. En pratique, la plupart des systèmes d'horodatation font appel à un tiers de confiance appelé Autorité d'horodatage (*TSA, Time-Stamping Authority*). Un horodatage est une attestation électronique émanant d'un TSA qui identifie qu'un document électronique lui a été présenté à une certaine date.

### 2.3.3. Archivage électronique

L'archivage électronique (*electronic archiving*) est l'action de recueillir, de classer et de conserver des informations à des fins de consultation ultérieure. L'archivage est une fonction en soi, qu'il ne faut confondre ni avec la sauvegarde ni avec la gestion électronique des documents. Dans un système de confiance, on aura recours à un archivage « sécurisé » (physiquement, mais aussi électroniquement via l'usage de la cryptographie pour permettre la vérification de l'intégrité du document, etc.), qui permettra de retrouver un document et de s'en servir comme preuve (« à valeur probante »).

### 2.3.4. Serveurs de preuve

Depuis une période récente est apparue le concept de « serveur de preuve » qui semble décrire les services associant les trois composantes déjà évoquées : signature électronique, horodatage et archivage numérique à valeur probante. Dans ce contexte, l'AFNOR a ainsi entrepris de normaliser les formats de preuves électroniques comme organe de base du marché de la confiance. C'est l'objet de la norme XP Z 74-600[34] dont la légitimité est fortement contestée par la FNTC[35].

[34] http://www.fing.org/confiance/IMG/pdf/Pages42A45de_E241.pdf

35 La lettre de la confiance - n°2 - juin 2004 – page 5. Abonnement par redaction@fntc.org

Les acteurs de la confiance ont, semble-t-il, bien du mal à se faire confiance mutuellement. Peut-être est-ce la preuve que l'on a bien quitté l'univers des laboratoires de recherche pour entrer résolument dans celui du marché.

## *2.4. Géolocalisation et Traçabilité*

Suivre ou être suivi à la trace peut être sécurisant. C'est aussi, parfois, une façon de miner la confiance. Les nouvelles applications liées à la mobilité des personnes ou des biens posent la question de la confiance dans un cadre renouvelé.

### 2.4.1. RFID

Les « tags » RFID, étiquettes intelligentes destinées à remplacer les codes à barre, auraient pu demeurer des technologies uniquement destinées à la logistique et l'approvisionnement, sans rapports directs avec la question de la confiance et de la sécurité.

Pourtant, très rapidement, des associations américaines de protection de la vie privée, comme Caspian, ont évoqué le spectre d'une société de la surveillance généralisée rendue possible par le RFID. Ces craintes, pas toujours fondées (du moins en l'état actuel de la technologie), ont rencontré un échos d'autant plus important que certains industriels faisaient preuve de maladresse en évoquant, voire en expérimentant des usages marketing pour le RFID. En France, la Cnil[36] s'est saisie de la question pour considérer que « *les RFIDs sont des identifiants personnels au sens de la loi Informatique et Libertés* ».

Les étiquettes RFID sont ainsi devenues une technologie susceptible de susciter la défiance du public alors qu'elles présentent, comme l'explique François Vacherand[37] (CEA-Leti) de fortes similitudes avec les cartes à mémoire sans contact généralement considérée comme des technologies de confiance.

Concrètement, un « tag » RFID peut être présenté comme une étiquette communicante associant une puce, une antenne, parfois une batterie et une mémoire, qui peut être lu par un autre appareil. Dans le cas des étiquettes actives, le signal est même envoyé vers un lecteur. Ces « lecteurs » peuvent être de toute nature : appareils mobiles, portiques, caisses sans contact...

[36] http://www.cnil.fr/index.php?id=1063

[37] http://www.fing.org/confiance/IMG/pdf/Fing.org_Confiance_-_CEA-LETi_-_Presentation_Tracabilite_et_Confiance.pdf

Les analyse de Joël Sarraillon[38] (pôle[39] traçabilité) et Yann Le Hegarat[40] (Cnil) tendent à montrer que les types d'applications sont très nombreux : contrôle d'accès, contrôle des pneumatiques, clés de voiture ; billetique, bagages aéroports, péages, animaux sur pied, lutte contre la contrefaçon de médicaments … C'est surtout dans le secteur de la distribution que les applications envisageables sont les plus nombreuses : logistique et réapprovisionnement, fidélisation, magasin sans caissières. Citons enfin l'importante fonction antivol qui illustre, si besoin était, qu'un système « de confiance » peut aussi reposer sur un fond de défiance.

Au-delà des aspects atteintes à la vie privée, les tags RFID soulèvent également une importante question de souveraineté dans le contexte des travaux de normalisation. Pour Joël Sarraillon, les travaux menés par l'organisation internationale EPCglobal reposent sur un concept « *trop américain* » ; une analyse qui est largement partagée par Thierry Dassault. Stéphane Cren, représentant français d'EPCglobal, abonde assez curieusement dans leur sens lorsqu'il écrit[41] : « *le réseau EPC a toutes les chances d'être la solution privilégiée à terme par les grands donneurs d'ordres anglo-saxons qui participent à son élaboration ».* Si le constat est identique, les recommandations diffèrent. EPCglobal France invite les sociétés françaises à se mobiliser en plus grand nombre au sein d'EPC. Joël Sarraillon espère que la normalisation ISO s'imposera en la matière.

### 2.4.2. Services géolocalisés

Pour reprendre la typologie proposée par Monique Gibeaux[42] (Bouygues Telecom) les services géolocalisés mobiles regroupent trois types de services : l'assistance en mobilité, l'aide au déplacement et la localisation des personnes. Dans la troisième famille figurent des services tels que la localisation et le suivi des personnes, qu'il s'agisse de ses employés, des enfants, des amis.

Pour mettre en œuvre ces services, nous explique Monique Gibeaux, quatre technologies, aux intitulés assez obscurs, sont sollicitées :

- Les technologies « LCS basées sur le Cell-ID » qui correspond à la localisation par la cellule ;
- Une variante plus précise de la localisation par la cellule avec le « Cell-ID + NMR »;
- Les technologies de localisation par satellite avec le GPS et l'AGPS ((*assisted GPS*, spécifiquement destiné à l'usage par des téléphones mobiles). A noter

[38] http://www.fing.org/confiance/IMG/pdf/Fing.org_Confiance_27042004_Pole_Tracabilite.pdf

[39] Basé à Valence, le Pôle traçabilité est un centre d'échange et de transfert des savoir-faire, aidant les entreprises à accélérer leurs processus d'innovation par l'utilisation des technologies de la traçabilité. http://www.poletracabilite.com/default.cfm

[40] http://www.fing.org/confiance/IMG/pdf/Fing.org_27042004-CNIL_3.pdf

[41] http://www.fing.org/confiance/IMG/pdf/EPC2004-061_Article_Reseau_EPC.pdf

[42] http://www.fing.org/confiance/IMG/pdf/Fing.org_27042004-_Bouygues_Tel_-_Geolocalisation_en_securite_et_confiance.pdf

que le grand projet Galileo de la Commission est à la fois concurrent et compatible avec le GPS ;

- Enfin, pour mémoire, la technologie E-OTD (*Enhanced Observed Time Difference*). Surtout utilisé aux Etats-Unis pour les services d'urgence, elle semble en voie d'abandon progressif du fait de ses coûts.

On pourra se contenter de retenir que la géolocalisation ne constitue pas une technologie, mais un ensemble de technologies avec deux grandes familles : la localisation terrestre et la localisation par satellite.

De son côté Cédric Nicolas[43], Bouygues Telecom, indique que les nouveaux services de téléphonie mobile doivent tirer partie des potentialités de quatre familles technologiques : l'infrarouge, le Bluetooth, le peu médiatique code à barres 2D et la carte sans contact déjà évoquée.

## *2.5. Protection des données personnelles et gestion de l'identité*

Si les nouvelles technologies sont susceptibles de porter atteinte à la vie privée, elles peuvent également apparaître comme un moyen d'assurer cette protection en complément ou en substitution du droit et de l'autorégulation. Les technologies de protection de la vie privée reposent pour une large part, mais pas uniquement, sur la dimension de confidentialité de la cryptologie (paragraphe 2.2). Dans le même temps, l'apparition des services de regroupement d'identifiant est un des indices qui tendent à montrer que l'on est passé d'une logique de protection/interdiction à une logique de maîtrise de la diffusion de « ses » données personnelles.

### 2.5.1. Technologies de protection de la vie privée (PETs)

Le secteur des Technologies de protection de la vie privée (*Privacy Enhancing Technologies* ou PETs) recouvre une large variété de technologies et de services crées non seulement par des entreprises mais aussi par des militants ou des institutions comme l'OCDE.

Le débat public sur l'intérêt des technologies de protections de la vie privée a pris de la vigueur devant les craintes que faisait naître, au plus fort de la bulle Internet, les discours volontariste sur la personnalisation des contenus.

On peut recourir à la typologie proposée par Yves Deswarte[44], LAAS-CNRS, qui distingue des catégories de PETs qui correspondent à des grandes finalités : les dispositifs de protection des adresses IP, les dispositifs de protection de la localisation, les dispositifs d'accès anonyme à des services, les services d'autorisation respectant la vie privée et, enfin, la gestion des données et de l'accès aux données.

[43] http://www.fing.org/confiance/IMG/pdf/Fing.org_Confiance_27042004_-_Bouygues_Tel_-_C._Nicolas.pdf

[44] http://www.fing.org/confiance/IMG/pdf/FING_30032004_MrDeswarte_LAAS-CNRS_Privacy.pdf

Une autre approche plus descriptive consiste à décrire les différents types de services et d'outils disponibles :

- Progiciels de chiffrement des e-mails et des documents joints.
- Stéganographie, technique qui consiste à dissimuler un message à l'intérieur d'un autre fichier ;
- Génération d'e-mails temporaires. Le texte des courriers n'est plus lisible passé un certain laps de temps ;
- Génération d'e-mails non rediffusables. Le destinataire du message ne peut pas le faire suivre à d'autres destinataires ;
- Services d'anonymisation de la navigation ;
- Remailer (re-acheminer), service qui permet d'envoyer des messages sans que le destinataire puisse identifier l'émetteur ;
- Service de disque dur distant avec chiffrement des données ;
- Progiciels de suppression des « traces » - cookies, cache, historique - sur l'ordinateur ;
- Gestionnaire d'identités virtuelles, etc.

Les dispositifs de filtrage anti-spam, anti-cookies, anti-spywares ou anti-pop-up sont parfois considérés comme des PETs. Les services de Webmails ne sont pas considérés comme des PETs alors qu'ils sont massivement utilisés pour la création d'adresses e-mail anonymes.

### 2.5.2. Services de regroupement d'identifiant

Longtemps perçue de façon réductrice comme une bataille entre Microsoft (*Passport*) et Sun (*Liberty Alliance*), la question des services de regroupement d'identifiant recouvre des enjeux fondamentaux pour l'économie numérique ou l'administration électronique. Comment doit s'organiser, sous le contrôle de l'usager, le partage de ses informations personnelles entre plusieurs organisations, par exemple un groupe de marchands ou plusieurs administrations.

Le service de base, emblématique de la gestion de l'identité en ligne est le « SSO ». Encore convient-il de préciser, souligne Yves Lions[45] (France Telecom R&D) s'il s'agit du très usité « *Single Sign On* » (procédure unique d'authentification), ou du «*Simplified Sign On*» (procédure d'authentification simplifiée) apparemment plus modeste dans ses ambitions. Le *Single Sign On* représente l'idéal d'ergonomie car l'utilisateur ne se ré-identifie pas en naviguant de site en site. Yann le Hegarat (Cnil) précise que les services de regroupement d'identifiant sont aussi des services de transfert de données. Dans le contexte des services avancés de l'administration électronique, la fonction SSO est complété par un « espace personnel[46] » sécurisé (ou coffre-fort électronique) qui permet, sous le contrôle de l'utilisateur, un partage des informations personnelles entre différents organismes.

[45] http://www.fing.org/confiance/IMG/pdf/FING_30032004_MrLions_FT_LibertyAlliance.pdf

[46] http://www.internet.gouv.fr/article.php3?id_article=1550

Deux modèles d'architecture sont envisageables. D'une part l'architecture centralisée qui était celle retenue pour le projet Passport de Microsoft et qui est souvent adoptée par les entreprises qui se dotent d'un annuaire LDAP pour leur besoins internes. D'autre part, l'architecture décentralisée qui est la philosophie retenue dans le cadre des initiatives WS-Federation[47] ou Liberty Alliance[48].

Les principaux concepts de la gestion fédérée de l'identité définis par Liberty Alliance sont respectivement : le cercle de confiance (*Circle of Trust*), ensemble des fournisseurs de services acceptant leurs utilisateurs respectifs ; le fournisseur d'identité (*Identity Provider*), site que le client a déclaré comme étant sa référence d'authentification pour entrer dans le cercle de confiance et les fournisseurs de services (*Service Providers*)

Pour l'utilisateur, la gestion de l'identité en ligne permet d'apporter une simplification de l'accès, une amélioration de l'ergonomie de la fluidité. Pour le fournisseur de services et le marchand, l'avantage essentiel réside dans la facilitation de l'accès, notamment l'acceptation de clients qui n'ont pas été identifiés par lui.

## *2.6. Les autres approches*

Sous ce vocable générique et imprécis ont été regroupé les différentes approches qui apparaissent « moins » technologiques, voire hétérodoxes, soit parce qu'elles reposent sur les statistiques, soit qu'elles se fondent pour une large part sur des mécanismes de réputation. Largement étrangères aux acteurs de la sécurité informatique qui n'y verront parfois « que du marketing », ces démarches représentent pourtant un pan significatif des dispositifs de confiance. De récentes initiatives dans le domaine de la recherche laissent entrevoir un possible rapprochement des cultures. Les plates-formes de confiance ont été également intégrées à ce paragraphe dans la mesure où elles sont assez largement étrangères à la culture nationale.

### 2.6.1. Marque de confiance et assurance

Les marques de confiance ou sceaux électroniques sont des mécanismes qui ne font pratiquement pas appel à la technologie. Malgré ou grâce à cela des initiatives américaines comme TRUSTe[49] ou BBBOnline[50] ont connues une large diffusion aux Etats-Unis dans le domaine du commerce électronique, principalement pour leur dimension « privacy » dans un pays qui ne dispose pas, au niveau fédéral, d'une loi informatique et libertés de portée générale. Dans le cadre de ces dispositifs, les

[47] http://www-106.ibm.com/developerworks/library/ws-fedworld/ ou http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnglobspec/html/ws-federation.asp

[48] http://www.projectliberty.org/

[49] http://www.truste.org

[50] http://www.bbbonline.org

entreprises signent une charte dans laquelle elles s'engagent à respecter certaines règles communes, notamment en matière d'information des utilisateurs ; elles peuvent également se soumettre à une forme d'audit de leurs pratiques et de leurs systèmes.

En France, de telles initiatives existent également à l'instar de Labelsite dans le domaine de commerce électronique BtoC ou de ChamberTrust pour le BtoB. La diffusion de ces « labels » reste cependant modeste.

Bien souvent ces marques de confiance vont se trouver confrontées à la concurrence des « marques de confiance de fait », comme le logo Visa ou la référence aux autorités de certification Verisign ou Thawte, qui contribuent à rassurer le public sans formalités ou engagements particuliers de la part du site marchand.

Curieusement, comme l'explique Jean-Laurent Santoni[51] (Marsh) l'assurance peut aussi être rattachée à cet univers. Le fait que l'assureur accepte de couvrir une technologie devient un label de confiance dont il est fait un usage marketing. Le marché est incité à faire confiance à celui qui, par nature, fera le moins confiance : l'assureur.

La démarche d'assurance peut se situer à la frontière de la marque de confiance et du système de détection des fraudes.

### 2.6.2. Bases fraude et scoring

En matière de lutte contre la fraude, par usurpation d'identité et/ou répudiation du paiement, il est possible de regrouper dans un même ensemble les approches fondées d'une part sur les bases d'information et d'autre part sur les technologies décisionnelles (scoring, datamining, réseaux de neurones) dans la mesure où elles sont souvent mises en œuvre par les mêmes sociétés. Ce sont des outils probabilistes ce qui tend à les rapprocher des solutions biométriques.

A titre d'exemple, trois grands types d'applications peuvent être cités :

- La mutualisation des informations sur la fraude comme dans le système d'analyse des commandes de la société Fianet : « Ce numéro de carte bancaire a déjà été utilisé chez un autre marchand, par un autre porteur pour un paiement frauduleux » ;

- La détection des incohérences dans les demandes de crédit : « Dans le formulaire de demande de crédit, l'adresse citée a déjà été utilisée plusieurs fois par d'autres demandeurs de crédit qui n'ont jamais honoré leurs remboursements » ;

[51] http://www.fing.org/confiance/IMG/pdf/Marsh_JLS_Fing_Confiance_securite_250504.pdf

- La détection des cartes bancaires qui « flambent » à l'étranger, ce qui engendre une suspicion d'usurpation d'identité sur la base d'une comparaison avec l'usage « normal » et « habituel » de la carte.

Dans les pays où il existe des *credit bureaus* ou fichier positif de crédit comme au Royaume-Uni, ces bases d'information peuvent devenir des outils d'aide à l'authentification en ligne et/ou au remplissage automatique des formulaires[52]. Elles deviennent alors des concurrents de fait (mais *a* priori moins protecteurs de la vie privée) des services de regroupement d'identifiant.

### 2.6.3. Systèmes à base de réputation et moteur de confiance

Les systèmes de confiance à base de réputation (ou *Reputation-Based Trust Models*) ont été popularisés par les profils d'évaluation des vendeurs en vigueur sur eBay. C'est aussi un domaine de recherche à part entière pour des chercheurs qui se proposent d'enrichir l'approche classique - la notation par les pairs - avec d'autres critères pour aboutir à des dispositifs sécuritaires particulièrement destinés aux réseaux P2P ou aux jeux en réseau. Pour Jean-Marc Seigneur du Trinity College de Dublin, à partir du moment où l'on travaille sur des modèles de confiance qui reposent sur la réputation, on est dans le domaine des « moteurs de confiance ». Il est lui-même impliqué dans le projet SECURE soutenu par la communauté européenne. Ce moteur de confiance associe un « module de confiance » avec les interactions précédentes et les recommandations par des tiers, ainsi qu'une « base de preuves » utilisée pour mettre à jour les niveaux de confiance et de risque et un « module de risques » qui évalue dynamiquement le risque[53].

Dans le domaine de la PKI, il existe également des systèmes de certification non hiérarchiques fondés sur la réputation. Ils constituent une alternative, peu répandue, aux mécanismes centralisateurs qui reposent sur les missions des Autorités de Certification.

### 2.6.4. Les plates-formes de confiance

Les plates-formes de confiance[54] (ou TPM pour *Trusted Platform Modules*) sont apparues à partir de 1999 avec la mise en place du *Trusted Computing Platform Alliance* (TCPA). L'objectif est de définir une architecture matérielle qui serait commune aux prochaines versions des ordinateurs de façon à renforcer la sécurité. Selon l'angle retenu, les plates-formes de confiance – popularisées par les sigles Palladium puis NGSCB (*Next Generation Software Computing Base*) – sont présentées par leurs initiateurs comme des technologies de protection des données mais aussi comme un moyen de faire respecter les droits de propriété intellectuelle

[52] http://www.uk.experian.com/business/featuredproducts/eseries/

[53] Pour une présentation détaillée en français : http://www.fing.org/confiance/IMG/pdf/articletrustcompubimob.pdf

[54] http://www.fing.org/confiance/IMG/pdf/FING_30032004_MrLe_Hegarat_CNIL_Identification_par_la_machine.pdf

sur les contenus numériques, principalement les progiciels, en empêchant techniquement les copies illégales.

Les sociétés américaines, dont Microsoft, étant en position de force dans le consortium, le concept de plateforme de confiance a suscité une grande défiance[55].

[55] http://www.fidens.fr/infosec2003.pdf

## Encadré : Difficulté des typologies, l'exemple de l'identité numérique

Dans un domaine connexe aux technologies et service de confiance – les services et technologies de gestion des identités numérique et de protection des données personnelles – on est confronté à la même difficulté lorsqu'il s'agit d'établir une typologie.

L'univers de l'identité numérique est en effet une bonne illustration d'un domaine phare de la confiance où des secteurs économiques différents travaillent sur des problématiques proches, enchevêtrées, sans forcément se concerter ni même avoir conscience de ce qui se fait ailleurs. Est-il possible de favoriser les coopérations, de partager les expériences pour gagner en efficacité ? Les tendances observées dans d'autres secteurs sont-elles susceptibles de remettre en cause certaines approches ?

Un aperçu rapide des quelques régions du paysage d'ensemble de l'identité numérique[56] :

- La signature électronique
- Les cartes d'identité électronique
- Les autres cartes (santé, ville, professionnelles)
- La biométrie
- Les projets LDAP ou IAM (Internet Access Management) des entreprises
- Les services de regroupement d'identifiant
- L'univers bancaire (Visa – 3D Secure)
- Les bases d'information anti-fraude
- L'univers des Télécom (Super annuaire Enum)
- Les noms de domaine
- Les privacy enhancing technologies
- Les nouveaux usages du pseudonymat sur les réseaux

[56] http://www.fing.org/index.php?num=4792,2

# 3. Cartographie des projets de recherche « Confiance et sécurité »

La confiance et la sécurité sont des thèmes récurrents, présents dans de nombreux chantiers ayant trait à l'économie numérique et à la société de l'Information. Dès lors, établir une cartographie des projets d'innovation et de R&D en la matière n'est pas chose aisée. Le foisonnement des initiatives pourrait même être susceptible de conduire à une perte d'efficacité. Les pouvoirs publics en sont conscients puisqu'en juillet 2003, le Conseil interministériel de la société de l'information (Cisi) a décidé une coordination nationale de la R&D en matière de Sécurité des systèmes d'information. Comme l'a indiqué Alain Esterle[57], Directeur adjoint de la DCSSI, ce travail a débuté par une coordination renforcée entre les équipes ministérielles (Recherche, Industrie, Anvar, DCSSI) ; il s'étend aujourd'hui auprès d'équipes de recherche, puis concernera à l'automne 2004 des partenaires industriels.

Pour établir une cartographie, forcément simplifiée, des projets de R& D dans le domaine « *Trust & Security* », il a paru pertinent de distinguer les initiatives menées au niveau communautaire des projets qui s'inscrivent dans un cadre national. Le tour d'horizon est complété par un panorama de travaux menés par quelques pôles de recherche aux Etats-Unis ou en Asie.

L'exercice permet d'identifier à grand trait les domaines prioritaires, de cerner l'évolution au cours des dernières années et de déduire les points forts de la France dans le domaine.

## *3.1. Les projets communautaires confiance et sécurité*

### 3.1.1. Les projets du Ve PCRD

Le Ve PCRD (Cinquième **P**rogramme **C**adre de la Communauté Européenne pour des actions communautaires de **R**echerche, de **D**éveloppement technologique et de démonstration) couvrait la période 1998 – 2002. Il comportait un volet significatif consacré à la sécurité, intitulé « *Vers un cadre globale de fiabilité et de sécurité* ».

Les informations diffusées[58] sur le site de la Commission européenne permettent d'accéder aux fiches descriptives de 64 projets portant sur ces thèmes. Certains de ces projets comme ePoch, Finread, Pisa ou Aequitas bénéficient d'une certaine notoriété en France dans une partie de la communauté de la confiance. En faisant abstraction du montant de ces projets et de leur éventuel succès, ce qui à l'évidence limite la portée de la démonstration, il est tout de même possible de situer le « centre de gravité » des projets à partir de leurs descriptifs et ainsi de disposer d'une vue d'ensemble de ce qu'étaient les priorités de la Commission européenne à l'époque du Ve PCRD.

[57] http://www.fing.org/confiance/IMG/pdf/FING_Confiance_28062004_CR_ABL.pdf

[58] Télécharger le fichier pdf « *Projects synopses* » à partir de la page http://www.cordis.lu/ist/so/dependability-security/projects/projects.htm

Sur les 64 projets ayant fait l'objet d'une fiche descriptive :

- 17 projets sont fortement connotés « carte à puce » (*smart card*)
- 7 projets « biométrie »
- 7 projets « DRM » et/ou « Watermarking »
- 6 projets d'infrastructure de sécurité
- 5 projets « signature électronique », « PKI » ou « preuve »
- 2 projets « *Privacy Enhancing Technologies* »
- 1 projets « cryptographie »
- 1 projet « sans-fil »
- 1 projet « *token USB* »

Cette classification pourrait être affinée en prenant en compte que certains projets associent plusieurs dimensions comme ceux qui portent à la fois sur les cartes et la biométrie (Projets Banca, Bee, S-Travel, …). De plus, la dimension cryptographie et/ou PKI est très souvent présente dans les descriptifs au-delà du projet qui apparaît comme « purement » cryptographique : Stork.

Les descriptifs des projets permettent également d'identifier en creux les domaines qui n'étaient pas considérés, à l'époque, comme faisant partie du champ *trust & security*. Aucun projet ne porte sur la traçabilité, sur les systèmes à base de réputation, sur les sceaux électroniques ou sur les approches décisionnelles (scoring, datamining, réseaux de neurones).

La présence française sur ces 64 projets est significative avec une forte tendance à se concentrer sur un domaine de prédilection : la carte à mémoire. 12 projets sur 64 affichent un coordinateur français, 8 fois dans le domaine *smart card* dont 4 projets coordonnés par le seul GIE CB. Le nombre des projets où il y a au moins un partenaire français s'élève à 35, soit plus de la moitié.

Dans le secteur privé, les partenaires les plus présents sont les suivants :

- France Telecom (5), Orange France : 6 projets
- Schlumberger Systèmes (4), Sema, Atos : 6 projets
- Gemplus : 5 projets
- Sagem : 4 projets
- Ingenico : 3 projets
- Oberthur Card Systems (2), Oberthur : 3 projets

Le secteur de la recherche est également représenté avec l'INRIA (3 projets), le CNRS (2), l'ENS (2), l'ENST, le Groupe des Ecoles des Telecommunications, etc.

Pour résumer, le coordinateur français type pour les projets « confiance et sécurité » du Ve PCRD est le GIE CB alors que le partenaire type serait plutôt une grande société privée du secteur de la carte à mémoire ou un laboratoire de recherche.

Là encore, la prise en compte des budgets des projets et de leurs succès permettraient certainement de disposer d'une autre vision. Ce travail reste à accomplir.

### 3.1.2. Les projets du VIe PCRD

Comme les programmes qui l'on précédé, le VIème programme-cadre de recherche (2002-2006) valorise les actions de recherche et de développement technologique, en cofinançant des projets menés en partenariat. Il parait pertinent pour analyser les projets menés dans le domaine de la sécurité de distinguer les classiques projets IST et les projets eTen ; ces derniers, avec des objectifs court terme, étant plutôt axés sur la question du déploiement.

IST : Projets intégrés et Networks of Excellence[59]

Le domaine de la sécurité recouvre 14 projets dont les intitulés détaillés, en anglais, donnent une vision d'ensemble des domaines couverts par les projets européens :

- DIGITAL PASSPORT : Next generation European Digital Passport with Biometric Data for Secure and Convenient Boarder Passage ;
- ECRYPT : European Network of Excellence in Cryptology ;
- e-JUSTICE : Towards a global security and visibility framework for Justice in Europe ;
- FIDIS : The Future of Identity in the Information Society ;
- INSPIRED : Integrated Secure Platform for Interactive Personal Devices ;
- MEDSI : Integration of Geographical Information Systems with DB, decision support management and an auditory system to develop an advanced system that will be able to give support on decisions in a crisis ;
- POSITIF : Policy-based Security Tools and Framework ;
- PRIME : Privacy and Identity Management for Europe ;
- s-BORDER : Privacy respectful and threat tuneable traveller smart monitoring system ;
- SCARD : Side-Channel Analysis Resistant Design Flow ;
- SECOQC : Development of a Global Network for Secure Communication based on Quantum Cryptography ;
- SECURE JUSTICE : Secure communication and collaboration framework for the judicial co-operation environment ;
- SECURE PHONE : Secure contracts signed by telephone ;
- SEINIT : Security Expert INITiative.

[59] Ce paragraphe reprend largement le contenu d'un document – « Compte-rendu d'activité, Décembre 2003 » - du Comité de pilotage du RTP 13 Sécurité du CNRS.
http://www.fing.org/confiance/IMG/pdf/Rapport_RTP_13_securite-3.pdf

Par rapport au Ve PCRD, les projets européens semblent marquer une montée en puissance de la thématique identité numérique. Elle apparaît en tant que telle (Fidis) ou associée aux aspects technologies de protection de données (Prime) ou document d'identité ou de voyage (s-Border, Digital Passport). On peut également noter que la cryptographie quantique fait son apparition dans les projets soutenus par la Communauté Européenne (Secocq).

Le coordinateur est français pour 4 projets : Gemplus (Inspired); EADS (s-Border); Thales Communications (Seinit) mais également IBM France (Prime).

La présence de la R&D française dans les projets du Vie PCRD ne se limite pas aux projets pour lesquels un organisme national assure le rôle de coordinateur. Le bilan – positif - que dresse le RTP 13 à propos de son action en témoigne :

- Pour le projet ECRYPT, le groupe de cryptologie de l'ENS est fortement impliqué dans ce *Network of Excellence*. Jacques Stern préside le comité stratégique. L'INRIA y participe également tout comme au projet INSPIRED ;
- Michel Riguidel, ENST, est le responsable scientifique du Projet SEINIT consacré à la sécurité sur les réseaux. Il participe également activement, tout comme Philippe Grangier (Institut d'Optique d'Orsay, CNRS,) au projet SECOQC portant sur la cryptographie quantique
- Refik Molva, Institut Eurécom, participe aux projets e-JUSTICE et PRIME sur la protection des données personnelles et la gestion des identités ; un projet auquel participe également Yves Deswarte[60], LAAS-CNRS ;
- Enfin, dans le domaine de la biométrie, le *Network of Excellence* BIOSECURE est piloté par l'INT.

<u>eTEN</u>

Parfois associés au VIe PCRD – le dispositif communautaire des aides à l'innovation n'est pas d'une grande lisibilité – les « Appels à propositions concernant des projets d'intérêt commun dans le domaine des réseaux transeuropéens de télécommunications » ou eTEN comportent un volet confiance et sécurité. Ces projets portent principalement sur le déploiement mais aussi la validation commerciale. Les objectifs se situent clairement dans le court terme. 6 thèmes sont prévus dans l'appel à projet diffusé en mars 2004, le thème 5 étant explicitement intitulé « Confiance et sécurité ». Les autres thèmes concernent les pouvoirs publics en ligne, la santé en ligne, l'intégration en ligne (*e*Inclusion), l'apprentissage en ligne, et les PME. La dimension confiance et sécurité couvre la moitié du domaine eTen si l'on considère que pouvoirs publics en ligne et santé en ligne sont deux domaines pour lesquels ces aspects sont essentiels.

[60] http://www.fing.org/confiance/IMG/pdf/FING_30032004_MrDeswarte_LAAS-CNRS_Privacy.pdf - page 11

### 3.1.3. La préparation du VIIe PCRD

Le VIIe PCRD[61], qui concerne la période 2007-2011, accordera une place importante à la sécurité dans la mesure où il s'agit d'un des deux nouveaux domaines prioritaires de l'Union avec le programme spatial européen. Cette orientation est d'autant plus importante que la Commission propose un doublement du budget du futur PCRD qui atteindrait 40 milliards d'euros. Des actions préparatoires dans le domaine de la sécurité sont prévues pour la période 2004-2006, avec un budget de 65 millions d'euros, pour lancer quelques cas test. Toutefois, il s'agit bien de la sécurité au sens large et non dans le seul domaine IST.

### 3.1.4. Les autres projets européens

Un travail complémentaire reste à effectuer pour identifier les projets confiance et sécurité pouvant être associés aux dispositifs rattachés à Eureka et liés aux au micro et nanotechnologies ou à la microélectronique : ITEA[62], Eurimus[63], Pidea[64] et Medea[65].

Dans le domaine de la sécurité, en mars 2004, l'union européenne a décidé de se doter d'une Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA)[66]. Cette agence, qui sera implantée à Héraklion en Grèce, « *aura une fonction de conseil et de coordinations des mesures prises par les Etats membres pour sécuriser leurs réseaux et systèmes d'information* ». L'ENISA entend également collecter et analyser des informations sur les incidents, promouvoir des méthodes de gestion des risques et favoriser des partenariats public/privé. Le soutien à l'innovation et à la R&D ne semble donc pas faire partie de ses attributions. L'agence, qui devrait être dotée d'une direction à l'automne 2004, semble connaître un démarrage assez laborieux.

## *3.2. Les projets « confiance et sécurité » en France*

Si les acteurs français de l'innovation et de la R&D sont présents sur des projets menés à l'échelle européenne, ils le sont également dans le cadre de programmes nationaux. Les projets ACI se situent en amont, ceux des réseaux de recherche concernent le moyen et long terme tandis qu'Oppidum est un dispositif orienté vers les réalisations à plus court terme.

---

[61] En savoir plus http://www.eurosfaire.prd.fr/bibliotheque/pdf/FP7_MAE_18-02-2004.pdf

[62] http://www.itea-office.org/index.php

[63] http://www.eurimus.com

[64] http://www.pidea.com.fr/index2.htm

[65] http://www.medea.org/

[66] http://europa.eu.int/scadplus/leg/fr/lvb/l24153.htm et http://www.enisa.eu.int/

### 3.2.1. L'ACI « Sécurité informatique »

Le Ministère délégué à la Recherche et aux Nouvelles Technologies a créé en 2003 une Action Concertée Incitative (ACI) intitulée «Sécurité Informatique »[67] qui est menée en collaboration avec le département Sciences et Technologies de l'Information et de la Communication du CNRS, l'INRIA et la DGA (Délégation Générale de l'Armement). Cette ACI traite à la fois de la sécurité et de la sûreté de fonctionnement.

Le dispositif concerne la recherche amont celle qui, schématiquement, est l'affaire des laboratoires et non des entreprises.

L'appel à proposition 2003 avait pour objectif de dynamiser la recherche sur l'ensemble des aspects de la sécurité des systèmes informatiques. Les champs disciplinaires concernaient notamment les aspects suivants : *composants, surveillance, diagnostic, sûreté de fonctionnement, preuve, vérification, tests, tolérance aux fautes, cryptologie, tatouage, chiffrement, identification, authentification, certification, méthodes statistiques, traitement du signal, approches métiers, aspects légaux et éthiques de la sécurité* ».

Cette liste permet de constater que les sujets fortement connotés confiance (« *preuve* ») ou ceux liés aux sciences sociales (« *aspects légaux et éthiques de la sécurité* ») faisaient dès l'origine partie de ce programme sécurité.

Sur les 28 projets initialisés en septembre 2003 figurent notamment des travaux abordant la biométrie multimodale, les réseaux quantiques, le chaos pour la sécurité des transmissions, …

L'Appel à propositions 2004 se situait dans le prolongement du précédent avec une prise en compte peut-être plus explicite de la dimension juridique. C'était l'une des cinq priorités indiquées par le texte de l'appel à projet: « *une attention particulière sera portée aux projets visant à développer les thèmes suivants :*

- *l'émergence et le suivi d'une législation garantissant à la fois le respect de la vie privée, les souverainetés nationales et les échanges internationaux basés sur une confiance réciproque démontrable,*
- *les recherches duales (i.e. civile et militaire),*
- *la vérification, la validation, le test, la mesure et l'évaluation de la sécurité et la sûreté de fonctionnement des systèmes informatiques,*
- *les mécanismes et algorithmes en ligne destinés à améliorer la sûreté et la sécurité des systèmes et des réseaux*
- *la sécurisation des couches basses des systèmes informatiques.*

Le conseil scientifique a retenu, avant confirmation de ces choix par le Ministère de la recherche, 19 projets devant être initialisés en septembre 2004. Parmi les domaines abordés, on retrouve notamment un projet (Asphales) qui porte sur « les

[67] Une information très complète est disponible sur http://acisi.loria.fr/

interactions entre sécurité informatique et sécurité juridique dans les chantiers normatifs de la Société de l'Information » ou un autre (Satin) sur « l'analyse de la sécurité pour des protocoles et infrastructures de confiance ».

### 3.2.2. Les projets des réseaux de recherche

Les réseaux de recherche ou pour reprendre la terminologie officielle les « réseaux de recherche et d'innovation technologique » (RRIT) ont pour objectif de développer les interactions entre la recherche académique et les entreprises. Ils ont été mis en place à partir de 1997 et 1998. Selon la présentation[68] officielle : « *les RRIT ont pour objectif de décloisonner les acteurs publics et privés de la recherche. Ils visent à permettre la préparation de projets technologiques stratégiques par une démarche conjointe des administrations, des institutions publiques de recherche et des milieux industriels, qu'il s'agisse de grands groupes ou de PME. Ils ont également pour objectif de favoriser les projets collaboratifs de R&D associant les laboratoires publics de recherche et les industriels, ainsi que de promouvoir la participation des PME-PMI dans des consortiums stratégiques* ».

Quatre réseaux de recherche, associés au groupe de travail de la Fing sont plus particulièrement concernés par la thématique « confiance et sécurité sur les réseaux » :

- Le RNRT[69] (Réseau National de Recherche en Télécommunications)
- Le RNTL[70] (Réseau National de recherche et d'innovation en Technologies Logicielles)
- Le RIAM[71] (Réseau Recherche et Innovation en Audiovisuel et Multimédia)
- Le RMNT[72] (Réseau micro et nanotechnologies)

Il s'agit logiquement des 4 réseaux, sur un total de seize, qui appartiennent au champ sectoriel « technologies de l'information et de la communication »[73].

Sur la base des fiches descriptives des projets labellisés par les réseaux de recherche, diffusées sur Internet, une analyse quantitative relative à la dimension confiance et sécurité peut être entreprise. Les limites de cette approche sont les mêmes que celles déjà évoquées précédemment à propos des projets européens (pas de prise en compte de l'importance des projets et de la dimension succès ou échec).

[68] http://www.telecom.gouv.fr/reseaux/body.htm

[69] http://www.telecom.gouv.fr/rnrt/index_exp.htm

[70] http://www.telecom.gouv.fr/reseaux/rntl.htm

[71] http://www.telecom.gouv.fr/reseaux/riam.htm

[72] http://www.rmnt.org/

[73] http://www.telecom.gouv.fr/reseaux/body.htm

RNRT

Pour le RNRT, le volet confiance et sécurité est une préoccupation ancienne (depuis 1998) et importante sur le plan quantitatif. 26 projets sont susceptibles d'y être rattachés en y intégrant un projet « identité numérique » (Numerobis), un projet traçabilité (Transwap) et un projet « méthodes formelles » (Calife). La labellisation de projets sécurité concerne aussi bien les projets précompétitifs (17) que les projets exploratoires (9).

Par rapport à l'ensemble des projets labellisés par le RNRT, la proportion de projets « confiance et sécurité » semble diminuer sur la période récente en passant d'un tiers en 2002 à un cinquième en 2003 (plus précisément 4 sur 18 pour les projets labellisés issus de l'appel à projet 2003 et 10 sur 29 en 2002).

Le tableau récapitulatif permet de disposer d'une vue d'ensemble sur la nature des projets concernés :

| Année de labellisation | Intitulé du projet | Type de projet | Intitulé détaillé |
|---|---|---|---|
| 2003 | SAFECAST | Exploratoire | Sécurité des Communications de Groupe |
| 2003 | X-CRYPT | Exploratoire | Outils cryptographiques adaptés aux réseaux de télécommunications à haut débit et aux réseaux sans fil émergents, combinant caractéristiques de sécurité avancées et faible consommation de ressources |
| 2003 | ADSR | Précompétitif | Architecture Dynamique pour la Sécurité |
| 2003 | PISE | Précompétitif | Passerelle Internet Sécurisée et flexible |
| 2002 | CRYPTO ++ | Exploratoire | Protocoles cryptographiques pour la sécurité multi-acteurs |
| 2002 | DURACELL | Exploratoire | Durcissement aux Attaques par fautes de Cellules pour circuits sécuritaires |
| 2002 | SEMANTIC-3D | Exploratoire | Service d'Echange et de MANipulation (Tatouage, Indexation et Compression) des objets 3D |
| 2002 | ANAIS | Précompétitif | Avancées vers une Nouvelle Air Interface pour des applications Sécurisées |
| 2002 | EPIS | Précompétitif | Embarquer un Protocole Internet Sécurisé. Définir, prototyper et tester les mécanismes de sécurisation des échanges de données entre les postes d'administration, les terminaux, et la carte à puce, dans le cas d'utilisation de réseaux ouverts et de l'utilisation des protocoles Internet pour des applications de gestion de parc. |
| 2002 | EVERYWARE | Précompétitif | Nouveaux usages basés sur le déploiement de services mobiles, sécurisés et multimédia dans un environnement sans fil hétérogène |
| 2002 | IdSA | Précompétitif | Infrastructure DNS sec et Applications |
| 2002 | RESODO | Précompétitif | Sécurité des réseaux domestiques ; usage des accès hauts débits et des liaisons sans fil |

| | | | |
|---|---|---|---|
| 2002 | NUMEROBIS | Précompétitif | Expérimentation nationale ENUM |
| 2002 | SDMO | Précompétitif | Diffusion sécurisée de musique vers les mobiles : 'Secured Diffusion of Music on mObiles' (SDMO |
| 2001 | MP6 | Exploratoire | Modèles et Politiques de Sécurité pour les Systèmes d'Informations et de Communications en Santé et Social |
| 2000 | ICARE | Précompétitif | Infrastructure de Confiance sur des Architectures de RésEaux internet & mobile |
| 2000 | SWAP | Précompétitif | Sécurité des applications et transactions exécutées depuis un terminal sans fil utilisant une pile de type WAP |
| 2000 | TRANSWAP | Précompétitif | Application de gestion d'une flotte de véhicules d'un transporteur routier utilisant un service WAP. |
| 1999 | TUAMOTU | Exploratoire | Tatouage électronique sémantique de Code Mobile Java |
| 1999 | TURBO-SIGNATURE | Exploratoire | Optimisation des ressources dans les protocoles de signature numérique et d'authentification à clé publique. |
| 1999 | ABBIS | Précompétitif | Automates Bancaires et Bornes Internet Sécurisés par vérification multimodale |
| 1999 | RAHMS | Précompétitif | Réseau Ad Hoc Multiservices Sécurisé |
| 1998 | CALIFE | Exploratoire | Environnement pour la Preuve formelle et le Test d'Algorithmes utilisés en Télécommunication |
| 1998 | AQUAMARS | Précompétitif | AQUAMAR quage des documents audiovisuels pour leur transmission, diffusion, circulation, distribution en toute Sécurité |
| 1998 | MobiSecV6 | Précompétitif | Gestion et sécurité de la mobilité dans l'Internet Nouvelle Génération (IPv6) |
| 1998 | SEVA | Précompétitif | Sécurisation d'Extranet Virtuels en utilisant des Agents intelligents |

RNTL :

Les projets possédant une forte composante confiance et sécurité sont peu nombreux parmi ceux labellisés par le RNTL. Cependant, à chaque fois, en 2000, 2001 et 2002, un des projets est lié à ces aspects pour un total respectif de 39, 30 et 35 projets.

Les trois projets concernés sont tous de type exploratoire. Il s'agit par ordre d'ancienneté d'EVA (Évaluation et Vérification Automatique de protocoles cryptographiques, 2000), de DICO (Détection d'Intrusion Coopérative, 2001) et d'EDEN (Validation formelle en vue d'une évaluation aux plus hauts niveaux des Critères Communs, 2002).

L'année 2003 semble marquer une sensibilité plus forte du RNTL à la question de la sécurité. Ainsi, lors de la journée RNTL du 17 octobre 2003, une session spécifique était consacrée à la Sécurité des systèmes d'information.

RIAM :

Pour le RIAM, un projet plate-forme - Pascal - a été labellisé au 31 mars 2004. L'acronyme signifie « Procédé Assurant la Sécurité des Contenus par l'Adjonction de Leurres ». Il s'agit d'un dispositif destiné à protéger les diffuseurs de contenus numériques par un mécanisme « d'escamotage » puis de « recomposition » des données[74]. Auparavant, 5 projets précompétitifs avaient été labellisés au 31 mars 2003 : Content Tracker, Haut débit pour tous, Samp4, Procrédo et Cosin. L'ensemble de ces projets est relatif à la gestion des droits, la protection ou le marquage des contenus.

Comme l'indiquait Marc Herubel[75] lors d'une réunion de travail, le problème principal pour le RIAM est celui de la confiance du fournisseur envers son client et les usages que celui-ci fait des contenus.

RMNT :

Il n'entre pas dans la vocation du RMNT de labelliser des projets sécurité et confiance à proprement parler. Cependant, bien des projets sont liés à l'amélioration de la carte à puce, alors que d'autres – comme ceux relatifs au RFID – sont susceptibles de faire surgir de façon incidente la question de la confiance, ou plutôt de la défiance, du public.

[74] Le mécanisme est clairement expliqué sur : http://www.riam.org/Download/Pascal.pdf

[75] http://www.fing.org/confiance/IMG/pdf/FING_Confiance_CR2601_040128.pdf

### 3.2.3. Les projets Oppidum

Oppidum[76] fait partie du dispositif PROGSI (Programme société de l'information) de la DiGITIP (Direction générale de l'industrie, des technologies de l'information et des postes) au sein du ministère de l'Economie, des Finances et de l'Industrie.

Oppidum s'adresse à des projets de recherche et de développement dans le domaine de la sécurité des systèmes d'information, avec pour objectif de soutenir la dynamique industrielle de ce secteur et de proposer des outils de la confiance pour le développement de la société de l'information.

- Oppidum 2001 et Oppidum 2002

Les deux premiers appels à projets Oppidum se sont déroulés dans un contexte précis : la libéralisation de la cryptologie, la définition du cadre juridique de la signature électronique et, plus généralement, l'essor des besoins en matière de sécurité. Parmi les domaines concernés figuraient la gestion des clés, les systèmes VPN, les services Web, les cartes signeuses, la signature électronique par téléphone mobile, la gestion numérique des brevets, les lecteurs personnels pour le paiement par carte, les méthodes formelles, les pare-feu, les réseaux de neurones.

L'un des projets labellisé par Oppidum – FIDES – pilotée par La Poste portait sur « *le développement d'un système de cachet électronique faisant foi et de service postal électronique fondé sur l'utilisation de la signature électronique et l'horodatage* ». Aujourd'hui le service qui en a découlé est commercialisé comme « la lettre recommandée électronique » de La Poste.

- Oppidum 2004

Lancé au premier semestre 2004, l'appel à projets 2004 portait sur les thèmes prioritaires suivant :

- Produits pour la sécurisation des réseaux privatifs (sécurité périmétrique, systèmes de chiffrement, systèmes d'administration, etc.) ;
- Produits pour la protection du poste individuel et des postes nomades (pare-feu, réseau privé virtuel client, sécurisation du Wifi, authentification unifiée, systèmes de chiffrement, etc.) ;
- Produits et services pour la protection des mineurs et de la vie privée (recherche et analyse de contenus, filtrage de la navigation et des spams) ;
- Produits pour la signature et l'identification (dans le contexte de la mise en place du cadre juridique pour la dématérialisation des processus, contrôle d'accès logique, modèles d'utilisation de la biométrie) ;
- Produits et services pour la sécurisation des transactions et des paiements (micro-paiement notamment).

[76] http://www.telecom.gouv.fr/oppidum/

L'accent était mis en particulier sur l'association des utilisateurs en amont pour orienter les travaux et en aval pour en valider la pertinence. La biométrie, peu présente dans les précédents Oppidum, devrait selon toute vraisemblance occuper une place plus importante au sein des projets qui seront labellisés, voire financés.

En novembre 2003, lors de l'appel à manifestation d'intérêt, un découpage thématique différent était envisagé puisqu'il recouvrait les trois dimensions suivantes :

- L'identité numérique
- Les systèmes de transactions électroniques sécurisés, notamment pour le paiement
- La sécurité informatique et des réseaux

### 3.2.4. Les autres projets confiance et sécurité

D'autres organismes que ceux cités dans les paragraphes précédents contribuent aux projets d'innovation dans le domaine de la sécurité et de la confiance. C'est notamment l'une des missions, peu connue, de la DCSSI[77] (Direction Centrale de la Sécurité des Systèmes d'Information). Elle dispose de trois laboratoires en charge de l'expertise scientifique et technique, en liaison avec ce qui se fait dans le cadre académique. Les domaines couverts sont la cryptographie, les signaux compromettants et l'assistance technique à la cryptographie.

La Délégation Générale pour l'Armement (DGA), déjà citée à propos de l'ACI « Sécurité informatique » investit dans la recherche[78]. Il s'agit notamment d'« *évaluer les opportunités et les dangers que représente pour la Défense l'émergence de nouvelles technologies* ».

## *3.3. Quelques tendances de la R&D confiance et sécurité au niveau international*

En complément de la cartographie des projets nationaux et communautaires, il semblait intéressant de disposer d'éléments d'informations sur quelques projets de R&D *trust & security* menés en Amérique du Nord, en Asie voire dans d'autres pays européens en dehors des projets communautaires.

Une mission de veille a été confié, entre décembre 2003 à février 2004 à deux étudiants - Sofiane Saadi et Fernando Pensado – du MISTE[79] (Mastère Spécialisé en Intelligence Scientifique Technique et Economique) de l'ESIEE ((École Supérieure

[77] http://www.fing.org/confiance/IMG/pdf/DCSSI_FING-28-06-04.pdf

[78] http://www.defense.gouv.fr/dga/fr/les_metiers/preparer_defense/developper_technologies/effort_recherche/index.html

[79] http://www.esiee.fr/masteres/miste/index.html

d'Ingénieurs en Électronique et Électrotechnique) sous la direction de Francis Moaty et de Patrice Santi.

Ce travail, qui ne prétend nullement à l'exhaustivité, a permis d'obtenir un indicateur de visibilité ou de communication sur les projets de R&D[80].

Ce travail a permis d'obtenir un indicateur de visibilité ou de communication sur les projets de R&D et non un reflet fidèle de la situation, mais les enseignements en sont tout de même intéressants.

Deux domaines pour lesquelles les initiatives sont nombreuses ressortent. Il s'agit de cryptographie quantique et de la biométrie. Un troisième domaine, les systèmes à base de réputation, a fait l'objet d'une veille approfondie car il produit des contenus fréquents alors qu'il semble, pour l'instant, peu présent dans les programmes français et communautaires.

### 3.3.1. La cryptographie quantique

Les principales ressources identifiées au terme du travail de veille dans le domaine de la cryptographie quantique sont les suivantes :

- L'*Imperial College* de Londres, le *Department of Physics* (DP) de l'université de Cambridge et le Toshiba Research Laboratory, pilote du projet, collaborent sur le programme « *Quantum light emitting diode for secure communications (Q-LED)* ». L'initiative est soutenue par le *Department of Trade and Industry* (DTI).
  http://www.osda.org.uk/projects/QLED.html
  http://www.toshiba.co.jp/about/press/2003_06/pr0501.htm

- Le Group of Applied Physics de l'université de Genève et trois entreprises genevoises (ID Quantique, WISeKey, OISTE) coopèrent pour la mise au point d'une infrastructure à clé quantique
  www.wisekey.com/download/7%20Press%20Release/ID%20Quantique%20Fr%20France.pdf
  http://www.gapoptique.unige.ch/Projects/Quantum/LookUp.asp?Group=2

- MagiQ Tehnologies, qui se présente comme l'une des premières entreprises commercialisant des solutions de sécurité basées sur la cryptographie quantique, le Department of Electrical & Computer Engineering et le Department of Physics de l'université de Toronto sont partenaires sur le projet « *Quantum information & Computation* »

[80] Compte tenu de la durée limitée de la mission et de la complexité du sujet, il ne s'agissait pas de produire un véritable mémoire sur l'état de la R&D « *Trust & Security* » dans le monde mais d'identifier les thèmes et les pôles les plus visibles sur Internet lorsqu'on effectue une requête sur les moteurs de recherche avec les mots clés suivants : *Privacy, Security, Trust Network, Trustworthy Computing, Trustworthy Networking, Safety, confidence, Confidence-Building Technologies, Network and Information Security, Technologies for Trust and Security, Biometrics, Cryptography, Electronic Signature, Trust Management, Trust in the cyberspace,Rreputation-based systems, Electronic seal.*

www.magiqtech.com/research/index.php

.

- University of Cambridge dispose de son *Centre for Quantum Computation*.
  http://cam.qubit.org

- Au sein du *Los Alamos National Laboratory*, des travaux sont menés par *The Quantum Institute*
  http://quantum.lanl.gov .

- Une approche de même nature est constatée au sein de l'University of Waterloo (Canada) avec l'IQC (*Institute for Quantum Computing*)
  http://www.iqc.ca/

- Au Japon, l'Université de Tokyo (département d'informatique), NEC , ERATO (*Exploratory Research for Advanced Technology*) et la *Japan Science and Technology Agency* (JST) conduisent le Quantum Computation and Information Project.
  http://www.qci.jst.go.jp/index.html.en

- Encore un acteur japonais mais cette fois-ci il s'agit d'une entreprise : le Projet MISTY de Mitsubishi Electric
  http://global.mitsubishielectric.com/info/telecom2003/showcase/encryption/part5/03.html

- Enfin, la SSF(*Swedish Foundation for Strategic Research)*, KTH (*Royal Institute of Technology*) et le *Laboratory of Optics, Photonics and Quantum electronics* mènent des travaux de recherche en technologie quantique.
  http://www.imit.kth.se
  http://www.stratresearch.se/eindex.html
  http://www.kth.se/eng .

### 3.3.2. La biométrie

Les ressources en matière de biométrie sont nombreuses et elles dépassent l'univers des laboratoires de recherche car le domaine est plus ancien que celui de la cryptologie quantique. Pour donner un aperçu de la variété des approches, ont été retenus deux sites américains qui font office de centres de ressources, un site chinois ainsi qu'un site allemand abordant les aspects sociétaux du domaine :

- Oeuvre du Département de biométrie de la *Michigan State University* ou de *The Biometric Consortium*, deux sites en anglais donnent accès à de nombreuses sources relatives aux différents aspects de la biométrie
  http://www.biometrics.org/html/research.html
  http://biometrics.cse.msu.edu

- The Institute of Automation de la Chinese Academy of Sciences mène au sein du CBAT (Centre for Biometric Authentication & Testing) diverses activités de recherche en biométrie.
  http://www.sinobiometrics.com/pdf/xuchenghua.pdf

- Au sein de TeleTrust, une organisation non gouvernementale allemande, le groupe BioTrust se consacre à l'acceptation par les utilisateurs des dispositifs de sécurité fondés sur la biométrie
  http://www.teletrust.de/default.asp?sw=3&Sprache=E_&HomePG=0
  http://biotrust.de

### 3.3.3. Les systèmes à base de réputation

Un ensemble de pôles de recherche aux Etats Unis travaillent sur le concept de *Reputation-Based Trust* alors que ce type de travaux semblent moins présents en Europe et a fortiori en France. Il est notamment possible de citer les projets suivants :

- Le *Reputation-Based Trust Management* est un sujet développé par Vitaly Shmatikov et Carolyn Talcott du Computer Science Laboratory (CSL)
  www.csl.sri.com/
  http://www.csl.sri.com/users/shmat/shmat_rtm.pdf

- *The Reputation Research Network* de l'Université du Michigan propose une page destinée aux chercheurs du domaine
  http://databases.si.umich.edu/reputations

- Le *College of Computing* de Georgie et le *Georgia Institute of Technology* oeuvrent conjointement sur un modèle de confiance fondé sur la réputation destiné aux communautés de commerce électronique en P2P (« *A Reputation-Based Trust Model for Peer-to-Peer eCommerce Communities* »).
  http://disl.cc.gatech.edu/PeerTrust/pub/xiong03reputation_abstract.pdf

- Au Japon également où le Systems Development Laboratory d'Hitachi et Kawasaki coopèrent sur une méthode de filtrage basée sur les réseaux de confiance pour récupérer des informations de confiance à partir des rumeurs.
  http://www.vs.inf.ethz.ch/events/ubicomp2003sec/papers/secubi03_p05.pdf

- Tout de même une source européenne sur le sujet avec le projet *Reputation-based System for P2P Networks* du Security Group de l'Université de Milan : P2Prep.
  http://seclab.dti.unimi.it/p2prep

.

# 4. Identification des nouvelles pistes pour la recherche et l'innovation

Les travaux de R&D et les projets d'innovation sont nombreux. Les chapitres précédents de ce document, sans prétention à l'exhaustivité, en procurent un aperçu. Dès lors, il peut être risqué, voire présomptueux, de proposer de nouvelles pistes pour la recherche. C'est pourtant ce que l'on se proposera de faire en s'appuyant sur les travaux menés pendant cinq mois par le groupe de travail « confiance et sécurité sur les réseaux » de la Fing.

Il a paru naturel aux auteurs, par tempérament, de formuler des propositions s'inscrivant dans une approche qui consisterait à couvrir de nouveaux champs ou à combler des points faibles relatifs de la R&D nationale. Une autre politique de R&D fondée sur le renforcement des points forts pourrait être tout aussi légitime.

Les propositions n'engagent que les auteurs de ce document. Elles ne reflètent pas la position du ministère de la Recherche, du ministère de l'industrie ou des réseaux de recherche. Elles ont naturellement vocation à être commentées, complétées, critiquées ou réfutées.

## *4.1. Promouvoir les nouvelles approches*

### 4.1.1. Les approches multimodales

Les approches multimodales semblent caractériser bien des travaux de recherche particulièrement novateurs. C'est notamment le cas de la biométrie multimodale[81] ou, dans le domaine des télécommunications, du projet Emily[82] qui associe la localisation terrestre et satellitaire.

Cette tendance pourrait être reprise dans d'autres domaines. Par exemple :

- En associant cryptologie par algorithme et cryptologie quantique (ou par chaos) ;

- En associant l'identification/authentification par carte et l'identification/authentification par méthode statistique (score et bases fraudes). La carte bancaire pour laquelle les deux approches coexistent sans être semble-t-il intégrées pourrait constituer un terrain d'application prioritaire.

[81] http://www.fing.org/confiance/IMG/pdf/FING_30032004_MmeDorizzi_INT-Evry_Biometrie.pdf

[82] http://www.fing.org/confiance/IMG/pdf/Fing.org_27042004-_Bouygues_Tel_-_Geolocalisation_en_securite_et_confiance.pdf - pages 13 et 14

### 4.1.2. Les coopérations entre technologies et sciences sociales

La coopération entre les « sciences dures » et les « sciences molles » est déjà une réalité comme en témoigne la publication commune de Michel Riguidel (Enst) et Dominique Boullier (UTC) en 2004 dans « Les Cahiers du Numérique ». C'est aussi une démarche déjà engagée par IDEAs Lab à Grenoble. Elle mériterait d'être approfondie.

L'apport des sciences sociales peut être précieux quand il s'agit d'identifier les véritables attentes du public, au-delà des fausses évidences. Comme le souligne Laurent Gille, ENST, la sécurité peut-être souvent un alibi stratégique utilisé par les individus : on dit « je n'ai pas confiance » ou « la sécurité n'est pas suffisante » alors qu'on pense « cela ne m'intéresse pas ».

Dans des domaines comme le RFID ou la biométrie, le comportement des consommateurs, l'acceptabilité individuelle ou sociale pourraient être intégrés dès le départ comme un des indicateurs de performance de la solution développée.

### 4.1.3. Passer d'une approche discipline à une approche centrée sur les thématiques

Il serait certainement stimulant d'abandonner parfois la démarche projet centrée sur une discipline ou un univers technologique (carte à mémoire, biométrie, certificats numériques, etc.) pour faire prévaloir une démarche centrée sur une thématique transversale comme, par exemple, celle de l'usurpation d'identité en ligne.

### 4.1.4. Approfondir les démarches de types « résilience »

Ce domaine concerne plus particulièrement la sécurité des réseaux, leurs comportements face aux défaillances et aux attaques. Ces technologies représentent une manière de réfléchir autrement à la confiance dans un système. Il s'agit de la confiance dans le fait de ne pas tout perdre quand il y a eu compromission. L'objectif n'est plus d'élever des barrières technologiques, mais de prévoir des méthodes pour restaurer un état sain, aussi proche que possible du premier état compromis. Cette méthode se distingue des approches plus classiques dans la mesure où on accepte l'idée qu'il y aura des problèmes. C'est la méthode du roseau en matière de confiance et de sécurité, et non celle du chêne. La sagesse du fabuliste nous apprend que ce n'est pas forcément la moins efficace.

## *4.2. Investir sur les domaines émergents*

### 4.2.1. Les plates-formes de confiance

Dans le domaine des plates-formes de confiance[83], (ou TPM pour *Trusted Platform Module*) la France semble aujourd'hui spectatrice alors que les questions posées sont fondamentales : s'agit-il d'une approche qui s'oppose à celle de la signature électronique, à la carte à mémoire ? S'agit-il pour reprendre la formule tonique de Michel Riguidel « *d'un putsch sur la sécurité, réalisé dans l'obscurité* ». Dans quelle mesure, les plates-formes de confiance, comme l'évoquent Yann Le Hegarat (Cnil) ou Yves Deswarte (LASS-CNRS) pourraient être considérées comme des technologies de protection de la vie privée ?

Des travaux de recherche pourraient être encouragés pour explorer la possibilité de créer une plate-forme de confiance intégrant dès la conception les valeurs du droit européen.

### 4.2.2. Les dispositifs de confiance, la mobilité et l'intelligence ambiante

Le domaine de la mobilité a été souvent cité par les intervenants du groupe de travail comme devant être une des priorités de la recherche en matière de confiance. Michel Riguidel indique qu'il faut faire évoluer les critères communs[84] pour prendre en compte la dimension mobilité.

Pour Yves Deswarte, c'est notamment dans le domaine de la localisation qu'il conviendrait de développer résolument des technologies de protection de la vie privée. La Cnil incite la recherche à se pencher sur les dispositifs permettant de désactiver les étiquettes RFID et de le prouver. François Vacherand, Cea Leti envisage des dispositifs d'effacement partiel permettant par exemple de conserver l'information sur le modèle en supprimant le numéro de série, voire à des dispositifs permettant à une personne de manifester son accord pour être tracée, avec la possibilité de changer d'avis à tout moment.

Dans un registre proche, des travaux pourraient être encouragés dans le domaine, peu exploré par le groupe de travail, de l'intelligence ambiante : machine to machine, réseaux ad hoc sans point central, reconfiguration continue...

### 4.2.3. La protection des contenus numériques (DRM, etc.)

La protection des contenus numériques, la lutte contre la contrefaçon numérique via les technologies de type DRM (*Digital Right Management*) représentent une priorité

[83] http://www.fing.org/confiance/IMG/pdf/FING_30032004_MrLe_Hegarat_CNIL_Identification_par_la_machine.pdf

[84] Les « Critères Communs d'Evaluation relatifs à la Sécurité des Systèmes d'Information » représentent le résultat d'une série d'efforts menés pour développer des éléments d'appréciations reconnus par la communauté internationale. Ils ont vocation à être le mètre-étalon de la Sécurité des Systèmes d'Information.

pour la recherche comme l'a rappelé[85] le Ministre de la recherche, François d'Aubert, le 1er juillet 2004, à l'occasion des États généraux européens du nommage et de l'adressage sur Internet (EGENI) : « (…) *je souhaite qu'au sein de nos réseaux de recherche et d'innovation technologique, nous mettions l'accent sur les projets dans le domaine à la fois de la lutte contre la contrefaçon numérique mais aussi et surtout de l'aide à la diffusion numérique de contenus légaux* ».

Sur ce thème propre à alimenter controverses et polémiques, il semblerait possible d'explorer de nouvelles approches du DRM qui soient centrées sur l'individu ou le foyer et non sur l'œuvre ou le terminal de lecture. « Je prouve que je suis moi et je peux donc ainsi accéder librement à un contenu, dans le respect de la propriété intellectuelle, partout, depuis n'importe quel terminal ». Le projet SmartRight (Thomson), soutenu par le RIAM, va dans ce sens.

### 4.2.4. Les modèles de confiance pour le P2P

La recherche française semble insuffisamment présente dans le domaine des systèmes à base de réputation (ou *Reputation Based Trust Model).* Or, il semble que ce type de solutions est particulièrement adapté au commerce électronique en P2P qui est l'un des secteurs les plus dynamiques de l'économie numérique.

### 4.2.5. Le modèle d'informatique « centrée autour de l'identité » (identity-centric computing)

L'*identity-centric computing*[86] se présente comme une forme de synthèse de différentes approches évoquées dans les paragraphes qui précèdent, un « nouveau paradigme » de l'informatique décentralisée, mobile et sûre. Il organise l'accès aux informations et aux applications autour d'une gestion des droits. Personnes, appareils, informations et applications disposent d'identités qu'ils transportent sur eux, auxquelles s'attachent des règles, des droits et différents « référents » (sources des droits, certificats...) L'interaction entre les uns et les autres passe par un langage commun (« interchange ») et des protocoles (techniques, mais aussi commerciaux et juridiques.) Même s'il est parfois difficile de faire la part des choses entre les réelles innovations et les discours marketing, c'est un domaine qui ne semble aujourd'hui abordé en tant que tel par le monde de la recherche en France.

## *4.3. Découpler les domaines confiance et sécurité*

Les réflexions du groupe de travail ont permis de mettre en évidence les liens ambigus entre confiance et sécurité. Dans bien des cas, le développement des systèmes de sécurité peut conduire à un effritement de la confiance. La contrainte

[85] http://www.recherche.gouv.fr/discours/2004/degeni.htm

[86] Voir par exemple les analyses de Digital ID World : http://www.digitalidworld.com/

que fait peser les systèmes de sécurité, leur manque de transparence, le manque de maîtrise de la part des utilisateurs, soulève rapidement une méfiance « systémique ».

Plaider, dans une optique recherche, en faveur d'un découplement des notions de confiance et de sécurité, n'invalide en rien les pistes explorées par les techniciens de la sécurité, mais cela montre qu'il faut en explorer d'autres, à la fois parce que les recherches actuelles ne couvrent pas tout le champ de la confiance et parce que ces recherches peuvent avoir des impacts positifs sur la sécurité et négatifs sur la confiance.

### 4.3.1. Adoption et simplicité : au-delà de la technologie

Des projets uniquement dédié à la dimension confiance devraient se focaliser sur a question de l'adoption (ou de la non-adoption) depuis l'individu jusqu'à la collectivité. Parmi les approches envisageables figure la modélisation économétrique ex-ante (voire ex post, pour en comprendre les déterminants avant de pouvoir les prédire) des conditions de la diffusion et de l'adoption des technologies de sécurité. Ce serait, sur le mode prédictif, un travail de même nature que celui effectué par David Bounie[87] (ENST) à propos de CyberComm.

La question de la confiance recouvre largement celle des usages ; elle renvoie donc à la problématique de la simplicité. Comment l'utilisateur peut-il éviter de gérer sans cesse les dispositifs de sécurité et de confiance, sans pour autant abdiquer en faveur des paramètres par défaut, son contrôle sur le niveau de protection de son patrimoine numérique ? Cela semble, à l'évidence, un champ prometteur pour des projets de recherche.

### 4.3.2. Des dispositifs de confiance pour invalider des systèmes de sécurité

Dans l'optique confiance, pratiquement opposée ici à la sécurité, les dispositifs permettant de masquer son identité, de mentir sur sa localisation, de refuser par défaut la collecte de certaines informations, deviennent un domaine de recherche important. Il s'agirait de permettre à des individus, ou à des collectivités, d'invalider certains systèmes de sécurité, mentionnés dans ce document, dans les cas où ils seraient concernés.

On imagine non seulement le client qui refuse la fonction d'identification utilisé par un marchand en ligne mais aussi l'Etat qui désactive, dans sa sphère d'influence, les plates-formes de confiance élaborées à l'étranger.

L'une des applications concernerait l'authentification sans identification ou la pseudonymisation. Il semble que les travaux en France ne soient pas très nombreux dans ce domaine, parfois désigné aux Etats-Unis sous le vocable de *credential*. Les quelques expérimentations menées en la matière le sont principalement en Amérique

[87] http://www.fing.org/confiance/IMG/pdf/Bounie_Fing_Confiance_securite_250504.pdf

du Nord, par exemple par Stefan Brands[88], avec le plus souvent une vocation militante pour la défense de l'anonymat. Ces technologies ne seraient pas forcément conformes au droit national.

Yves Deswarte[89] indique que les *credentials* peuvent être créés sur la base des certificats X509 et il fait référence aux travaux déjà menés par Fabrice Boudot sur les certificats restreints. Il s'agit de cartes à mémoire volontairement limitées qui ne peuvent répondre que par « oui » ou « non ». La France a su développer des technologies grand public structurellement respectueuse de la vie privée, comme la télécarte des cabines téléphoniques, la Moneo Verte ou le Minitel, mais elles n'ont pas été promues, ni peut-être même pensées, comme telles.

La biométrie pourrait par exemple être envisagée comme un des moyens qui pourrait servir pour établir un lien fiable entre un certificat d'attributs sans identification et une personne physique.

Un autre domaine concernerait la confidentialité par rapport aux prestataires techniques ; prestataires de confiance ou qui devraient l'être. Avec les informations dont disposent sur leurs abonnés les Fournisseurs d'Accès Internet, il serait intéressant de mener des réflexions dans le domaine des dispositifs permettant d'assurer une confidentialité sur les usages, et pas uniquement sur les messages.

Ces dispositifs ne pouvant être, dans une optique de généralisation, des solutions d'anonymat absolu, ils devraient intégrer dès les étapes de R&D les mécanismes permettant de les neutraliser, par exemple sur demande d'un juge.

[88] http://www.ercim.org/publication/Ercim_News/enw49/brands.html

[89] http://www.fing.org/confiance/IMG/pdf/FING_30032004_MrDeswarte_LAAS-CNRS_Privacy.pdf - page 9

## Encadré : les préconisations d'un groupe de travail composé d'industriels

Un groupe de travail composé d'industriels et de représentants de la recherche publique, initié par le Ministère de la Recherche, a publié le 1er mars 2004 un document[90] intitulé « Quels axes de recherche pour la sécurité et la confiance dans les usages numériques ? ». Il a été réalisé par des représentants des sociétés EADS, Sagem, Cryptolog, Edsi et Edelweb.

Le nouveau contexte de la sécurité pose, selon les auteurs, la question du « *maintien de la souveraineté des Etats et de leur maîtrise des technologies en jeu, du maintien de la souveraineté des individus et de leur maîtrise des outils et de l'identité et de la signature* ».

Les nombreuses préconisations qui figurent dans le texte portent sur trois axes de recherche :

Mesure et Supervision d'un système sécurisé

Dans ce domaine trois axes principaux sont identifiés : l'évaluation du niveau de sécurité d'un système, la supervision qui recouvre les capteurs et sonde de sécurité, l'enregistrement des alertes et l'analyse des renseignement, et, enfin, l'administration et la gestion des modes opérationnels et de secours.

Les menaces et les vulnérabilités

Les industriels ne sont pas à l'abri d'une percée significative dans la conception des moyens d'attaque, notamment dans le domaine de la biométrie. La connaissance de ces moyens d'attaque est nécessaire pour concevoir les parades et les inclure dans les produits et systèmes. Outre la biométrie, l'analyse des menaces et vulnérabilités devrait également concerné la transmission radio, les protocoles et API de ressources cryptographique, la cryptanalyse, etc

La plate-forme sécurisée constitue le troisième axe de recherche préconisé. La plate-forme sécurisée complète de toute la chaîne allant des utilisateurs aux composants en passant par les applications. Les efforts de recherche devrait porter sur la sécurisation des interactions avec l'utilisateur, la sécurisation du système d'exploitation et la sécurisation des applications elles-mêmes.

[90] http://www.fing.org/confiance/IMG/pdf/Min_Recherche_-_GT_Industriels_-_17-2-04.pdf