Etude d'impact : la signature électronique et les infrastructures à clé publique dans le contexte de l'identité numérique :

Quels usages pour les titres sécurisés émis par l'état dans le monde de l'économie numérique ?

Ce document a été réalisé avec le soutien de :

CAPGEMINI
Cabinet d'avocats Caprioli & Associés
La CDC
KEYNECTIS

Nous remercions chaleureusement toutes les personnes ayant participé à la réalisation de ce document, à savoir :

- M. Charles de Couessin, du Cabinet de conseil ID Partners , consultant pour AFNOR, Maîtres Eric Caprioli et Pascal Agosti du Cabinet d'avocats Caprioli & Associés, M. Jean-François Legendre AFNOR,

- Les co-auteurs,

- Tous les membres du comité de pilotage qui ont commenté et relu en détail le document,

- et les nombreuses personnalités[1] qui ont accepté d'être interviewées et sans qui le document n'aurait pu voir le jour.

[1] Nous remercions, entre autres, Mr Ravisé d'Altenor, qui nous a fourni des informations fort pertinentes sur les attentes des acteurs dans les domaines du crédit et de la banque.

- Table des matières :

Avant-propos :

Les co-auteurs du présent document sont :
AFNOR
CAPGEMINI
Le Cabinet d'avocats Caprioli & Associés
La CDC
KEYNECTIS

Les organismes suivants ont participé au comité de pilotage et ont fait part de leurs commentaires/ avis/ suggestions :
CAPGEMINI
Le Cabinet d'avocats Caprioli & Associés
La CDC
La DGME
KEYNECTIS
Le Ministère de l'Intérieur - ANTS

Les organismes suivants ont été interviewés dans le cadre de cette étude :
Argovie
Altenor
Aon
Cabinet d'avocats Caprioli & Associés
Caisse des Dépôts et Consignations
Cetelem
CFONB
Chambre des Notaires
CNAM
CNIL
Cofinoga
Cortal Consors
DGME
Dictao
FEVAD
Fianet
Forum des droits sur Internet
Gemalto
GIE CB
GIE Sesam Vitale
GIP DMP
Keynectis
LastMinute.com
Ministère de l'Intérieur, Agence Nationale des Titres Sécurisés
Natexis
Paypal
Sofinco

I - **Rappel du contexte, méthodologie et périmètre de l'étude**

1. Objectifs de l'étude

Une récente étude Gartner[2] livre des chiffres qui requièrent la plus grande prudence quant au succès de l'économie numérique : 30% des interrogés déclarent minimiser leurs achats en ligne pour des raisons liées à la sécurité des paiements, les trois quart d'entre eux se connectent moins et 14% avouent avoir cessé toute activité bancaire en ligne. Un constat négatif qui nécessite de conduire un état des lieux sur les relations entre économie numérique et identité. Doit-on s'identifier ou s'authentifier pour conduire une transaction en ligne ? Quels mécanismes sont mis en œuvre par ces deux modes de connexion[3] et comment répondent-ils à différentes attentes du marché ? Quelles transactions requièrent une signature et comment cette signature se distingue-t-elle de l'authentification ? Mais également, quels types de signatures sont attendus par les acteurs de l'économie en ligne ?

Notre étude se propose de **clarifier ces technologies, préciser pourquoi et comment elles sont mises en œuvre dans le contexte des programmes d'identité électronique conduits en France actuellement**. Il est rappelé que le port de la Carte Nationale d'Identité (CNI) ne constitue nullement une obligation[4] contrairement à la plupart des pays d'Europe[5].

L'étude se limite au potentiel de la future Carte Nationale d'Identité Electronique (CNIe), telle qu'elle est spécifiée par l'équipe en charge de sa mise en œuvre[6,] mais également à celui de la Carte Sesam Vitale[7] vu son usage attendu vis à vis de la sphère publique[8]. Dans la logique du Rapport Truche, et bien que le citoyen ait le libre choix de moyens lui permettant de prouver son origine, nous ne traiterons pas des multiples cartes de services, d'associations, de transports, etc. dont l'autorité de délivrance ne bénéficie pas de moyens suffisants pour garantir l'identité d'un possesseur de titre, même s'il porte son patronyme et sa photographie[9].

---

2 Cité par The Economist. Economist Intelligence Unit. Complying with rules for identity management. Dec 2006.

3 Le service d'authentification permet de garantir l'intégrité et l'origine du message des données authentifiées mais, contrairement au service de signature électronique, il ne signifie pas que l'émetteur manifeste son consentement sur le contenu du message des données. PRIS version 2.0 1° Juin 2005.

4 Bien qu'instauré en 1955, le port de la carte nationale d'identité (CNI) ne constitue nullement une obligation pour les citoyens français. Lorsqu'ils ont à justifier de leur identité, ils peuvent présenter tout document officiel portant leur photographie : passeport, même périmé depuis moins de deux ans, permis de conduire, carte d'invalidité, carte d'abonnement aux transports collectifs ou carte professionnelle par exemple.

5 Environ la moitié des pays de l'UE qui ont institué la carte d'identité ont rendu sa détention obligatoire.

6 Il s'agit aujourd'hui de l'Agence Nationale des Titres Sécurisés sous la responsabilité du Préfet Raphaël Bartolt (JO du 24 février 2007).

7 Loi n° 2004-810 du 13 août 2004 relative à l'assurance maladie et Article L161-31 du Code de la Sécurité Sociale.

8 « Les organismes d'assurance maladie délivrent une carte électronique individuelle inter-régimes à tout bénéficiaire de l'assurance maladie qui comporte une photographie de celui-ci. Cette carte est valable partout en France et tout au long de la vie de son titulaire….".

9 C'est par la possession d'un titre d'identité (carte d'identité ou passeport), délivré à travers une procédure codifiée, qu'un citoyen détient la preuve qu'il est bien le titulaire de son identité. En un

2- Identité électronique et économie numérique

Initié bien avant les évènements du 11 septembre 2001[10], le programme de « Protection de l'Identité »[11] du Ministère de l'Intérieur français a été décalé en raison du contexte électoral de 2007. Pourtant, les débats entretenus par la presse et les forums d'usagers[12] attestent d'une perception quasi liberticide par l'opinion, contrairement à son objectif premier visant à faciliter l'économie numérique. Bien que la France dispose d'un arsenal législatif qui préserve la vie privée, l'analyse des débats témoigne d'un amalgame entre des technologies répondant à des procédures et contextes juridiques bien différents : code PIN, biométrie, certificats et signature électronique, comme si elles étaient équivalentes et interchangeables.

Ainsi l'une des confusions majeures porte-t-elle sur les procédures d'identification et de conclusion de l'acte d'achat, deux actions pourtant bien différentes ; l'un des opposants au projet demandant: «*Pourquoi une "identification certifiée" (…) pour une transaction électronique privée ? En somme, si le commerce repose depuis l'antiquité sur la confiance, le commerce électronique devrait-il reposer sur l'authentification forte et les mesures biométriques ?*»[13]. Pourtant la dématérialisation des moyens de règlement – chèques, cartes de crédit - fait depuis longtemps appel à des mécanismes puissants de confirmation d'identité et de solvabilité[14] et ne se satisfait plus des rapports de confiance traditionnels à l'économie marchande. Bien que la VPC, relayée par le Minitel, ait largement ouvert la voie au commerce électronique en dématérialisant tout à la fois le rapport entre les parties, la relation aux biens vendus et les moyens de paiement, l'actuel essor de l'économie numérique nécessite que des règles fiables soient instaurées pour faire face aux menaces de fraude. Rappelons que l'impulsion sur la signature électronique est venue de la Commission des Nations Unies pour le Droit Commercial International (CNUDCI) ; la loi type sur le commerce électronique ayant été adoptée sur 16 Décembre 1996 par l'Assemblée Générale, bien avant la parution de la Directive Européenne (Décembre 1999)[15].

Il s'agit donc de restaurer la confiance nécessaire aux relations marchandes, qui ne peuvent plus reposer sur l'appréciation mutuelle des parties mais sur les technologies de

---

sens, c'est la délivrance du titre d'identité qui « fixe » l'identité. Avant la délivrance du titre, un enfant, par exemple, est doté d'une forme embryonnaire d'identité, son inscription sur le registre d'état civil (dont il peut obtenir copie sous la forme d'un extrait de naissance), son inscription dans le livret de famille ou sur le passeport des parents. Rapport Truche Administration électronique et protection des données personnelles. Paris 2002. Rappelons qu'aujourd'hui les enfants mineurs doivent détenir leurs propres passeports et que leur inscription dans le passeport des parents n'est plus suffisante pour quitter le territoire français.

[10] Il a été initié sous le label de « Titre Fondateur » par le Ministre de l'Intérieur Daniel Vaillant en 2000.

[11] Il s'agit du nouveau nom du programme d'identité électronique, précédemment intitulé INES.

[12] Forum des droits sur l'internet. 16 juin 2005. Rapport Projet de carte nationale d'identité électronique.

[13] « Quel besoin d'une identification forte pour les télé-procédures ? D'autant que l'anonymat de l'agent public correspondant pourrait, lui, être respecté, "si des motifs intéressant la sécurité publique ou la sécurité des personnes le justifient" (art. 4 de la loi n°2000-321 du 12 avril 2000 relative aux droits des citoyens dans leurs relations avec les administrations). » Intervention du 7 mars 2005. Le Forum des droits sur Internet. Rapport sur le Projet de carte nationale d'identité électronique 16 juin 2005.

[14] A titre d'exemple, le réseau des cartes de paiement certifie – quasiment en temps réel - la solvabilité de l'acheteur mais également sa possession légitime du titre par la génération du PIN code.

[15] Directive 1999/93/CE du Parlement européen et du Conseil, du 13 décembre 1999, sur un cadre communautaire pour les signatures électroniques.

l'information dans un cadre réglementaire défini. C'est précisément l'objectif de la Carte Européenne de Citoyen[16], initié par le Ministère de l'Intérieur français en 2002, qui vise la mise en œuvre d'une infrastructure numérique solide et l'interopérabilité des systèmes d'authentification lors du passage à l'Euro bien plus qu'un contrôle identitaire sur la toile. La Commission européenne a également subventionné de nombreux travaux visant les procédures d'identification, d'authentification et de signatures par les financements des 5° et 6° et actuel 7° PCRD[17]. Les initiatives visant l'identité et le contrôle aux frontières ne sont apparues que tardivement et dans l'urgence des évènements du 11 septembre 2001, vu la réplique américaine du Patriot Act[18] . Mais les financements tardifs du PASR[19] de la Commission, visant à combattre le terrorisme - environ 25 Millions par an entre 2004 et 2006 - paraissent dérisoires comparés aux milliards alloués à l'économie numérique dans le cadre du programme IST (Information Society) de Bruxelles.

D'abord intitulé «Titre fondateur», **le programme d'identité électronique français ambitionne la mise en service d'une carte de nationalité spécifique, qui se distingue des cartes sectorielles** par les points suivants : délivrance par l'Etat mais surtout avec un **objectif « d'identification générale et non des usages spécifiques, comme le permis de conduire ou le passeport »[20]**. Comme le rappelait le Rapport Truche, les mécanismes inhérents aux certificats électroniques constituent une véritable mine de renseignement si, à l'avenir, les fichiers devaient être croisés par les détenteurs des traces[21]. Aussi met-il l'Etat en garde que la future CNIe ne remplace à l'avenir le numéro INSEE[22] ou NIR[23].

---

16 CEN/TC 224 - Identification personnelle, signature électronique et cartes lisibles par machine, dispositifs d'interface associés et fonctionnement.

17 Programme Cadre de Recherche et Développement : eJustice Towards a global security and visibility framework for Justice in Europe (eJustice) March 2004 to February 2006 http://www.ejustice.eu.com/, Porvoo Group http://www.porvoo10.net/p10/, eEPOCH http://www.eepoch.net/ : to develop and provide a practical demonstration of interoperable and secure smart card based digital identification system in 7 pilot sites over Europe (eEurope Proof of Concept for a Holistic approach).

18 http://www.epic.org/privacy/terrorism/hr3162.html 24 octobre 2001.

19 Preparatory Action in the field of Security Research.
http://www.eurosfaire.prd.fr/news/EEppZpVAVEgypGwnqw.html

20 La carte d'identité se distingue des autres pièces d'identité par la réunion de trois conditions :
– elle est délivrée par l'État ;
– elle vise des fins d'identification générale et non des usages spécifiques (comme le permis de conduire ou le passeport) ;
– elle contient des renseignements qui en font, en comparaison des autres pièces d'identité, un document privilégié pour identifier les personnes. Rapport Truche- Administration électronique et protection des données personnelles. Paris 2002.

21 « Les risques et les perceptions en matière de vie privée se sont déplacés de la constitution de «grands fichiers » vers la problématique de la gestion des « traces » que l'on laisse dans les systèmes que l'on utilise ; Les risques et les perceptions en matière de vie privée se sont déplacés des fichiers publics, principaux créateurs et gestionnaires de fichiers, vers les opérateurs privés, spécialistes de marketing et de gestion « optimisée » (du point de vue de l'entreprise) de la relation client ». Administration électronique et protection des données personnelles. Rapport Truche-Synthèse Paris 2002.

22 A l'origine, le NIR a été créé dans un but militaire : René Carmille, qui travaillait pour le gouvernement de Vichy pendant la seconde guerre mondiale, a eu la mission de préparer secrètement la mobilisation d'une armée française. Dans un but de camouflage, il créa un Service National de Statistiques et répertoria toutes la population française (femmes enfants et vieillards compris) à partir des registres de naissance de l'Etat Civil. Pour faciliter le tri des mobilisables, il créa un numéro dont les trois premiers chiffres permettaient de les repérer : le sexe et l'année de naissance pour en déduire l'âge. Ce répertoire fut créé d'avril à août 1941. René Carmille est mort déporté en janvier 1945 à Dachau ;

Dans ce contexte sensible, notre étude se propose de **clarifier le rôle de l'identité vis-à-vis de télé-procédures qu'il s'agisse de la sphère publique ou privée**, considérant que des actions aussi variées que signer sa déclaration de revenus, consulter un compte bancaire, ouvrir une DUE[24], acheter un DVD sur eBay, contracter un prêt ou encore souscrire une assurance-vie, ne relèvent pas du même contexte réglementaire.

Chaque application appelle un flux spécifique de données – identification, authentification ou signature – qui dépend du niveau de confidentialité des informations proposées sur le web, mais surtout du cadre juridique, sachant qu'un même titre d'identité peut contenir plusieurs catégories de certificats, publics ou privés. On pourra ainsi lever l'ambiguïté d'une carte « signeuse » [25] généralisée, dénoncée par les internautes ; la signature n'étant requise qu'exceptionnellement et seulement si le contexte réglementaire l'exige.

Comme le remarquait fort pertinemment le Rapport **Truche,** « **Le concept même d'identité numérique n'est pas, et pas plus que l'identité « traditionnelle » univoque et uniforme** : l'identité numérique se compose d'un ensemble d'identifiants partiels, finalisés, et des relations qu'entretiennent ces identifiants. L'essor de l'administration électronique, et plus largement de la société de l'information, multiplie et complexifie ces identités partielles et ces relations, sans pour autant conduire à les fusionner : cela pose la question de l'interopérabilité des identités numériques »[26]. La multiplicité des technologies disponibles pour accéder aux sites web, se connecter à son compte ou confirmer une transaction répond à cette variété d'identités, qui ne nécessite nullement l'usage d'une carte délivrée par l'Etat mais se satisfait des login / mots de passe traditionnels.

Notre travail porte donc sur les certificats liés aux programmes d'identité - CNIe, Carte Vitale – en se limitant à leurs usages vis-à-vis des sphères publiques ou privées : sites marchands, crédit à la consommation, banque de réseau et banque en ligne, actes juridiques, assurance maladie et services de l'Etat, essentiellement des relations B2C (Business to Consumers) vis-à-vis de personnes morales (publiques ou privées).
Sachant que nous ne disposons pas à ce jour d'éléments précis concernant la transposition dans le domaine de l'économie numérique des règles de fonctionnement d'actes sous seing privé[27]. Il ne semble pas qu'il y ait une demande ou un marché aujourd'hui en ce sens mais

---

[23] Le NIR (Numéro d'Inscription au Répertoire) est un numéro à treize caractères dont la composition est précisée dans l'article 4 du décret n° 82-103 du 22 janvier 1982 : "Le numéro attribué à chaque personne inscrite au répertoire comporte 13 chiffres. Ce numéro indique successivement et exclusivement le sexe (1 chiffre), l'année de naissance (2 chiffres), le mois de naissance (2 chiffres), et le lieu de naissance (5 chiffres ou caractères) de la personne concernée. Les trois chiffres suivants permettent de distinguer les personnes nées au même lieu, à la même période."

[24] DUE Déclaration Unique d'Embauche d'un employé.

[25] Daniel Kaplan, délégué général de la Fondation Internet Nouvelle Génération (FING)41 estime également que le développement d'une carte « signeuse » est potentiellement dangereux. En effet, parce que la CNIe bénéficiera d'un statut officiel et qu'elle proposera un dispositif très fort d'authentification, elle risque d'inciter un grand nombre d'acteurs à se reposer sur elle pour leurs relations avec des tiers (clients, fournisseurs…) même si ce niveau d'authentification n'est pas nécessaire. D'une manière générale, la plupart des intervenants ont souhaité une variabilité de l'authentification en fonction de l'usage (Le Forum des droits sur Internet. Rapport. Projet de carte nationale d'identité électronique 16 juin 2005).

[26] Rapport Truche- Administration électronique et protection des données personnelles. Synthèse Paris 2002.

[27] C'est un acte conclu sans le concours d'un officier ministériel, notaire ou huissier, rédigé et signé directement par les parties à l'acte, ou avec le concours d'un rédacteur d'acte. Un acte sous seing privé n'a de date certaine que s'il est enregistré (auprès de n'importe quelle recette des impôts)

si elle devait être formulée, il serait nécessaire d'en clarifier la démarche juridique et technique.

Tout au contraire, il est essentiel de **ne pas négliger l'usage potentiel des certificats de CNIe dans des contextes professionnels**. Rappelons que sur trois millions d'entreprises françaises, plus de deux millions sont mono-personnelles ou ne comptent qu'un seul employé ; 90% d'entre elles ne dépassant pas les dix salariés.
Vu leur haut niveau de qualification[28], ces certificats pourraient **être idéalement utilisés dans le cadre de formalités administratives** telles que : signature de mandataires sociaux, réponses aux appels d'offres ou TéléTVA[29], à l'égal des certificats d'entreprise[30]. Les formalités des sociétés unipersonnelles et PME sont ainsi susceptibles de constituer un formidable « produit d'appel » pour la future CNIe.
Pareillement, on ne peut exclure que ces certificats puissent être utilisés par de grandes entreprises dans le **cadre de délégation de pouvoirs**, grâce à des outils de workflow ou de paraphe électronique. Dans ce contexte, l'individu signe soit sur la base du certificat de l'Etat, soit au moyen de certificats professionnels, qui pourraient être hébergés par la CNIe, si cette hypothèse est retenue par le Ministère de l'Intérieur.

Sans prétendre à l'exhaustivité, notre étude propose une **photographie de l'écosystème numérique français à l'horizon 2007 vis-à-vis de l'identité en ligne** ,sachant que le lancement prochain du programme d'identité électronique risque de bouleverser la donne.
Même si la littérature traitant du sujet est abondante, nous avons privilégié les entretiens dans la mesure où de nombreux projets se situent dans une phase de gestation et que les acteurs expriment fort clairement leurs attentes vis-à-vis de la future CNIe. D'ailleurs, ils mettent souvent en œuvre des solutions transitoires, propriétaires, mais qui préfigurent ses fonctions. Ils constituent un terreau idéal qui devrait permettre au Ministère de l'Intérieur (MI) d'affiner les fonctionnalités du programme préalablement à la consultation des entreprises, prévue pour 2008.

Partant des émetteurs – MI, CNAM –, l'étude se propose d'investiguer **un large spectre d'acteurs de l'économie numérique depuis l'achat d'un bien en ligne jusqu'à sa réception en précisant les demandes de tous les intervenants du circuit** : crédit, assurance emprunteur, débit bancaire ; sans oublier de vérifier la conformité des procédures par rapport au cadre réglementaire (CNIL, avocats, notaires). Cette approche très large permet de confronter les projets des fournisseurs d'identité aux attentes des prestataires.

Comme nous le verrons plus bas, **l'identité électronique ne doit nullement être considérée comme la transposition de règles de fonctionnement du monde physique** mais, grâce au saut technologique mis en œuvre, elle permet d'anticiper des gains de productivité importants et favorise l'apparition de nouveaux métiers d'intermédiation.

---

au contraire de l'acte authentique qui a l'avantage d'avoir une date certaine, et d'être conservé dans les archives de l'office ministériel sans limite de durée.

[28] PRIS***, Politique de Référencement Intersectorielle de Sécurité (PRIS). Agence pour le Développement de l'Administration Electronique. Premier Ministre 01/06/2005.

[29] TéléTVA s'adresse à l'ensemble des redevables de la TVA qui exercent à titre habituel une activité commerciale, industrielle, civile, agricole ou libérale, quel que soit le régime réel d'imposition à la TVA auquel ils sont soumis (réel normal et réel simplifié, périodicité mensuelle, trimestrielle ou saisonnière). Les redevables dont le chiffre d'affaires ou les recettes réalisés au titre de l'exercice précédent est supérieur à 760 000 € HT ont l'obligation, à compter du 1er janvier 2007, d'utiliser TéléTVA*.

[30] « Il y a par ailleurs une zone de recouvrement entre personnes physiques et personnes morales : un très grand nombre d'entreprises sont unipersonnelles ». Rapport Truche - Administration électronique et protection des données personnelles. Paris 2002.

Il est donc question ici d'une nouvelle chaîne de valeurs dont on décrit les intervenants et les enjeux financiers correspondants.
Par contre, nous nous **focaliserons sur les questions relatives à l'identité numérique** et n'aborderons pas d'autres sujets connexes tels que, par exemple, la "réputation numérique", le "droit à l'oubli sur les réseaux", etc.

II - Les attentes des acteurs et synthèse des entretiens

1- Programme de Protection de l'Identité. Ministère de l'Intérieur[31]

En date de l'étude, le MI a décidé de restreindre le périmètre du programme de la future carte d'identité électronique piloté par l'**ANTS**[32]. Les certificats d'authentification et de signature seront facultatifs mais fournis gratuitement aux ayant droits, lors de la remise du titre et activés par code PIN face à l'agent de mairie. Une procédure qui répond aux exigences des certificats qualifiés au sens de la Directive Européenne 1999/93 et conforme à la réglementation PRIS***[33].
Par contre, **l'Etat n'entend prendre aucune responsabilité quant à leur usage ultérieur**. Il ne serait plus question que la CNIe héberge des certificats privés, comme envisagé initialement. Non obligatoire, le titre a une validité de 5 ans comme les certificats[34].

Il semble que les prestataires de services en ligne n'aient pas encore perçu **le potentiel considérable de ces certificats pouvant générer des signatures juridiquement équivalentes à une signature manuscrite et distribués à l'échelle d'un pays.**
Un procédé qui renverse la charge de la preuve et confère donc aux millions d'internautes potentiels, une présomption de fiabilité lors de leurs transactions sur le net. Soucieux de favoriser la mise en œuvre de nouvelles télé-procédures (et pas uniquement vis-à-vis de la sphère publique), le Ministère de l'Intérieur est favorable à ce que des lecteurs de cartes USB soient largement distribués par les banques ou les mairies lors de la remise du titre[35]. Le coût de revient est évalué à moins de cinq Euros pour des volumes importants.
A chaque transaction « en ligne », l'usager sera authentifié (et donc pas seulement identifié) par son code « PIN » frappé sur le clavier du PC (et non sur un clavier dédié de type Cybercom).

Par cette approche « forte », le Ministère de l'Intérieur se positionne comme l'un des acteurs majeurs de l'identité en France. En effet, même si la CNIe ne devait pas être rendue obligatoire, elle s'inscrit dans une hiérarchie des titres qui ne sera pas la même dans le contexte de l'économe numérique et du monde physique.

La possibilité nouvellement offerte de s'authentifier et de signer des contrats sur le web aura naturellement tendance à requérir l'usage d'un média qui offre la garantie la plus étroite entre l'ayant droit et l'autorité régalienne de dévolution du titre de citoyenneté.
Comme le remarquait justement le rapport Truche, «C'est par la possession d'un titre d'identité qu'un citoyen détient la preuve qu'il est bien le titulaire de son identité ; (par contre) c'est la délivrance d'un titre qui fixe l'identité[36] ».

---

31 Le programme INES, d'Identité Nationale Electronique Sécurisé est devenu le Programme de Protection de l'Identité. Entretien avec Mr Fabrice Mattatia, Ingénieur en Chef Ministère de l'Intérieur, le 14 décembre 2006.

32 L'Agence Nationale des Titres Sécurisés sous l'autorité du Préfet Raphaël Bartolt (JO du 24 février 2007) est chargée de la conception, de la mise en œuvre et de la réalisation du programme.

33 Il est remis en main propre sur la base d'un face à face et stocké sur un support physique inaltérable.

34 La PRIS préconise une durée de validité de 3 ans pour les certificats *** alors que Ministère de l'Intérieur a prévu de l'étendre à 5 ans. Ce point sera précisé par l'équipe projet du programme d'identité électronique.

35 L'Etat n'exclut pas de s'impliquer fortement dans la phase de promotion du nouveau média.

36 Rapport Truche - Administration électronique et protection des données personnelles. Paris 2002, p.37.

La CNIL devra prochainement statuer sur la constitution d'une base biométrique centralisée permettant de vérifier l'unicité de l'identité des citoyens lors de la remise des titres. Par contre, la France exclut le recours à un numéro unique de citoyen, comme c'est le cas dans de nombreux pays de l'EU[37]. Toutefois l'authentification biométrique sera exclusivement réservée aux forces de police et gendarmerie sans qu'il soit possible d'y recourir dans le cadre des télé-procédures, qu'elles soient publiques ou privées. Seront stockées les images des empreintes digitales, et non les minuties, afin de garantir l'interopérabilité des lecteurs de police en Europe.
La France a donc opté pour une approche minimaliste de l'authentification biométrique, contrairement à d'autres pays de l'Union Européenne, qui l'ont autorisée pour des applications privées.

2- Programme SESAM Vitale, CNAM [38]

La CNAM et le GIE SESAM VITALE ont récemment débuté **une étude sur l'usage et les conditions de mise à jour de certificats électroniques dans la Carte Vitale 2**[39] vis-à-vis des services en ligne de la sphère santé-sociale, notamment le Dossier Médical Personnalisé (DMP) qui en constitue le chantier majeur.

Bien que les résultats de ce travail ne soient pas disponibles à ce jour, des fonctions de type « identification », « authentification » et « signature » pourraient être mises en œuvre de façon à formaliser les rapports entre usagers (assurés, patients..) et prestataires de services, et notamment contractualiser leurs relations avec les hébergeurs de données.

Le GIE SESAM-VITALE est financé par les organismes d'assurance obligatoires et complémentaires, fort soucieuses de sécuriser les échanges avec leurs assurés. Lors du démarrage de la télétransmission SESAM-Vitale (1998), le recours au code PIN[40] n'a pas été retenu pour la facturation des prestations médicales ou lors de la délivrance de médicaments, pour des questions de facilité d'usage des assurés.
Actuellement, des expérimentations sont prévues, pour vérification en ligne du taux de remboursement de médicaments dans le cadre de la prise en charge des affections longues durée.

La CNAM et la DGME étudient les besoins exprimés pour l'usage de la Carte Vitale 2, notamment pour accéder à certains services sociaux de l'Etat, tels que l'authentification forte aux services de la CAF.
Etant donné que **le face à face avec un agent habilité n'est pas envisagé à court terme** (les besoins de sécurité actuellement exprimés n'imposant pas la remise de carte en main propre), la classification du certificat correspondrait, au démarrage du programme, à un échelon de type PRIS*.
La capacité à renforcer le niveau de sécurité initial (par exemple pour satisfaire des exigences de services sociaux souhaitant combattre la fraude et s'assurer de l'identité des ayants droits) est également étudiée.

---

37 Belgique, Finlande, Espagne, Estonie, Suède…

38 Entretiens avec le GIE Sesam Vitale, le 8 Février 2007, la Caisse Nationale d'Assurance Maladie, le 13 Juin 2007 et le GIP DMP.

39 Cabinet Dictao.

40 Le code PIN primaire est neutralisé, par contre le code secondaire est actif.

L'usage du PIN – ou une approche de type OTP[41] – pourrait être envisagé pour se connecter au DMP afin de protéger les données médicales et de sécuriser des procédures coûteuses comme la prise en charge d'Affections Longue Durée (ALD) ou de protocoles de soins. Bien naturellement le patient pourra consulter en ligne ses historiques de remboursement.

Avec les mutuelles complémentaires[42], la CNAM étudie actuellement comment bénéficier de l'architecture technique de la carte Vitale (par inscription de données en carte Vitale ou dans d'autres cartes dites DUO, compatibles avec ses lecteurs[43]).

L'étude en cours sur les usages de la carte Vitale concerne l'ensemble des acteurs du monde santé-social (organismes d'assurance obligatoire ou complémentaire, DMP, services sociaux de l'Etat,..). Bien que les résultats de cette étude ne soient pas encore publiés, on anticipe que les complémentaires exigeront à terme la mise en place d'une procédure d'authentification forte de façon à confirmer l'identité d'un ayant droit, lors d'une consultation ou de l'achat de médicaments en pharmacie.

Parmi les projets prospectifs, citons le programme Netc@rds, dont le GIE SESAM Vitale est le coordonnateur, qui vise l'interopérabilité des contrôles de droits, dans la plupart des cas sur base de lecture des cartes de santé locales en Europe.
Concernant les procédures d'authentification visées, le projet étant dans sa phase de démarrage, il est prématuré d'en préciser ici le périmètre.

3- La vente en ligne[44]

A chaque branche de l'économie numérique correspond la formalisation d'un rapport client / fournisseur qui transpose les procédures du monde réel. Pas plus que dans l'usage courant, acheter un objet ne nécessite de prouver son identité mais simplement d'en payer le prix, et, dans la majorité des cas, sans formalités juridiques.
L'économie numérique ne modifie nullement les règles du jeu mais utilise au mieux les outils disponibles en fonction du niveau de risque et du contexte réglementaire : mails, mots de passe statiques et dynamiques, SMS ou mélange de technologies, de façon à tracer, en cas de litige, les actions de l'internaute.

Pour acheter sur un site d'enchère, nul besoin de s'identifier, encore moins de s'authentifier, mail et mot de passe suffisent ! Quant à la transaction, son fonctionnement est déjà cadré par les cartes bancaires, donc remboursement sur preuve d'usage frauduleux du titre.

Le commerce électronique en France pèse 13 Milliards d'Euros en 2006, dont 60% d'offres de services (90% de voyages), le reste correspondant à la vente de biens, marquant une progression de 40% sur 2005.
La fraude sur les cartes de paiement est faible, soit 0,2% du CA total ; la grande majorité des litiges proviennent d'une tromperie sur la nature des objets ou prestations proposées.

---

41 One Time Password, Mot de Passe Dynamique.

42 Notamment la FFSA (Fédération Française des Assureurs), membre du GIE Sésame Vitale

43 De son coté, la FNMF (mutualité française), également membre du GIE, a fait le choix d'héberger les données administratives des complémentaires, sur la carte Vitale.

44 Entretiens avec la Fevad : Fédération des Entreprises de Vente à Distance, et divers acteurs de la banque en ligne.

Vu le faible niveau d'authentification requis, tout comme l'absence de formalisme de la transaction, les prestataires de vente en ligne n'expriment pas d'attentes vis-à-vis des certificats de CNIe.

En revanche, les acteurs majeurs, comme cette filiale d'eBay[45], ou encore l'un des poids lourds français du domaine, se sont positionnés **comme intermédiaires visant à rétablir les relations de confiance de l'économie de marché.**
D'un côté, validation des capacités du fournisseur, de l'autre, puissants mécanismes de *profiling* et *scoring* pour prévenir la fraude (correspondance adresse / nom) ou définir des comportements d'achat ; des technologies d'apprentissage basées sur réseaux de neurones développés à l'échelle mondiale.
Ces prestataires d'un genre nouveau font l'objet de **tentatives d'«hameçonnage[46]» ou de « keylogging[47] »,** par le biais d'écrans détournés ; des actes de malveillance qui contribuent à freiner l'essor du commerce électronique et la stratégie internet des banques en France. Aussi l'un d'eux propose-t-il un **service optionnel de certificats** pour accéder à un service sécurisé de loggin, sur la base de quelques Euros / mois, de façon à rassurer les acheteurs.

La démarche de ces intermédiaires de vente en ligne se base sur le constat suivant :
plus de **50% des internautes abandonnent leur transaction en route** ; par ailleurs, si des procédures interbancaires de type « 3D Secure » sont implémentées, 20% des acheteurs restants vont de nouveau abandonner leur transaction.
Ces acteurs nouveaux se sont donc engouffrés dans un champ laissé vierge par les banques qui, en sur-dimensionnant les risques de fraude, ne se sont pas positionnés avec réactivité sur le marché de la confiance entre acheteurs et vendeurs, dans un contexte d'absence de contact physique avec les objets.
Des offres récentes de type « Receive and Pay » répondent bien à la demande d'internautes qui souhaitent **vérifier la qualité d'un achat négocié en ligne**, avant d'enclencher le mécanisme de paiement. Bien que recommandée par la Banque de France, la solution « 3D Secure » est majoritairement rejetée par les sites marchands qui la considèrent comme un frein au commerce sur le net.

Faute de faire appel à ces nouveaux cercles de confiance, les déconvenues des vendeurs ne sont pas rares. Malgré la mise en garde de la FEVAD[48], certaines PME avouent avoir été séduites par des commandes miracles sans réaliser qu'un paiement par carte est invalide si le porteur de titre ne peut être identifié avec certitude. Dans ce contexte qui ne bénéficie, ni de systèmes interbancaires fiables (3D Secure), ni de médiateurs de transaction décrits ci-dessus, il n'est pas rare que la PME soit obligée de restituer le montant de la transaction, si la carte de paiement a été utilisée frauduleusement (et sans récupérer sa marchandise, lors d'un envoi à l'export).

---

45 4 millions de comptes en France, 50,000 nouveaux comptes par semaine, 100,000 à Noël, 130 millions de comptes dans le monde.

46 L'hameçonnage, appelé en anglais *phishing*, est une technique utilisée par des fraudeurs pour obtenir des renseignements personnels dans le but de perpétrer une usurpation d'identité. La technique consiste à faire croire à la victime qu'elle s'adresse à un tiers de confiance — banque, administration, etc. — afin de lui soutirer des renseignements personnels : mot de passe, numéro de carte de crédit, date de naissance...

47 Un *keylogger* (littéralement *enregistreur de touches*) est un dispositif chargé d'enregistrer les frappes de touches du clavier et de les enregistrer, à l'insu de l'utilisateur. Il s'agit donc d'un dispositif d'espionnage.
Certains *keyloggers* sont capables d'enregistrer les URL visitées, les courriers électroniques consultés ou envoyés, les fichiers ouverts, voire de créer une vidéo retraçant toute l'activité de l'ordinateur !

48 Fédération des Entreprises de Vente A Distance.

Ce **marché d'intermédiation** reste malgré tout fort modeste[49]. Il confirme **le manque de maturité de cette activité** mais aussi le faible entrain des entreprises françaises à se propulser vers l'économie numérique.
Dans la mesure où beaucoup de PME ne disposent pas d'infrastructures de vente en ligne, faute d'activité suffisante sur le web, les cas de fraude mentionnés par la FEVAD permettent d'anticiper le recours à des services sécurisés de paiement basés sur l'identité et non plus les mécanismes interbancaires (en quelque sorte, des médiateurs de transactions, qui proposeraient des services « à la demande » sans nécessiter de comptes récurrents acheteur /vendeur comme cela est proposé aujourd'hui). Vu le risque de ces transactions « one shot », il est probable que l'authentification forte par CNIe constitue l'élément clé de ces services futurs.

→ On anticipe que l'offre de médiateurs évolue dans les années à venir de façon à faire face aux zones d'ombres de l'économie internet. Deux voies peuvent être identifiées dès maintenant, mais il est probable qu'avec l'essor de la vente en ligne d'autres services voient le jour prochainement :
D'une part, **combattre la fraude** – même faible - des paiements en ligne par cartes[50], évalués à 30 Millions d'Euros en France et qui va certainement suivre la progression du secteur, soit 40% par an.
De l'autre, **l'autorisation de prélèvement bancaire de particuliers ne disposant pas de cartes de paiement**. Un marché qui représente 15% du commerce en ligne, soit plus de 2 Milliards d'Euros ; dans ce cas, des intermédiaires pourraient prélever quelques % en fluidifiant, par le biais de la future CNIe, l'actuelle procédure courrier, en total décalage avec l'économie numérique !

Ces acteurs de confiance ne montrent pas d'attente particulière vis-à-vis de la CNIe, dans la mesure où ils proposent des règles de fonctionnement sans identifier l'internaute ni formaliser leurs achats.
Par contre, ceux qui visent des marchés mondiaux n'excluent pas de modifier leurs procédure d'authentification si une approche commune des CNI était adoptée par l'Union Européenne. En effet, les marges des fournisseurs sont très faibles sur le net, aussi les intermédiaires, comme les vendeurs de voyages en ligne[51], sont-ils à l'écoute de toute solution innovante leur permettant de faire face à ce pourcentage incompressible de fraude qui rogne leurs bénéfices.

Il est possible que d'autres acteurs se positionnent prochainement sur ce créneau juteux de l'intermédiation, ou que nos prestataires développent de nouvelles offres de service. Suivant une enquête FEVAD, plus d'un internaute sur quatre confie avoir procédé à un achat sur le net au cours du dernier trimestre. Il est donc probable que les 40 % de progression de 2006 soient largement dépassés et **que l'adoption de SEPA[52] (Sigle European Payment Area) constitue un nouveau facteur de croissance**. Quel en sera le rôle de la CNIe ? Il est encore prématuré de le déterminer, mais on ne peut négliger que l'authentification forte jouerait à terme un rôle si ce secteur devait connaître une progression plus importante.

---

49 Deux acteurs majeurs se partagent le marché français : d'une part 1,5 M euros, de l'autre, 2,1 M Euros. Près de 1000 entreprises adhèrent au système sur la base d'un % du CA généré en ligne.

50 0,2 % de 14 Milliards d'Euros en France, chiffres FEVAD.

51 Les sites de vente de voyages en ligne évaluent la fraude à 1% de leur CA, un pourcentage non négligeable, connaissant la modicité de leurs marges.

52 Lancé en 2002, le projet SEPA (Single Euro Payments Area), c'est-à-dire espace de paiement unique en euro, a pour objectif final d'assurer que tous les paiements de détail en euro soient exécutés de façon efficace, sûre et au même coût en Europe qu'au niveau national. L'impact de SEPA sur le commerce en ligne, et notamment les questions relatives à la fraude constituent un sujet complexe qui n'a pu être traité dans le cadre de cette étude.

L'un de ces intermédiaires de vente nous confiait être prêt à prendre des risques sur l'incompressible pourcentage de fraude avoué de façon à gagner des parts de marché sur le commerce en ligne . On peut anticiper que ces risques puissent être minimisés si l'Etat met prochainement en œuvre son programme de CNIe. En effet dans des cas litigieux, repérés par les mécanismes de scoring, notre médiateur pourrait demander une confirmation d'authentification, sur la base de CNIe, qui permettrait, sinon d'éliminer, du moins de réduire sensiblement le pourcentage de fraude.

4- Le Crédit à la consommation[53]

Le **contrôle d'identité** n'intervient que marginalement dans le cas de la vente en ligne, et seulement pour résorber la fraude. En revanche, **cette formalité constitue la base des relations entre clients et organismes de prêt**. En cas de litige, les tribunaux débouteront systématiquement le prêteur s'il n'a pas respecté les procédures préalables à l'octroi de financement. Vu la multiplicité des offres, la DGCCRF(Direction Générale de la Concurrence, de la Consommation et de la Répression des Fraudes) examine scrupuleusement leurs sites web de façon à détecter d'éventuelles irrégularités.

Il n'est donc pas étonnant que les acteurs du crédit en ligne soient parmi les précurseurs d'offres nouvelles et pionnières sur la base d'authentification forte et de signatures par le biais de certificats électroniques.
Cela pour deux raisons simples: **fluidifier leurs relations avec leurs clients mais surtout gagner des parts de marché sans pour autant négliger les fondamentaux juridiques**[54]**.**

Le modèle économique traditionnel des organismes de crédit, longtemps porté par les grandes enseignes de la distribution, est en train de basculer vers le « tout web ». Alors qu'autrefois on sortait de la FNAC avec une télévision sous le bras et un crédit en poche, aujourd'hui, l'internaute négocie simultanément achat et emprunt personnalisé grâce aux accords entre sites marchands et prêteurs de deniers. Bien que la majorité des contrats (80/20) de financement soient encore conclus par les réseaux de revendeurs, on anticipe une parité avec les contrats 100% web dans les trois ans à venir.

Cet intérêt pour le web ne fait que poursuivre la stratégie ancienne des financeurs qui consiste à proposer des prestations nouvelles aux clients une fois recrutés par les enseignes : crédits revolving, crédits amortissables, cartes d'achat, etc. Mais, à la différence du mode historique qui passait par les télévendeurs et campagnes marketing, le web devient, aujourd'hui le média privilégié par sa facilité de communication avec les clients.
Par contre, les coûts de traitement deviennent relativement lourds, dans la mesure où le web génère un volume considérable de dossiers incomplets ou fantaisistes.

Outre les contrôles d'identité - pivot du dossier - les prêteurs procèdent aux méthodes de scoring traditionnelles :

---

[53] Entretiens avec les représentants des acteurs majeurs du crédit à la consommation en France.

[54] C'est en France que l'emprunteur est le plus protégé d'Europe. La réglementation française impose diverses contraintes aux établissements de crédit établis sur son territoire. En matière de crédit à la consommation, les lois Scrivener et Neiertz prévoient :

- un délai de rétractation de sept jours ou de quatorze jours en vente à distance de service financier,
- l'interdépendance entre le contrat principal et le contrat de prêt,
- ainsi que le droit au remboursement anticipé sans aucune indemnité.

cohérence nom/ adresse par bases de données téléphoniques, accès au FICP [55] et fichier négatif de la Banque de France.
Malgré ces traitements automatiques, le délai moyen d'étude des dossiers est encore évalué à 3-4 jours, faute d'une méthode d'identification sûre en ligne ; une éternité vis à vis de comportements sur le net particulièrement instables !

Le crédit à la consommation connaît **deux types d'approches** : **la conquête de nouveaux clients, et le *cross-selling***, pour démarcher des comptes existants, à raison d'un ratio de 20/80 au profit du second ;
Les deux approches sont soumises aux contraintes des **Lois Scrivener-Neiertz**, à savoir le respect du délai de rétractation et la rédaction d'un contrat de prêt.
Vu les frais importants de marketing et de constitution de réseaux de distribution, la conquête demeure une opération coûteuse – pouvant atteindre plusieurs centaines d'Euros pour des offres complexes de type rachat de crédit - alors que le cross-selling se réduit à quelques dizaines d'Euros, une fois le client connu de l'organisme de crédit.

L'évolution des modalités de transactions sur le web devient très perceptible et c'est à qui simplifiera les démarches au maximum dans l'attente du procédé magique - et juridiquement fiable - qui permettra de s'authentifier et signer en ligne.
En effet, depuis 2001 certains financeurs ont commencé à proposer, d'abord une acceptation préalable de crédit, puis l'offre préalable de crédit à imprimer et retourner après signature manuscrite.
Bien conscient que le temps joue en sa défaveur, le financeur vise des solutions en ligne de bout en bout, qui empêchent l'internaute d'imprimer son offre pour ensuite la renégocier auprès d'un banquier comme c'est souvent le cas aujourd'hui[56].

La **communication en ligne de justificatifs numérisés** (CNIe, RIB, relevé EDF, etc.), proposée récemment par un financeur, constitue déjà un moyen de gagner du temps ; car toute démarche qui éloigne l'internaute de l'écran, comme imprimer un dossier et le poster, contribue à décourager les adeptes du moindre clic !
Grâce à cette approche nouvelle, l'organisme de crédit réduit les efforts de courriers, générateurs de pertes. Il peut également proposer un package complet, notamment une assurance emprunteur et enclencher sa contractualisation en ligne, dans l'attente d'une acceptation définitive.

Dans l'attente d'un programme fort de type CNIe, les organismes de crédit testent aujourd'hui toutes les démarches qui visent à supprimer ces jours incompressibles de traitement de dossier en interne, un gain de temps fort utile dans l'univers particulièrement réactif du web où le client ne manquera pas de faire jouer la concurrence par quelques clics de souris.

Dans cette course à la fluidification des traitements et à la croissance de parts de marché, les mécanismes nouveaux d'authentification forte et de signatures à valeur juridique sont particulièrement bien accueillis par la profession.
Aussi, au moment précis de ces entretiens, la majorité des grands financeurs étudie-t-elle avec attention des solutions à base de certificats[57] électroniques pour conquérir de nouveaux clients ou faciliter le *cross-selling* de comptes existants.

---

55 FICP : Fichier national des Incidents de remboursements de Crédits aux Particuliers.

56 Les financeurs sont très discrets sur le nombre de contrats non retournés, mais il est notoire que l'absence de loyauté constitue l'une des caractéristiques majeures du web. Cela, d'autant plus que des sites de type meilleurtaux.com ont construit leur offre sur le principe de mise en concurrence.

57 Pour de nombreux secteurs, Internet est une opportunité tout aussi bien qu'un obstacle. C'est le cas des activités nécessitant la signature de contrats. Ainsi dans les secteurs bancaires et

Leur constat est simple : peu d'internautes concluent aujourd'hui leur transaction sur le web, impliquant notamment d'imprimer un contrat et de retourner les pièces justificatives.

Aussi, dans l'attente d'un outil d'authentification / signature à valeur juridique, proposent-ils de télécharger un certificat pour signer immédiatement l'offre préalable de crédit ; **le délai Scrivener** permettant amplement de procéder aux vérifications d'usage. Mais, **le point fort**, c'est de **réduire au minimum** – quelques minutes - **la procédure de constitution du dossier** en enclenchant une mécanique juridique solide qui respecte les délais et sera irréprochable en cas de litige.

Concernant les démarches de *cross-selling,* la préoccupation d'authentification / signature est identique dans la mesure où les financeurs sont fréquemment confrontés aux accidents de vie (surendettement, perte de travail, séparation, divorce, décès, etc…). Aussi les tribunaux requerront-t-ils les pièces justificatives, en cas de litige.
Le crédit revolving, qui permet de jouir d'une réserve de trésorerie, exige non seulement d'authentifier le demandeur mais exige aussi la signature des co-emprunteurs, le cas échéant. D'où l'intérêt d'outils sur le web permettant de fluidifier ces démarches en ligne, sachant que les clients procèdent à environ trois-quatre demandes par an.

Contrairement à la signature électronique sécurisée qui bénéficie d'une présomption de fiabilité, **les téléchargements de certificats nécessiteront**, en cas de litige, **de démontrer la légitimité du procédé**, d'où l'échange de multiples pièces justificatives dites de « gestion de preuve ».

Ces procédures innovantes, qui réduisent l'effort « papier » en faisant la part belle aux transactions sur web, laissent présager une croissance forte des demandes de financement en ligne, une fois la CNIe délivrée, qui suivra naturellement la progression du commerce électronique. La nécessité de télécharger son certificat les rend encore fastidieuses, mais ces procédures ouvrent la voie à un mode opératoire qui, par le biais d'un simple lecteur USB, permettront à l'internaute, de prouver son identité et d'apposer une signature juridiquement irréprochable.

On estime également que des initiatives visant la mise en place de cercles de confiance privés, de type « Microsoft passeport » qui permet de gérer en ligne des données privatives multiples, vont accroître encore cette tendance à la fluidité ; l'internaute pourra alors communiquer des informations sensibles comme sa déclaration de revenus ou ses bulletins de salaires, sans devoir les numériser ou les photocopier puis les envoyer par courrier.

---

financiers, la dématérialisation de la procédure va rarement jusqu'à la signature, qui reste "physique" pour des questions de sécurité et d'identification des signataires. Un obstacle que veut faire sauter (…) le lancement d'un système de signature électronique.

"Les quelques offres existantes en France ne s'adressaient qu'aux clients établis (...). La procédure, mise en place (...) avec un prestataire de services de certification électronique, comprend l'authentification, avec envoi par le prospect de documents justificatifs en format numérique (carte d'identité, RIB, justificatif de domicile...), la vérification et l'étude du dossier, puis éventuellement le téléchargement d'un certificat privatif. L'internaute peut alors signer électroniquement le contrat.

Avec cette transaction dématérialisée de bout en bout, l'internaute n'a plus à se déplacer ou à envoyer de documents par la poste. De son côté, "la société cliente élargit sa cible aux prospects, qu'elle ne pouvait toucher jusque là que par le papier" : Baptiste RUBAT du MERAC, Journal du Net.

5- Banque de réseau [58]

Les représentants de la banque ont été parmi les plus assidus à suivre les démarches du Ministère de l'Intérieur sur la future CNIe mais ont **opté à court terme pour des technologies propriétaires**, vu la demande du marché d'accéder aux comptes en ligne et les retards du projet d'identité de l'Etat.

Comme pour la vente sur le web, les moyens mis en œuvre répondent au souci de sécuriser l'accès à un compte et de faire face aux menaces de fraude. Mais, contrairement à la négociation de crédits en ligne, ici la signature d'un contrat est rare, sinon pour l'ouverture d'un compte.
En effet, consulter son compte requiert un minimum de confidentialité mais pas de signer un contrat ; en revanche, **engager une transaction ou procéder à un virement nécessite du formalisme**, pas nécessairement juridique, mais qui garantisse sa **traçabilité** en cas de litige.

Un constat, largement partagé par la profession, qui a favorisé les technologies mixant codes aléatoires, mots de passe dynamiques (OTP)[59], mails et SMS pour déjouer les malveillances en modifiant les identifiants à chaque transaction.
Mais, vu les récentes tentatives d'hammeçonnage et de *keylogging*, qui peuvent générer des montants considérables de fraude, les transactions bancaires sur le web sont encore très limitées : consultation de relevés, négociation de valeurs mobilières. Les virements de comptes à comptes, ou transferts vers l'étranger nécessitent que le bénéficiaire soit répertorié au préalable.

Pourtant, la signature de documents à caractère juridique nécessite de transposer sur le web les usages du monde réel.
Aussi, dans un souci identique à celui constaté auprès des acteurs du crédit, les banques de réseau commencent-elles à proposer un téléchargement de certificats pour signer des contrats ou des avenants aux contrats en cours. Dans ce cas précis, les risques de fraude sont faibles, le client étant déjà connu du banquier ; par contre il dégage sa responsabilité en cas de litige.
Dans ces contextes, **le recours à la signature, même téléchargée, est précieux** : il permet de fluidifier les rapports entre usagers et la banque tout en préservant le cadre légal. C'est la procédure retenue par certains établissements pour proposer des contrats d'assurance ou faciliter un changement d'intitulé de compte.

Bien que les banquiers semblent se satisfaire aujourd'hui de technologies d'authentification assez rudimentaires, ils se montrent très sensibles aux perspectives de la future CNIe. Notamment pour **la première « mise en relation » avec leurs clients**, qu'il s'agisse de banques de réseaux ou de banques «en ligne», afin de répondre à la réglementation sur le blanchiment ou la justification de l'origine des fonds.
Leurs interrogations portent également sur **le contenu « facial » du futur titre d'identité** : photographie, date de naissance, sexe, etc. pour éviter d'équiper les agences en lecteurs afin de récupérer des informations non visuellement disponibles.
L'accès aux listes de révocation des certificats apparaît aussi comme une demande primordiale de façon à s'assurer de la légitimité d'un titre, sachant que l'accès aux données biométriques ne sera pas autorisée. Plutôt maximalistes dans leur approche, les banquiers

[58] Entretiens avec la société Altenor mais également avec des représentants de banques et d'organismes interprofessionnels (CFONB, GIE CB) .
[59] One Time Password

vont jusqu'à regretter que la CNIe ne soit pas rendue obligatoire et qu'il soit impossible d'authentifier le porteur d'une carte au moyen de ses empreintes[60].

Bien que nos interlocuteurs aient refusé de s'engager sur la mise en œuvre d'infrastructures lourdes, faute de visibilité sur le programme CNIe, ils n'excluent pas que ses certificats jouent à terme un rôle clé pour accéder aux comptes en ligne. Mais, dans cette perspective, ils demandent que soient clarifiés les rôles respectifs des acteurs ; tout en reconnaissant le rôle régalien de l'Etat vis-à-vis de l'identité, ils souhaitent que le certificat « signeur » soit émis par leur soins. Une attitude qui rejoint une proposition initiale du MIAT afin que la future CNIe puisse héberger des certificats tiers et ainsi dégager toute responsabilité quant aux usages de la carte.

Cette approche parait légitime dans la mesure où on ne peut exclure que des transactions en ligne puissent être opérées par détournement – physique ou logique – d'un code d'usager.
Le certificat de banque pourrait donc être remis de façon discrétionnaire, en fonction d'une relation aux clients et d'usages possibles, suivant un modèle de coûts à préciser, à l'image des cartes bancaires d'aujourd'hui. En fonction du type de certificat souscrit, la banque pourrait alors autoriser des virements, transactions de valeurs mobilières, garantir un découvert ou même couvrir une tentative de fraude.
On ne doit également pas sous-estimer le risque de répudiation suite à des négociations hasardeuses en ligne. Dans ce contexte, l'activation d'une transaction par signature électronique prend une valeur légale ; aussi est-il fondamental de s'entendre sur l'origine d'un tel certificat, sachant que ce n'est pas à l'Etat de garantir sa validité.

→ Faute d'une feuille de route de la CNIe, les banques n'ont pas développé de stratégie concernant ces certificats d'usagers, mais cette piste semble fort prometteuse et amenée à se développer une fois le titre d'identité instauré. Si ce document d'identité ne devait pas héberger de certificats tiers, il pourrait être envisagé d'utiliser successivement deux cartes pour des transactions en ligne : d'abord la CNIe pour s'authentifier, puis une carte « signeuse » pour les transactions engageant la responsabilité de la banque. Lecteur bi-fente, succession de cartes dans un même lecteur USB ou même génération de certificats privés à partir des clés publiques de la CNIe ? Il serait nécessaire de pousser plus avant cette étude pour y répondre.

6- La banque en ligne[61]

Les banques de réseau sont quelque peu à la traîne des organismes de crédit (qui sont en général leurs filiales !) pour la mise en œuvre d'offres sur le web, dans la mesure où le contact client s'effectue majoritairement en agence et que les démarches contractuelles sont bien moindres.
La banque en ligne, au contraire, par son ambition de dématérialiser la gestion de comptes, constitue un champ privilégié d'authentification forte, tout au moins pour la première « mise en relation » avec leurs clients.
On peut anticiper que, une fois l'ouverture de compte effectuée, clients et banquiers se satisfassent de technologies rudimentaires mentionnées plus haut dans la mesure où les consultations en ligne et applications transactionnelles nécessitent moins de formalisme.

---

60 MOC (Match On the Card ne nécessite pas d'accès à un serveur distant mais permet d'authentifier l'usager en comparant ses empreintes aux données numériques stockées dans la puce.

61 Entretien avec des représentants majeurs de la banque en ligne.

Le blanchiment d'argent constitue une préoccupation majeure du secteur ; aussi l'origine des fonds est-elle systématiquement contrôlée, tout comme les virements pour des montants élevés. Les établissements préfèrent recourir à des méthodes traditionnelles comme le chèque de façon à vérifier leur origine comme recommandé par le CISI[62] et le GAFI[63]

La procédure d'ouverture de compte est en général assez simple : document au format PDF dynamique à remplir en ligne, imprimer et retourner signé manuellement avec des pièces justificatives telles que photocopie de la CNI, RIB et attestation de domicile.
Bien qu'elles soient soumises aux traditionnelles procédures de *scoring* basées sur les fichiers négatifs et contrôles de cohérence avec les bases de données téléphone, ces pièces sont aisément falsifiables. **Aussi l'attente de ces établissements bancaires est-elle forte vis-à-vis de procédures d'authentification sur la base de CNIe et certificats électroniques.**

En effet, les perspectives de croissance du secteur suivent l'engouement des internautes pour le web. Ainsi l'un des grands acteurs du domaine envisage-t-il un encours supérieur au milliard d'Euros en 2010 en dématérialisant sa gestion de contrats d'assurance vie. Deux autres établissements totalisent près d'un demi-milliard d'encours en réduisant leurs droits d'entrée à 0,5% au lieu des 3% perçus généralement sur les contrats d'assurance vie. Un point non négligeable dans la mesure où les montants négociés sur le web atteignent 20,000 Euros contrairement aux 4,000 Euros contractés en moyenne par les courtiers ; ce qui confirme l'attrait de populations averties et relativement aisées, pour la banque en ligne.

Tous acteurs confondus, la banque en ligne totalise près de deux millions de comptes en France aujourd'hui avec une croissance annuelle d'environ 25%, dont plus de la moitié des adhérents seront recrutés par le web, et non plus par les courtiers (donc sans aucun contact « physique » avec les guichets).

Dans ce contexte, la future CNIe semble bien positionnée, d'abord pour répondre à la contrainte réglementaire d'authentifier les clients mais surtout pour leur attribuer des droits étendus, dès l'ouverture, avec des services du type carte Visa « Premier » ; des privilèges qui nécessitent en général une période probatoire, vu le souci de s'assurer du sérieux des clients et prévenir le risque fréquent de fraude dans les premiers mois.

Connaissant les possibilités de falsification de l'actuelle CNI, un des établissements a institué un RIH (Relevé d'Identité sur l'Honneur) et envisage de recourir prochainement à des webcams pour traiter avec ses internautes !
En effet, la FFSA[64] exige que le client d'une assurance-vie soit connu et identifié à chaque transaction, notamment pour la vente d'un contrat au profit de tiers, source de fraude non négligeable !
En attendant mieux, certains ont réfléchi à la possibilité que les contrats en ligne soient signés par les certificats de télé-déclaration de revenus. Une solution techniquement possible, mais sans validité juridique et réelle efficacité, en cas de fraude, dans la mesure où leurs listes de révocation ne sont pas disponibles aux acteurs du secteur privé.

Les acteurs de la banque en ligne sont très conscients de la limite des mécanismes de transactions proposés à ce jour en anticipant l'apport des nouvelles technologies, comme le confirme ce site web « *Le client reconnaît que l'utilisation de son code d'accès par téléphone ou internet vaut signature. (...) pouvant toujours exiger la confirmation d'un ordre par écrit.*

62 Comité Interministériel pour la Société de l'Information
63 Groupe d'Action Financière http://www.fatf-gafi.org
64 Fédération Française des Sociétés d'Assurance

Les moyens d'accès sont susceptibles d'être complétés, modifiés ou supprimés, à tout moment, sans préavis, notamment en fonction des évolutions technologiques ».

Parmi les secteurs les plus susceptibles de malversations qui pourraient bénéficier d'une authentification forte, citons :

- le versement sur des comptes tiers,
- le contrôle d'accès aux comptes,
- la non-répudiation des ordres passés en ligne.

Par son objectif de dématérialiser l'ensemble de la relation client, la banque en ligne constitue, après le crédit à la consommation, l'un des secteurs les plus favorables à l'usage de la CNIe. En effet, l'ouverture de comptes (authentification) et les transactions sur le web (signature) - par nécessité d'en assurer la traçabilité et non-répudiation – nécessitent la mise en œuvre d'outils pouvant avoir une valeur juridique en cas de litige.

Les pays démocratiques ont largement pris conscience des liens étroits noués entre terrorisme et blanchiment d'argent. Bras armé des états, le GAFI (Groupe d'Action Financière)[65] a proposé le principe d'une coopération internationale étroite, tout en soulignant la nécessité de mettre à profit les technologies de l'information[66] pour contrer les actes de malveillance.
Alors que l'Europe visait, par le biais du passage à l'Euro, la montée en puissance de l'économie internet, les Etats-Unis prenaient conscience de la fragilité des échanges dématérialisés par le célèbre « Know your customers » du Patriot Act, rédigé dans la foulée des attentats du 11 Septembre 2001[67].
Ainsi, le CIP (Customer Identification Program) détaille-t-il les mesures à prendre pour authentifier les acteurs d'une transaction financière[68].

La Directive Européenne 2005/60/CE du Parlement et du Conseil du 26 octobre 2005 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme, en constitue la réponse de Bruxelles.
Elle fait largement place au contrôle d'identité « Conformément à ses dispositions, chaque État membre est tenu d'interdire le blanchiment de capitaux et d'imposer à son secteur

---

65 Anglais FATF (Financial Action Task Force)

66 In recent years, several governments worldwide have instituted electronic commerce laws that directly or indirectly require companies to reduce their vulnerability to identity theft. The United States, the European Union, Korea, Brazil, Japan, Australia, Singapore and many other nations have drafted or implemented regulations to safeguard consumer privacy, protect corporate data integrity and enhance auditing accountability. Standards to combat money laundering and terrorist financing that include customer identification have been proposed by the Financial Action Task Force (FATF), an inter-governmental organisation, and have been adopted by more than 150 jurisdictions. In large part, these rules call for companies to adopt stronger identity authentication measures to assure governmental authorities about the veracity of their electronic transactions. Current and prospective regulations have created a boom in the interest in and use of identity authentication technologies such as digital certificates, biometrics, one-time passwords (OTP) and tokens.

67 Section 326, od the US Patriot Act : "Legislation requires financial institutions to verify each new account's holder's identity before opening an account.

68 "(It) is also required to include procedures to verify the identity of customers opening accounts. Most financial institutions will use traditional documentation such as a driver's license or passport. However, the final rule recognises that in some instances institutions cannot readily verify identity through more traditional means, and allows them the flexibility to utilise alternate methods to effectively verify the identity of customers".
La dernière phrase recommandant largement le rôle des technologies de l'information pour procéder au contrôle des documents d'identité « As part of a CIP, financial institutions must maintain records including customer information and methods taken to verify the customer's identity ».

financier, y compris les établissements de crédit et une vaste palette d'autres établissements financiers, d'identifier ses clients, de conserver des pièces justificatives appropriées…. Il y a lieu, conformément aux nouvelles normes internationales, d'introduire des dispositions plus spécifiques et plus détaillées sur l'identification du client et de tout bénéficiaire effectif et la vérification de leur identité. Pour ce faire, une définition précise du bénéficiaire effectif est indispensable. Et, plus précisément, les mesures de vigilance à l'égard de la clientèle comprennent :

- l'identification du client et la vérification de son identité, sur la base de documents, de données ou d'informations de source fiable et indépendante;
- le cas échéant, l'identification du bénéficiaire effectif et la prise de mesures adéquates et adaptées au risque, pour vérifier son identité, de telle manière que l'établissement ou la personne soumis à la présente directive ait l'assurance de connaître ledit bénéficiaire effectif (Article 8) ».

→ Nous sommes aujourd'hui à la conjonction de trois vagues qui vont nécessairement converger dans les années à venir : **l'essor de l'économie sur le net, la prise de conscience de la relation étroite entre actes de malveillance et blanchiment de capitaux et, enfin, la montée en puissance de l'identité électronique sur la base des technologies de l'information**.

Comme mentionné dans notre préambule, la gestion des certificats liés à l'identité électronique permet de satisfaire aux exigences à la fois réglementaires et légales, authentifier de façon certaine un individu et procéder à une signature à teneur juridique. Gageons que ces outils vont connaître une éclosion importante dans les années à venir.

7- Le notariat [69]

La fonction notariale n'échappe pas à l'attrait du web pour formaliser ses actes. Tout comme les praticiens de la santé, notaires et clercs se sont dotés d'un certificat qualifié[70] de signature simple, appelé **Carte REAL.**
Il permet de s'authentifier au fichier des testaments, aux comptes de la Caisse des Dépôts et Consignation et à PLANET : une application qui gère les flux financiers avec la DGI (notamment les états hypothécaires).

Dans la mesure où les **actes authentiques nécessitent la présence physique des parties** pour que le notaire puisse attester de leur libre consentement, seuls les mouvements inter-notaires sont aujourd'hui dématérialisés et signés électroniquement par la procédure REAL.

Depuis le 1° septembre 2007, cette carte est remplacée par une clé USB qui contient des certificats qualifiés. Une procédure de remise de clés doit être mise en œuvre pour l'attribution aux collaborateurs.
Il devient ainsi **possible que des particuliers, non présents physiquement sur le même lieu, signent des actes en présence de leurs notaires respectifs sur la base de cette procédure**. Il est même envisagé de recourir à des tablettes graphiques pour signer numériquement les documents à l'avenir.
Par contre aucune décision n'a été prise pour que des certificats électroniques soient utilisés par les particuliers lors de la signature d'actes authentiques. Ce point, qui relève du Garde

69 Entretien avec la Chambre des Notaires, 12 Février 2007,
70 Depuis le 1er sept 07.

des Sceaux, va certainement évoluer dans le contexte du lancement de la CNIe et même faciliter les procédures de dévolution de procurations vis-à-vis de tiers.

De plus, les notaires sont très enclins à échanger des courriers électroniques avec leurs clients, pendant la phase préliminaire à l'établissement d'un acte authentique. Il leur apparaît donc fort utile que ces échanges puissent être signés électroniquement, d'où un intérêt très fort pour les procédés d'authentification et de signature à valeur juridique.

8- Les services publics [71]

Concernant l'accès aux services de l'Etat, il importe de distinguer **les demandes des entreprises des besoins de particuliers.** Mais, comme mentionné précédemment, il est fondamental de ne pas négliger l'utilisation possible de certificats de CNIe par les PME, travailleurs indépendants, artisans et professions libérales[72].
En effet, on évalue les démarches administratives à plus de 130 millions de formulaires par an, dont 20 millions pour les DUE (Déclaration Unique d'Embauche) et DUE MSA contractées pour l'embauche de saisonniers en milieu agricole. Sans compter les 2 millions de DCR[73] qui constituent la base des cotisations versées par les indépendants aux caisses de RSI[74] et URSSAF. L'idéal pour le déclarant étant de récupérer son SIRET à partir d'une procédure d'authentification forte à base de certificats de CNIe et ensuite valider électroniquement son envoi ; une personne physique pouvant signer pour le compte d'une personne morale. Dans ce contexte, il n'est pas réellement question de sécuriser la connexion aux comptes, vu les faibles risques de fraude, mais plutôt de fluidifier l'accès aux services publics.

Pour **les particuliers**, les certificats de CNIe pourront servir à signer leur déclaration de revenus et à se connecter à leur dossier fiscal, qui, pour des questions de confidentialité, requiert ce mode d'authentification forte.
Bien que les projets de la Carte Vitale ne soient pas entièrement arrêtés à ce jour, il est envisagé que cette dernière permette également de se connecter aux services de TéléIR. Dans ce cas, le certificat remplace la signature manuscrite du déclarant, qui, par ce biais, confirme sa déclaration.
De façon à faciliter les démarches administratives, l'Etat entreprend la mise en œuvre du site « Monservicepublic » [75] qui permettra d'accéder aux services suivants : CNAF, ANPE, Documentation française, Éducation Nationale…
Des fonctions additionnelles telles que « porte-documents électronique » seront également proposées pour conserver en ligne ses dossiers administratifs.

La DGME[76] qui pilote cette opération, n'a pas pris de décision exclusive quant aux moyens d'authentification[77]: mot de passe, téléphone mobile, carte à puce…. requis pour accéder à « Mon Service Public ».

---

71 Entretiens la CNIL, le Forum des Droits sur Internet et la Caisse des Dépôts et Consignation,

72 Le CFONB ne souhaite pas la confusion entre certificats personnels et professionnels, pourtant les micro-entreprises constituent un formidable « produit d'appel » pour la CNIe

73 Déclaration Commune des Revenus.

74 Assurance Maladie.

75 http://www.service-public.fr/monservicepublic/index.html

76 La Direction Générale pour la Modernisation de l'Etat qui remplace l'ADAE, Agence pour le Développement de l'Administration Electronique.

Conformément à l'ordonnance 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre usagers et autorités administratives et entre autorités administratives, c'est l'autorité administrative elle même qui met en place son télé service pour déterminer les fonctions de sécurité de sa protection ainsi que le niveau de sécurité de ces fonctions.
Dans ce contexte, l'usager s'authentifiant avec un mot de passe à « Mon Service Public », ne pourra accéder qu'aux services requérant ce niveau d'authentification, l'usager s'authentifiant avec un certificat de niveau PRIS *** pourra accéder à tous les télé services.

Lors de nos entretiens, la CNIL[78] n'a montré aucune objection quant à un usage étendu de la future CNIe, si la vie privée de l'internaute est préservée et si l'Etat ne procède pas à un « t*racking* » de ses actions sur le web.
Au plus, les représentants du Forum des Droits sur Internet[79] ne souhaitent-ils pas un usage systématique de cette CNIe pour des accès en ligne, ce qui est le cas aujourd'hui sachant que la politique de la DGME consiste à diversifier les méthodes de connexion (mot de passe, Vitale, CNIe) pour accéder aux services de l'Etat.
Pareillement la CNIL ne formule aucune objection de principe à ce que des certificats tiers soient embarqués dans la future CNIe, si cela ne va pas à l'encontre du respect de la vie privée des citoyens.
A l'image du « Government Gateway » Britannique, il peut être envisagé que les citoyens français disposent prochainement d'un coffre-fort électronique[80], à distance ou sur leur PC, qui contienne des données personnelles, déclaration d'impôts, numéro d'allocataire, références à différentes prestations sociales. On pourra ainsi naviguer entre les différents services de l'administration à partir d'un accès de type « jeton ». Mais, pour des raisons de confidentialité, il sera nécessaire d'utiliser un certificat numérique pour y accéder.

Ici encore, CNIe et Vitale constituent deux médias bien adaptés, mais avec toujours la prérogative, pour le titre d'identité de l'Etat, d'offrir une possibilité d'authentification forte.

Il serait donc souhaitable que les usagers puissent opter, à leur convenance, pour un ou plusieurs modes de connexion. Mais, par expérience, l'accès aux services web est grandement facilité si on utilise toujours la même procédure, ce qui fait de la CNIe un média idéal, qu'il s'agisse de comptes bancaires ou des services publics.
Dans cette perspective d'un usage étendu, il sera nécessaire de banaliser son usage auprès des citoyens.

---

77 Les degrés d'authentification sont classés comme suit : Login + password : niveau 0 ; procédure OTP par GSM : niveau 1 ; certificat qualifié: niveau 3.

78 Entretien avec la CNIL, le 3 Mai 2007.

79 Entretien avec le Forum des Droits sur Internet.

80 La notion de coffre-fort électronique n'est pas normalisée à ce jour.

III - Modèles économiques et chaînes de valeurs

Il est impropre de parler d'un modèle économique des certificats de CNIe dans la mesure où ce sont les applications privées qui vont le plus bénéficier de ce service d'authentification forte, mais sans participer aux investissements d'infrastructure.

Par contre, en initiant le programme, l'Etat exerce pleinement sa fonction régalienne par la mise en œuvre d'un processus « de bout en bout » permettant de certifier l'identité des citoyens.
Il est donc essentiel d'évaluer, au moins dans ses grandes lignes, les retombées financières ou gains de productivité générés par le programme.

1- La gestion de l'infrastructure à clés publiques de CNIe

La gestion de l'infrastructure de certificats, qu'elle soit assurée par l'Etat lui-même ou externalisée chez un opérateur privé, constitue l'un des volets majeurs du programme de CNIe. Est-ce un service profitable ? Quel en est le montant ? Cette activité peut-elle être couplée à d'autres solutions centrées sur l'authentification des personnes et la sécurité des paiements ?

Bien que gratuit pour qui en fait la demande, le coût de mise en œuvre des certificats qualifiés de CNIe revient à une dizaine de centimes /an et par usager. Il inclut leur délivrance et activation par PIN code, la gestion et mise à jour des listes de révocation de même que leur régénération à l'issue d'une période estimée aujourd'hui à cinq ans[81].
Concernant ces listes de révocation, deux approches sont possibles : soit leur téléchargement régulier, soit un accès transactionnel à chaque interrogation sur la base du protocole OCSP[82], de façon à vérifier la validité du certificat[83].
Tout opérateur privé de services pourrait avoir accès à ces informations moyennant quelques centimes d'Euros par transaction suivant le modèle actuel de validation des transactions opérées par les cartes de crédit[84].

Peut-on anticiper l'apparition de services de confiance sur la base des certificats de CNIe ?

Il est encore prématuré d'y répondre, alors que le programme est encore à l'étude. Pourtant le relatif succès des intermédiaires de vente en ligne, tout comme les risques importants de fraude et de blanchiment sur Internet, laissent augurer la possibilité de mise en œuvre de telles offres.

---

81 Il est envisagé que le certificat puisse être régénéré en ligne par l'usager lui-même, pour une période de validité de 3 ans. Ce point sera précisé ultérieurement par l'équipe du programme d'identité électronique.

82 OCSP : On-line Certificate Status Protocol

83 Et son statut de révocation.

84 C'est aujourd'hui le modèle suédois par lequel l'Etat perçoit 10 centimes d'Euros par interrogation. Sachant que 40 millions de consultations sont enregistrées annuellement par TéléIR en France, ce seul service générerait 4 Millions de recettes, une fois la CNIe mise en place.

2- Les organismes de crédit

La seconde voie à explorer porte sur l'impact des certificats de CNIe - authentification et signature - dans le contexte de l'économie numérique.
Le commerce électronique ne constitue pas une piste privilégiée à court terme, hormis certains segments de marché comme :

- l'autorisation de débit bancaire pour les usagers ne possédant pas de cartes de paiement,
- ou l'authentification forte pour des transactions en ligne très ponctuelles, sachant qu'il est prématuré d'anticiper l'impact de SEPA sur la vente en ligne.

Par contre les prestataires de crédit et de la banque en ligne constituent deux secteurs particulièrement prometteurs dans la mesure où la réglementation leur impose des contraintes très strictes qui peuvent être idéalement mises en œuvre par ces certificats.

Comme mentionné, le crédit à la consommation et la banque en ligne constituent deux secteurs pouvant fortement bénéficier d'un programme de CNIe. Il est pourtant délicat de déterminer les gains de productivité attendus ou les croissances d'encours potentiels dans la mesure ou beaucoup de projets sont encore dans les cartons ou, dans le meilleur des cas, en phase expérimentale. Il est toutefois possible de proposer des estimations connaissant l'engouement des français pour l'achat en ligne.

On estime à plus de trente millions le nombre cumulés d'emprunts contractés auprès d'organismes de financement spécialisés en crédit à la consommation, à l'acquisition de véhicules ou au rachat de crédits.

Un chiffre qui exclut délibérément les prêts contractés auprès de banques de réseau, dans la mesure où la contractualisation des dossiers, traditionnellement réalisée en agence, n'est pas réellement tributaire de mécanismes du web (notre étude visant à privilégier les secteurs pouvant bénéficier d'une croissance exceptionnelle par la mise en service de CNIes).

Par ailleurs les banques de réseau n'ambitionnent nullement de concurrencer un secteur largement occupé par leurs filiales de crédit. Nous proposons d'écarter également les prêts immobiliers de cette étude, dont on estime qu'ils ne sont pas soumis aux exigences d'immédiateté comme c'est le cas pour l'achat d'un bien en ligne. Si les banques de réseau devaient développer de telles offres, tout au plus pourrait-on évoquer une fluidification des mécanismes sans nécessairement envisager une croissance des encours.

Les établissements de crédit connaissent actuellement une croissance moyenne du nombre de prêts d'environ 10 à 12% par an. Bien que les offres via internet soient encore mineures aujourd'hui (inférieur à 20%), ce sont celles qui connaissent la plus forte progression, aux dépens des canaux traditionnels comme les grandes enseignes ou le télémarketing.
Ici, les frais moyens de conquête peuvent être estimés à plus de 200 Euros par client, si l'on intègre la somme des coûts tels que marketing, rédaction /envoi /retour du contrat, traitement et vérification des pièces, suivi de dossier[85].
Un ratio de l'ordre de 5% si on évalue l'encours moyen des prêts à 4000 Euros[86].

[85] La gestion de la preuve est estimée à 5-10 Euros

[86] Ce chiffre constitue une moyenne entre les crédits revolving (750 à 2000 Euros), les crédits consommation (1000-4000 Euros) et les rachats de crédits (2500-35K Euros)

La croissance des financeurs dépend de leur stratégie de *cross-selling*, notamment de la vente de nouvelles prestations une fois le client acquis par les distributeurs ou en conquête directe : revolving, carte de crédit, points de fidélité….
Ici, les coûts sont bien moindres dans la mesure où le dossier emprunteur existe déjà: déclaration de revenus, bulletins de salaires, justification de domicile, RIB.
Pourtant, même dans ce cas, ils n'échappent pas à l'exigence d'authentification et de signature du client pour toute nouvelle offre. Connaissant cette contrainte réglementaire, on imagine aisément le **gain de productivité si la CNIe permet au client de s'authentifier et de signer l'offre en ligne, qu'il s'agisse de conquête ou de *cross-selling***

Sachant que les organismes de crédit envisagent à terme de contracter la moitié des offres sur le web, on pourrait **estimer leur coût moyen de conquête à environ 50 Euros, une fois la CNIe mise en service.**
Une diminution réaliste, sachant que des technologies de *scoring* puissantes permettront d'automatiser le rejet de dossiers non pertinents (mais considérant que le contrôle de pièces et la constitution du dossier reste incontournable[87]).
Le but ultime est de faire signer l'offre préalable de crédit, à partir d'une CNIe insérée dans un lecteur USB, avec renversement de la charge de la preuve au bénéfice de l'internaute, alors que, dans le meilleur des cas, il doit aujourd'hui télécharger son certificat depuis un serveur distant.
On imagine aisément **la facilité de procédure et le confort des usagers**, sachant que la majorité des usagers abandonnent les transactions si les écrans sont trop nombreux et complexes.

Dans cette perspective d'automatisation par CNIe, le rapport entre prêt moyen et coût de conquête pourrait diminuer de 5% à 3,75%, soit un gain de productivité de plus de 200 Millions d'Euros si on estime le total d'encours à plus de 14Mds Euros.
Pareillement, le traitement du *cross-selling*, entièrement géré sur le web, deviendrait relativement modique, l'ensemble de la relation avec le client étant dématérialisée (estimons-le à environ 30 Euros !) sachant que le contrôle de pièces actualisées reste indispensable, même pour un client connu.
Dans ce cas, **le ratio encours / conquête tombe à 3%,** d'où un gain de productivité de plus de 600 Millions d'Euros sur un total estimé de 10 Mds d'Euros en *cross-selling*.

Mais leur véritable gain, outre une réduction des frais de traitement, proviendra certainement de la **progression des encours**.
Partant d'une croissance annuelle de 8-10% grâce aux facilités du web, (notamment par la possibilité de comparer les offres, simuler un coût de crédit, gérer sa réserve de trésorerie, bénéficier de cartes d'achats….) et sachant que la vente en ligne progresse de 40% par an, on peut raisonnablement estimer que les demandes de prêt vont augmenter de 3% en plus de la croissance déjà constatée[88] (soit 750 Millions d'Euros qui seront injectés dans l'économie, sur la base d'un montant d'encours cumulé d'environ 25 Mds d'Euros).

Gageons que l'automatisation future des traitements via les certificats de CNIe et la mise en ligne d'un portfolio de données personnelles, (comme proposé par Monservicepublic)

---

87 Mentionnons pour information que ces coûts restent aujourd'hui relativement élevés dans la mesure où, la CNIe n'existant pas, les organismes de crédit doivent faire face à un très grand nombre de dossiers numériques incomplets ou fantaisistes.

88 Tout acquisition en ligne ne requiert pas un crédit, mais on peut envisager qu'un packaging de plus en plus étroit et simplifié entre achat et financement, avec notamment possibilité de livraison immédiate de l'objet, contribuera à la progression du financement.
L'usage banalisé d'une CNIe, permettant de réduire la charge administrative de l'internaute, constitue un facteur incitatif de demande de crédit.

pouvant intégrer déclaration de revenus, bulletins de salaires et justification de domicile, devraient encore accroître le volume des crédits dans les années à venir.

Concernant **l'assurance emprunteur**, le packaging en ligne d'une solution intégrée à l'offre de prêt, comme ceci tend à devenir la norme, constitue également un facteur de croissance des offres.
Si on estime à environ 3% le montant moyen des primes perçues sur des encours de prêts (en conquête et cross-selling) évalués à plus de 25Mds d'Euros, le traitement dématérialisé des contrats d'assurance permettrait de réaliser un gain de productivité d'environ 150 Millions d' Euros, en baissant le coût de traitement des dossiers.

Il est difficile de mesurer quel pourrait être l'impact de la CNIe sur la fraude, sachant que les contrôles d'identité sont déjà conduits très systématiquement par les organismes de crédit.
En revanche, on peut anticiper une automatisation plus complète de la chaîne de traitement des pièces justificatives, déjà prise en compte par les gains de productivité mentionnés ci-dessus.

A la différence des milieux bancaires qui souhaitent disposer de leurs propres certificats « signeurs » pour ratifier une transaction, les financeurs sont surtout intéressés par le **potentiel juridique des certificats** : notamment, bien authentifier les usagers dans le contexte délicat de co-emprunts souscrits par des couples confrontés à des accidents de vie, tout en obtenant une signature à valeur juridique forte.

3- La banque en ligne

La banque en ligne offre des perspectives de croissance assez proches de celles constatées auprès des organismes de crédit. Et cela, pas nécessairement sur les frais de traitement déjà faibles dans la mesure où la relation au client est déjà dématérialisée mais surtout sur la « mise en relation » qui nécessite de contrôler très rigoureusement l'identité du futur client.

Dans la **perspective d'une authentification forte réalisée par les certificats de CNIe, qui permet au banquier de satisfaire pleinement aux exigences réglementaires, on peut estimer une baisse des coûts de conquête d'environ 100 à 50 Euros**, soit un gain de productivité d'environ 13 Millions d'Euros, si l'on considère que la moitié des nouveaux clients contracteront exclusivement par internet[89]. Un montant relativement modeste à l'image de ce secteur encore à ses débuts mais qui risque de croître, étant donné l'engouement des français pour la banque en ligne.

Mais le **véritable dynamisme se trouve dans la progression des sommes investies par le biais du web** – près de 2 Mds d'Euros à ce jour - avec une croissance d'environ 10% l'an.

On pourrait objecter que ces montants seraient de toute façon placés en bourse par le biais des banques de réseaux. Ce n'est pas exact dans la mesure où la banque en ligne propose des facilités de gestion et une réduction[90] de frais de garde très significatives. Elle s'adresse à une clientèle nouvelle et très avertie d'internautes[91] qui exploitent et gèrent de façon active

89 Environ 500,000 nouveaux comptes sont ouverts chaque année.

90 ING et Boursorama facturent des droits d'entrée de 0,5% au lieu des 3% habituels sur les assurances vie. Chez ce dernier, les droits d'entrée, de sortie et de garde des titres ne sont pas facturés sur plus de 700 fonds communs de placement.

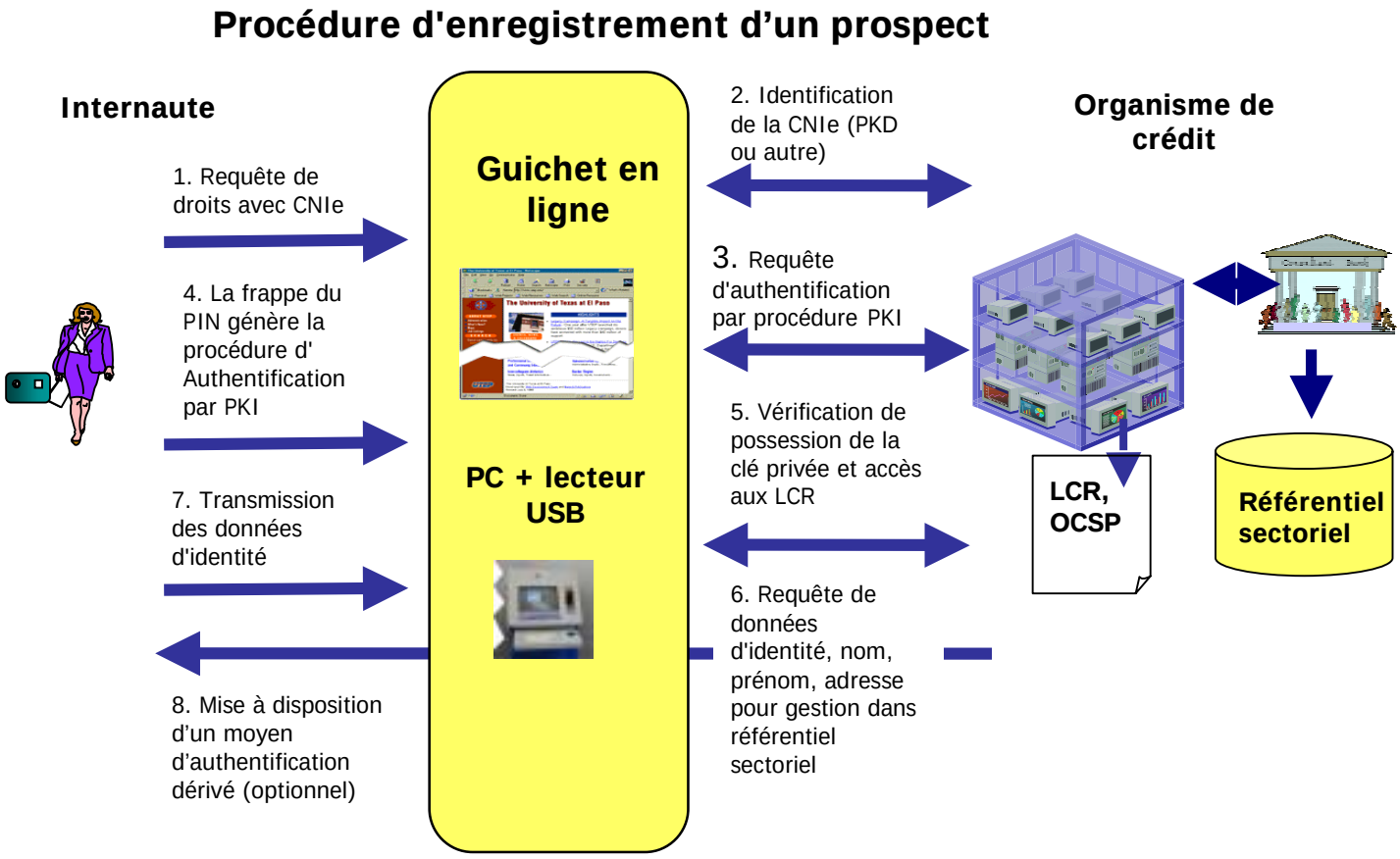
91 A ce jour, 33% des français utilisent internet pour gérer leurs comptes bancaires ou leurs placements financiers, contre 19% un an plus tôt.

leurs portefeuille sur le web, bien plus que via les banques traditionnelles. Cette clientèle est séduite par les ressources multiples de ces sites - tableaux de bords, gestion de portefeuille en ligne, simulations, alertes….
Une étude TNS Sofres évalue à 47% les détenteurs d'actions en France, contre 33% en 2005 et 24% en 2004 ![92]. C'est donc un secteur amené à se développer suivant un rythme de croissance de plus de 40% par an.

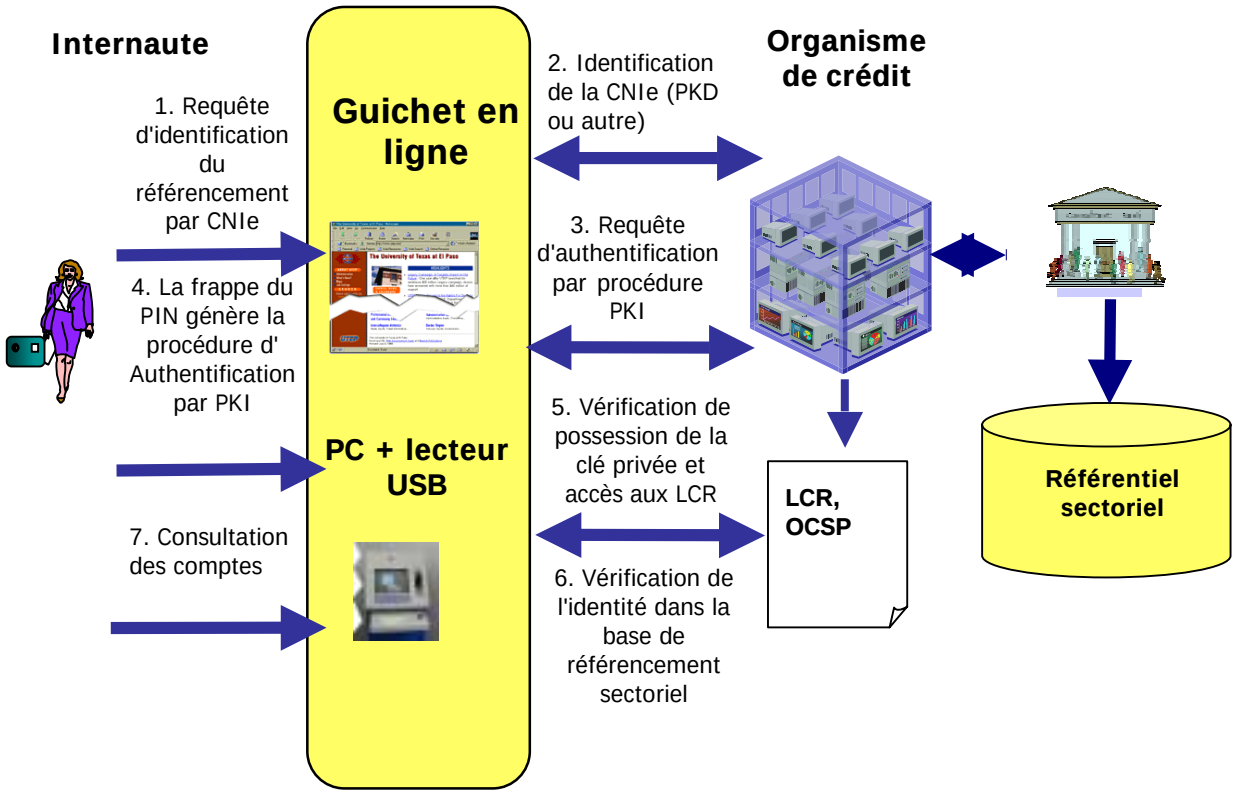
Au vu de ces chiffres, on perçoit l'enjeu réglementaire et le souci d'éviter que la banque en ligne ne devienne une véritable industrie à blanchir les capitaux ou financer les actes de malveillance.
On estime que les contrôles amont deviendront particulièrement stricts, donc que la vérification de l'identité par le biais de certificats de CNIe constituera une formalité préalable aux ouvertures de comptes.
Comme mentionné précédemment, le client en confiance par adhésion via CNIe pourrait immédiatement bénéficier de conditions privilégiées – de type carte Visa Premier – sans période probatoire, comme c'est le cas aujourd'hui, dans la mesure où les fraudes interviennent dans les premiers mois d'ouverture des comptes.

[92] Concernant les assurances-vie, 25% de nos concitoyens en ont souscrit à ce jour (1000 milliards d'encours). Le vieillissement de la population, comme la nécessité de complémenter le régime des retraites, laisse présager une augmentation des encours dans les années à venir et une prépondérance du web, vu la possibilité de comparer les offres en ligne, simuler des versements de primes etc….

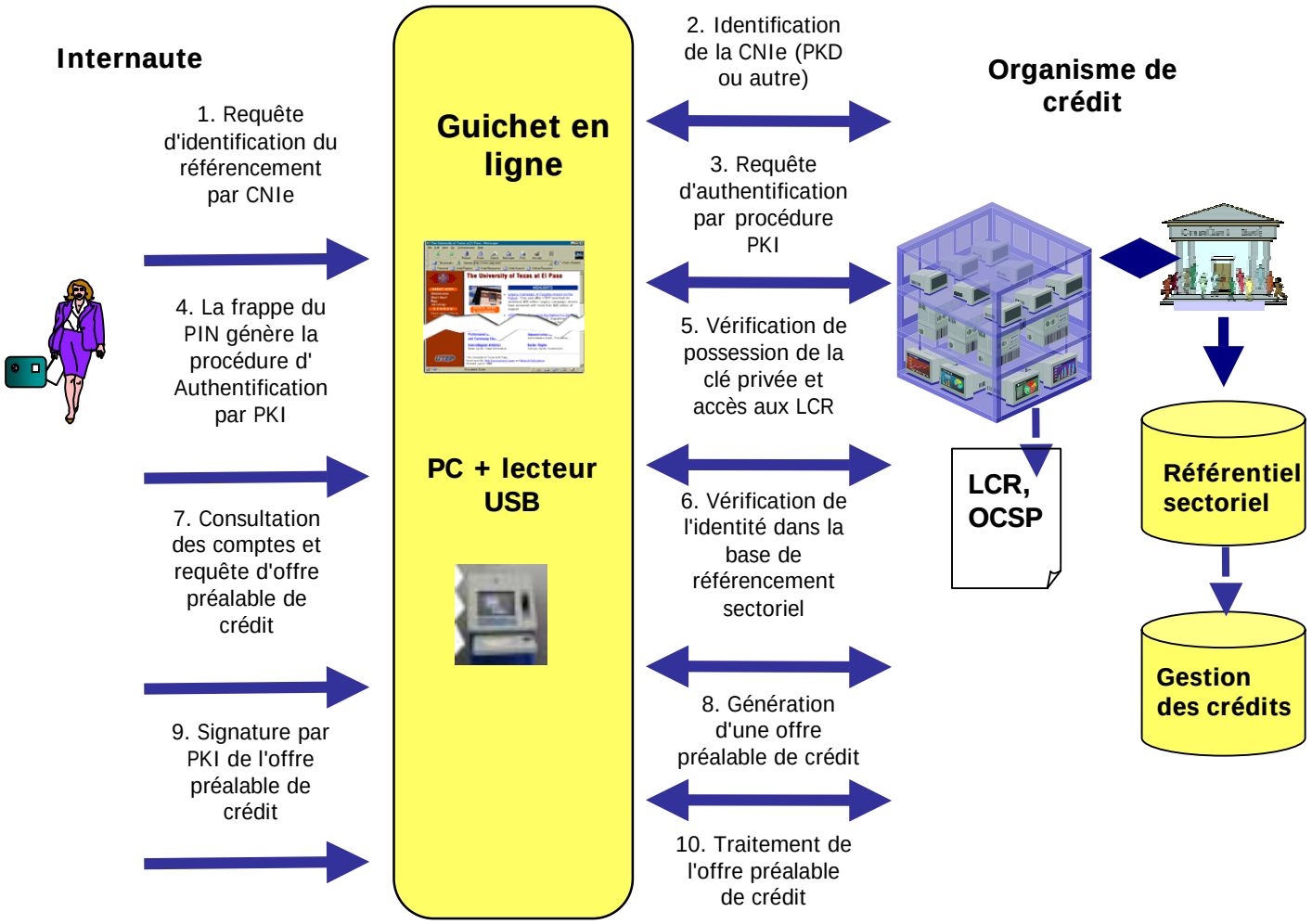
4- Mise en œuvre d'une architecture à base de PKI



Procédure d'authentification avec carte e-ID



Procédure de signature avec carte e-ID



IV - Perspectives stratégiques, moteurs et freins à l'adoption de solutions de PKI vis-à-vis des secteurs identifiés

Le potentiel de développement des services en ligne sur la base de certificats de CNIe est considérable. Ce marché n'existe pas aujourd'hui, mais il apparaît fort mature dans la mesure où de nombreux programmes pilotes sont initiés via des jeux de clés téléchargés sur le web. Bien qu'ils ne répondent nullement aux exigences d'une signature sécurisée, ils permettent néanmoins de signer les documents et préfigurent le potentiel d'usage et de fluidification de la future CNIe. Ces développements suivent l'engouement pour la vente en ligne, en pleine croissance grâce à la généralisation de l'ADSL.

Ainsi, par sa faculté d'intégration aux sites marchands, en proposant un pavé « financement » à la conclusion d'un achat, l'offre de crédit est-elle aujourd'hui pionnière sur le web mais sans réellement avoir pu exploiter toutes les ressources d'une signature de CNIe.
La génération en ligne d'une « acceptation préalable de crédit », puis de « l'offre préalable de crédit » à imprimer et retourner avec signature manuscrite, proposée récemment par un des protagonistes, représente déjà un gain précieux d'environ trois jours, fort utile dans cet univers très compétitif ou le client se joue de la concurrence en quelques clics.
On peut aisément estimer que la possibilité de signer les contrats de prêts en ligne par certificats de CNIe, ouvrira des perspectives nouvelles aux financeurs.

Ainsi l'offre « *Receive and Pay* » de deux grands acteurs de la place permet-elle déjà de déconnecter l'achat du financement, donc de satisfaire le souci d'immédiateté des internautes et de gagner des parts de marché.

Comme mentionné précédemment, le secteur public proposera prochainement de nombreux services en ligne. Même si la majorité d'entre eux n'a pas mis en oeuvre d'authentification forte ou des signatures à teneur juridique[93], il se pourrait que les usagers, non nécessairement férus d'internet, puissent être séduits par une carte permettant de se connecter à de multiples sites – publics et privés - par une procédure unique et simplifiée d'authentification.
Si cette démarche devait être massivement adoptée par les professions libérales, PME et indépendants, ce sont plus de 130 millions de formulaires qui pourraient être traités automatiquement, d'où un gain de productivité considérable pour les agents de l'Etat.

[93] justement du fait qu'il n'y a pas encore de CNIe avec signature électronique.

1- Réduction de la fraude et gains de productivité attendus par introduction de la CNIe :

Secteur	Type de fonction	Mode de calcul	Gains de productivité ou Marché adressable/ an pour nouveaux services
Commerce en ligne	Fraude aux cartes de paiement	0,2% du CA (14 Milliards Euros)	28 Millions d'Euros
Commerce en ligne	Autorisation de prélèvement bancaire	15% du CA (14 Milliards Euros)	2 Milliards d'Euros
Vente de voyage en ligne	Fraude au paiement.	1% d'un CA de 1 Mds Euros	10 Millions d'Euros
Banque en ligne	Conquête nouveaux clients	500,000 nouveaux comptes / an ½ sur internet . Coût moyen de traitement de dossier 50 Euros	25 Millions d'Euros
Crédit consommation	Conquête nouveaux clients	36 Millions de comptes, 10% de croissance, 200 euros coût de conquête	720 Millions d'Euros
Crédit consommation	Vente de nouveaux produits en cross-selling	Ratio : 1 conquête génère 3 cross selling, coût du cross selling : 50 Euros	540 Millions d'Euros
Assurance	Assurance automobile	3 Millions d'immatriculation / an. Coûts de traitement 50 Euros	150 Millions d'Euros
Administration	Déclaration de DUE / DUE MSA	130 millions de formulaires x 10 Euros / formulaire	1,3 Milliards d'Euros
Ministère des finances	Télé IR	10 Millions de formulaires / an	

2- La vente en ligne

Le chiffre d'affaire consolidé de la vente en ligne reste relativement faible en France, 14 Mds en 2006, avec une croissance de 40% par rapport à 2006.
Elle concerne majoritairement les acteurs traditionnels de la VPC et grandes enseignes de la distribution qui y ont vu un canal puissant de diversification. Par contre les PME françaises restent fort conservatrices ; aussi ne doit-on pas exclure la mise en œuvre de services de confiance à l'intention d'entreprises ne traitant que rarement sur le web ou souhaitant «sourcer » leurs ventes en ligne.

→ Il n'est pas exclu que la CNIe puisse jouer un rôle clé dans ces échanges, notamment pour les personnes peu familières avec les sites de vente, mais désireuses de procéder à des achats très ponctuels.

3- Divers

La problématique du « recommandé » n'est généralement traitée que du point de vue de l'émetteur ; Aussi la Poste a-t-elle proposé sa fameuse LRE (Lettre Recommandée Electronique) qui génère, via le web, les courriers en RAR.
Le mode de réception ne change pas : livraison à domicile si présence du destinataire ; sinon démarche aux guichets, toujours en échange d'une signature manuscrite.
Pourtant, quel gain de productivité si la réception devait être réalisée sur PC en échange d'une signature électronique ! Cela suppose cependant que le récipiendaire possède un jeu de certificats qualifiés de type CNIe pour s'authentifier et activer sa signature par PIN code.
Même si les émetteurs peuvent être tentés de rédiger de tels courriers sans passer par un service spécialisé, grâce à une simple signature de CNIe, il est envisageable que la Poste - ou des prestataires indépendants - maintienne son offre en archivant électroniquement les éléments de preuve (émission et réception, horodatage) de façon à les produire en cas de litige.
D'autres secteurs, contraints par la loi aux exigences du RAR, pourraient également profiter d'une telle offre : syndics d'immeubles pour les convocations et PV de copropriété mais également les sociétés cotées pour leurs votes aux AG (Loi NRE 2001-420[94] du 15 Mai 2001). Dans chacun de ces cas, les certificats de CNIe satisfont à l'obligation légale de communiquer au préalable les ordres du jour, puis vote des résolutions avec un souci de **traçabilité** pour éviter les fraudes et risques de réclamation.

Hormis les gains de productivité aux guichets, cette activité d'émission /réception et archivage de pièces à valeur légale pourrait générer de nouveaux revenus auprès de la Poste ou de prestataires privés, comme la Chambre des Notaires vu les risques de litiges dans un monde de transactions dématérialisées.
Il **ouvre la voie au vote électronique à caractère professionnel**, pour les élections syndicales ou prud'homales et, à terme, pourrait constituer l'un des modes de validation du suffrage universel . La CNIe constitue un média idéal d'authentification et de signature, pouvant être rapidement comptabilisé et contribuer à baisser le taux d'abstention.
La problématique est identique : authentification forte de la personne puis validation de son choix par signature à teneur légale, devant garantir la traçabilité, en cas de litige.

D'autres pistes nécessitent d'être explorées **comme l'accès aux sites web réservés aux personnes majeures[95], notamment la Française des jeux, le PMU[96] et ultérieurement d'autres services, si leur monopole devait cesser** (comme le réclame aujourd'hui la Commission Européenne) et le gouvernement autoriser des prestataires privés à proposer ce type d'offre en ligne.
Comme ce secteur peut être amené à se développer, il pourra être envisagé un **marqueur de majorité** dans le certificat d'authentification de la future CNIe, ou la possibilité de requérir volontairement un certificat contenant cette information. Il est prématuré de préciser plus avant cette fonction, mais l'essor probable des jeux d'argent sur le net nécessite que ce secteur soit exploré plus en détail.

---

94 Loi n°2001-420 du 15 mai 2001 relative aux nouvelles régulations économiques http://www.legifrance.gouv.fr/WAspad/UnTexteDeJorf?numjo=ECOX0000021L#

95 Pour accéder au canal multimédia de la Française des jeux, le futur joueur doit être identifié, être titulaire d'un compte de résident et déclarer sur l'honneur qu'il est majeur. Dès l'accès au site, l'internaute confirme être en conformité avec cette demande.

96 Pour ouvrir un compte PMU, il faut être une personne physique âgée d'au moins 18 ans. L'usager doit saisir sa date de naissance et déclarer résider en France métropolitaine ou dans les départements d'outre-mer ou encore à Monaco.

V - Contexte Réglementaire

1- L'identification :

Les activités de l'homme le conduisent à s'identifier auprès des autres. Avec le temps, l'identité est devenue de plus en plus complexe, associant aux nom, prénom, et lieu géographique, des identifiants physiques (taille, couleurs des yeux, empreinte digitale) et sociaux (nationalité, profession, filiation, …).

Identifier consiste à exprimer l'identité d'une personne.
Celle-ci recouvre «*l'ensemble des composantes grâce auxquelles il est établi qu'une personne est bien celle qui se dit ou que l'on présume telle (nom, prénoms, nationalités, filiation...)* »[97] ainsi que tous « *les traits juridiquement pertinents qui se retrouvent aussi bien dans le numéro national d'identification attribué par l'INSEE que sur la carte nationale d'identité délivrée par le ministre de l'intérieur ou sur les actes de l'état civil*. »[98].

Concernant une personne physique, Gérard Cornu définit l'identité comme « *ce qui fait qu'une personne est elle-même et non une autre ; par extension ce qui permet de la reconnaître et de la distinguer des autres ; l'individualité de chacun, par extension, l'ensemble des caractères qui permettent de l'identifier.* »[99].

L'identification des personnes constitue la condition sine qua none de la sécurité des échanges sur les réseaux numériques, qu'il s'agisse de transactions ou de simples correspondances privées.

Il en va de même de l'authentification (vérification de l'origine) d'un message ou d'une requête. En effet, en droit, un acte ou un fait, doit **pouvoir être imputé – en principe – à une personne déterminée**. Le droit à l'anonymat n'est ainsi consacré que dans certaines hypothèses strictement limitées (accouchement sous X, défense de la liberté d'expression, données de connexion après un délai légalement prévu, anonymat « relatif » des personnes physiques qui publient des contenus sur le web, etc.)[100]. Rappelons ici que le droit à l'anonymat doit se mesurer à l'aune d'une responsabilité juridique essentielle de la personne : **celle de rendre compte de ses actes au cours de la vie sociale.**

Les internautes doivent rendre des comptes dans certains cas. En effet, l'utilisation des réseaux numériques n'est pas neutre, bien au contraire. L'Internet est rentré dans les foyers. Par conséquent, les comportements des internautes ne sauraient s'affranchir du respect des règles de droit.

De nombreux risques doivent ainsi être pris en compte :

- Les risques liés à **la dénégation d'un acte juridique** conclu par voie électronique (remise en cause d'un engagement/contrat sur les réseaux) ;

---

97 Lexique des termes juridiques, éd. Dalloz, 1999, p.280.

98 Alain Supiot, *L'identité professionnelle* in Les orientations sociales du droit contemporain. Ecrits en l'honneur du Professeur J. Savatier, PUF, 1992, p. 409 et s.

99 Gérard Cornu, *Vocabulaire juridique*, Ass. H. Capitant, PUF 2000.

100 Eric A. Caprioli, *Anonymat et commerce électronique*, in *Les premières journées internationales du droit du commerce électronique*, Litec, 2002, Act. de droit de l'entrep., p. 149 et s. disponible sur le site : www.caprioli-avocats.com.

- Les risque liés à **une utilisation délictuelle des réseaux** (par exemple, infractions liées aux actes de paiement, aux dénis de service (saturation), ou infractions facilitées ou liées à l'utilisation des technologies de l'information : diffusion de contenus illicites (pédo pornographie, racisme, antisémitisme, etc.), escroqueries par utilisation frauduleuse de numéro de carte bancaire pour une transaction en ligne (phishing[101]), les escroqueries par fausse vente sur un site d'enchères en ligne, les contrefaçons de logiciels ou d'œuvres audiovisuelles, que ces actes soient effectués à partir d'un ordinateur situé au domicile d'une personne ou dans une entreprise[102].

Une pièce d'identité est quant à elle « *un document écrit (généralement une carte) qui énonce et atteste l'identité civile d'une personne physique* »[103]. La Carte nationale d'identité est un document portatif individuel, délivré par l'Etat, permettant de vérifier l'identité de son porteur, voire de le contrôler. C'est dans cette optique que le programme INES (Identité Nationale Electronique Sécurisée) avait été lancé par le Ministère de l'Intérieur en 2005, ce programme consistant à [104] :

- fusionner les procédures de demande de carte d'identité et de passeport ;
- améliorer la gestion des titres dans de nouvelles applications ;
- délivrer des titres conformes aux exigences internationales[105] ;
- offrir des moyens d'identification et de signature électroniques aux citoyens.

Il est actuellement suspendu. Le projet va de pair avec la mise à disposition des citoyens de moyens d'identification et d'outils de signature électronique comme composantes de leur carte nationale d'identité électronique.

Or, la signature électronique fait d'ores et déjà l'objet d'une réglementation précise et détaillée sur le territoire national. Transposant la directive 1999/93/CE du 13 décembre 1999 pour un cadre commun sur les signatures électroniques[106] du Parlement et du Conseil européens, la loi du 13 mars 2000[107] a posé le cadre juridique de la preuve et de la signature électroniques.
Elle a été complétée par les décrets n° 2001-272 du 30 mars 2001[108] et n° 2002-535 du 18 avril 2002[109] ainsi que l'arrêté du 31 mai 2002[110]. Ce dernier arrêté a d'ailleurs été abrogé par un arrêté du 26 juillet 2004[111] relatif à la reconnaissance de la qualification des prestataires de services de certification électronique et à l'accréditation des organismes qui procèdent à leur évaluation.

---

101 Eric A. Caprioli, *Le phishing saisi par le droit*, Comm. Com. Electr. Février 2006, p.4 8, n°37.

102 Eric A. Caprioli, *Le risque pénal dans l'entreprise et les technologies de l'information*, JCP E, 2006, Cah. Dr. Entrep., janvier-février 2006, n°10.

103 G. Cornu, *préc*.

104 V. Le programme INES, émis par le Ministère de l'Intérieur, de la Sécurité Intérieure et des Libertés Locales, version 2 du 1 mars 2005.

105 Règlement (CE) n°2252/2004 du Conseil du 13 décembre 2004 établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les Etats membres, JOUE du 20 décembre 2004, L. 385/1.

106 Directive 1999/93/CE du 13 décembre 1999, JOCE n° L. 13, 19 janvier 2000, p.12 s.

107 V. notamment E. Caprioli, *La loi française sur la preuve et la signature électroniques dans la perspective européenne*, J.C.P. éd. G, 2000, I, 224 et *Ecrit et preuve électroniques dans la loi n°2000-230 du 13 mars 2000*, J.C.P. 2000, éd. E, cah. dr. entr. n°2, Suppl. au n°30, p.1- 11.

108 J.O. du 31 mars 2001, p. 5070.

109 J.O. du 19 avril 2002, p. 6944. v. à cet égard, D &P, février 2003, p. 116, obs. E. Caprioli.

110 J.O. du 8 juin 2002, p. 10223.

111 J.O. du 7 août 2004, p. 14104.

Enfin, la loi n°2004-575 pour la confiance dans l'économie numérique du 21 juin 2004 a consacré la validité juridique des écrits sous forme électronique (article 1108-1 du code civil)[112].

L'étude juridique de ce cadre réglementaire est un pré-requis essentiel pour déterminer les enjeux sociétaux, économiques et politiques de la CNIe.

2- La signature électronique :

Définition de la signature électronique

A titre liminaire, il conviendra de définir la notion de signature électronique. La loi du 13 mars 2000, a donné pour la première fois une définition légale en suivant une approche fonctionnelle de la signature.

Ainsi, selon l'art. 1316-4 alinéa 1 du code civil, toute signature doit remplir deux fonctions juridiques de base : l'identification de l'auteur de l'acte et l'expression du consentement du signataire au contenu de l'acte.

La définition générale de la signature électronique se retrouve à l'article 1316-4, al. 2 code civil, qui dispose : « *Lorsqu'elle est électronique, elle* (la signature) *consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d 'Etat.* »

Le procédé de signature électronique doit donc identifier le signataire, garantir le lien entre l'acte et la personne dont il émane et assurer l'intégrité de l'écrit signé.

A l'heure actuelle, seules les signatures électroniques basées sur la cryptologie à clé publique (à savoir les signatures numériques) répondent a priori à ses exigences légales et notamment à la garantie de la solidité du lien entre la signature et le message. Par conséquent, seule la signature numérique pourra être considérée comme une signature électronique sécurisée.

Celle-ci se définit suivant l'article 1.2 du décret du 30 mars 2001 comme : «*une signature électronique qui satisfait, en outre, aux exigences suivantes :*

- *être propre au signataire ;*
- *être créée par des moyens que le signataire puisse garder sous son contrôle exclusif; garantir avec l'acte auquel elle s'attache un lien tel que toute modification ultérieure de l'acte soit détectable*».

Cette signature électronique sécurisée est présumée fiable, contrairement aux autres formes de signature dont la fiabilité devra être démontrée, si elle est «*établie grâce à un dispositif sécurisé de création de signature électronique et que la vérification de cette signature repose sur l'utilisation d'un certificat électronique qualifié*»[113].

---

[112] J.O. n° 143 du 22 juin 2004, p. 11182. V. à ce titre, E. A. Caprioli et P. Agosti, *La confiance dans l'économie numérique*, P. Aff., 3 juin 2005 p 4 s.

[113] Art. 2 du décret du 30 mars 2001.

Au vu de cette définition doivent donc être pris en compte le dispositif sécurisé de création de signature électronique et le certificat électronique qualifié[114] pour caractériser une signature électronique sécurisée.

Or, comme l'énonce l'article 6 du décret du 30 mars 2001, «*Un certificat électronique ne peut être regardé comme qualifié que s'il comporte les éléments énumérés au I et que s'il est délivré par un prestataire de services de certification électronique satisfaisant aux exigences fixées au II*. ». Ces dispositions s'appliquent également en matière de validité juridique de l'acte (crédit à la consommation…), en vertu du nouvel article 1108-1 du code civil introduit par la L.C.E.N.

En tout état de cause, le marché français ne dispose à ce jour d'aucune signature électronique sécurisée ni de certificats qualifiés (hormis celui établi par la Banque de France dans ses relations avec les banques). Seuls certains modules sont accrédités par la D.C.S.S.I.

Signature électronique et signature électronique sécurisée

Cependant, il faut rappeler avec force que d'un point de vue strictement juridique, peu importe que la signature électronique soit sécurisée, qu'elle utilise un certificat qualifié ou qu'elle soit « simple », **elles ont toutes la même valeur juridique**. C'est le juge qui décide si la signature et l'écrit sous forme électronique sont admissibles ou non, pour la valeur probante ou la validité de l'écrit qui lui est présenté dans le cadre d'un litige.

Entre les signatures électroniques la seule chose qui change c'est la **charge de la preuve** ; elle variera selon que l'on bénéficie ou pas de la présomption de fiabilité. Mais la présomption de fiabilité est une présomption simple, qui peut donc être combattue par celui qui conteste les qualités du procédé de signature utilisé. Dans un cas, il appartient à l'utilisateur du procédé de signature de prouver cette fiabilité (signature électronique « simple »), dans l'autre, c'est celui qui la conteste qui devra prouver son absence de respect des exigences (signature électronique sécurisée). **Le certificat qualifié constitue donc une condition sine qua none pour disposer d'une signature électronique sécurisée. La qualification portera sur une famille de certificats donnés, émis sous une politique de certification donnée.**

---

[114] Ce certificat d'identification délivrée par le P.S.C.E. devra précisé, pour être considéré comme qualifié : «*a) Une mention indiquant que ce certificat est délivré à titre de certificat électronique qualifié ;*

b) L'identité du prestataire de services de certification électronique ainsi que l'Etat dans lequel il est établi ;

c) Le nom du signataire ou un pseudonyme, celui-ci devant alors être identifié comme tel ;

d) Le cas échéant, l'indication de la qualité du signataire en fonction de l'usage auquel le certificat électronique est destiné ;

e) Les données de vérification de signature électronique qui correspondent aux données de création de signature électronique ;

f) L'indication du début et de la fin de la période de validité du certificat électronique ;

g) Le code d'identité du certificat électronique ;

h) La signature électronique sécurisée du prestataire de services de certification électronique qui délivre le certificat électronique ;

i) Le cas échéant, les conditions d'utilisation du certificat électronique, notamment le montant maximum des transactions pour lesquelles ce certificat peut être utilisé.».

Régime juridique des P.S.C.E

Le système juridique français repose implicitement sur le certificat électronique. En effet, si le Code civil ne se réfère pas explicitement à ce moyen d'identification, il n'en reste pas moins vrai que le cadre réglementaire est construit autour de la notion de certificat. Le rôle des P.S.C.E. est donc, pour ces raisons, essentiel.

Les P.S.C.E. délivrent, à titre principal, des certificats électroniques permettant d'établir le lien entre les données de vérification de signature électronique (clé publique) et le signataire[115]. Ce dernier devra non seulement répondre à des exigences juridiques mais également à des exigences techniques. Si les exigences juridiques sont énoncées dans le cadre juridique ci-avant mentionné, les exigences techniques se retrouvent, en majeure partie, dans des travaux internationaux réalisés à l'I.E.T.F. (Internet Engineering Task Force) et à l'E.T.S.I. (European Telecommunications Standards Institute). Ce processus de normalisation permet la régulation de l'activité de P.S.C.E. en tentant d'assurer une interopérabilité technique minimale entre les différents prestataires. Dans cette optique technique, les différents P.S.C.E. se situent au cœur d'une Infrastructure à clé publique (I.C.P.)[116].
Cette I.C.P. comprend plusieurs entités qui ont des fonctions et des responsabilités distinctes. Plusieurs métiers coexistent : Autorité de certification, Opérateur de certification et Autorité d'enregistrement, Services de publication (annuaire ou liste de révocation des certificats ou des autorités de certification reconnues).
Il ressort de ce système que la confiance dépend de l'ensemble des composantes de l'I.C.P. Les P.S.C.E. au sein de l'I.C.P. auront intérêt, pour démontrer leur fiabilité technique et assurer cette interopérabilité, de respecter les dispositions de différents documents : une ou plusieurs politiques de certification (P.C.) ainsi qu'une ou plusieurs *Déclaration des Pratiques de certification* (D.P.C.) ou « *Certification practices statement*» (C.P.S.).
En règle générale, c'est l'A.C. qui sera le P.S.C.E. dans la mesure où c'est elle qui est responsable du certificat émis.
Du fait de leur rôle central dans les réseaux numériques, les P.S.C.E. ont un régime juridique différencié selon qu'ils délivrent ou non des certificats qualifiés.
A ce titre, un certain nombre d'obligations pèsent sur ce prestataire (A) qui pourra être tenu responsable vis à vis de ses clients et des personnes qui se fient à la signature électronique (B).

A/ Obligations du P.S.C.E.

Le système juridique français précise les obligations juridiques qui pèsent sur les P.S.C.E. dans le cadre du décret du 30 mars 2001.

Pour émettre des « *certificats qualifiés* », les P.S.C.E. doivent fournir un certain nombre de garanties dont les exigences sont prévues à l'article 6 du décret du 30 mars 2001, peu importe dans ce texte que le P.S.C.E. bénéficie d'une accréditation volontaire ou qu'il se conforme à la directive sans passer par le régime d'accréditation lorsqu'il dit délivrer des certificats qualifiés.
Sans entrer dans le détail des prescriptions de l'article 6, nous signalerons que le P.S.C.E. doit utiliser des systèmes et produits fiables tant pour leur fonctionnement que pour la conservation des certificats (article 6-II g et l) et employer du personnel qualifié (article 6-II, e).

115 Article 1. 11 du décret du 30 mars 2001.
116 Ou encore appelée Infrastructure de Gestion de Clés (I.G.C.).

En cas de litige, il aura également à faire la preuve qu'il est suffisamment fiable pour fournir des services de certification (article 6-II, a). Le P.S.C.E. doit disposer des garanties financières suffisantes pour fonctionner en permettant l'indemnisation des utilisateurs autant que de besoin et notamment par le biais de souscription d'une police d'assurance appropriée. S'agissant de la communication et de la reconnaissance avec d'autres P.S.C.E., il conviendra que l'interopérabilité des systèmes de signatures électroniques soit garantie, par exemple en respectant les normes et les standards en vigueur.
Pour que toutes les parties intéressées aux services de certification (ex : les abonnés, les tierces parties au contrat d'abonnement qui se fient aux certificats) puissent être en mesure de les utiliser dans leurs opérations en ligne, il est nécessaire que le P.S.C.E. leur procure une information correcte sur les modalités d'utilisation du certificat, la demande de qualification ainsi que les modalités de contestation et de règlement des litiges (article 6-II, o).
Lorsque le P.S.C.E. fournit à son client des services de gestion de clés, il ne doit ni stocker, ni copier les données afférentes à la création de signature de celui-ci (Article 6-II, i). Cette exigence découle directement d'un principe de sécurité en vertu duquel il faut disposer de deux paires de clés distinctes lorsque l'on entend signer et chiffrer des messages. L'usage d'une seule paire de clés à la fois pour la signature et pour le chiffrement des messages aurait pour conséquence de créer le risque de voir un tiers s'approprier ou reconstituer la clé privée de signature d'une personne et qu'elle se fasse passer pour elle (usurpation d'identité). Dans le cas de signature numérique, la clé privée doit rester secrète et sous le "*contrôle exclusif*" du signataire. Pour les clés de confidentialité, en revanche, le P.S.C.E. peut être amené à les conserver dans l'hypothèse où un client, suite à la perte de sa clé, lui demanderait de la reconstituer (service de recouvrement de clé de confidentialité) pour être en mesure d'accéder à l'ensemble des fichiers qu'il aurait antérieurement chiffrés.

Dans toute Infrastructure à clé publique (I.C.P.), l'enregistrement des abonnés aux services de certification s'effectue par l'entremise d'Autorités d'enregistrement (A.E.). L'enregistrement peut s'effectuer soit en ligne et les pièces justificatives de l'identité sont envoyées par voie postale (pièces d'identité, extrait K-Bis, et autres quittances attestant du domicile), soit de visu (face-à-face) aux bureaux ou aux agents prévus à cet effet (sur présentation des pièces justificatives).
Cette opération est très importante car elle permet de vérifier l'identité conformément aux exigences posées par le décret (article 6-II, m). Concernant l'exactitude des informations que le certificat doit contenir, il faut reconnaître qu'elles ne peuvent que résulter des pièces fournies lors de l'enregistrement (ex : pièce d'identité, quittance).
En cas de falsification, tant matérielle qu'intellectuelle, du ou des document(s), ou d'informations obsolètes, l'A.E. ne devrait pas être responsable des informations inscrites dans le certificat. En effet, actuellement les enregistrements s'effectuent le plus souvent en ligne et par l'envoi des pièces justificatives par courrier. Mais ce problème de faux documents serait le même dans le cadre des procédures d'enregistrement en face à face. L'A.E. ne peut garantir que l'exactitude formelle des informations au vu des pièces transmises et non leur exactitude sur le fond.

Cette entité ne souscrit pas d'engagement juridique envers les clients, elle est uniquement en relation contractuelle avec l'A.C. Cette dernière génère le certificat numérique d'identification sous sa seule responsabilité et à ce titre elle s'engage à remplir certaines obligations essentielles (art. 33 de la LCEN), c'est à dire établir et garantir le lien qui existe entre une personne et une paire de clés asymétriques dont elle est titulaire. En outre, le P.S.C.E. crée et assure, sous sa responsabilité, le fonctionnement d'un service d'annuaire (rapide et sûr) et d'un service de révocation (fiable et immédiat) (article 6-II, c).

Concernant les données à caractère personnel contenues dans le certificat, la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des

traitements de données à caractère personnel modifie la loi n° 78-17 du 6 janvier 1978 relative à l'informatique aux fichiers et aux libertés prévoit dans son article 33 :« *sauf consentement exprès de la personne concernée, les données à caractère personnel recueillies par le prestataire de services de certification électronique pour les besoins de la délivrance et de la conservation des certificats liés aux signatures électroniques doivent l'être directement auprès de la personne concernée et ne peuvent être traitées que pour les fins en vue desquelles elles ont été recueillies* »[117].

B/ responsabilité du P.S.C.E

L'article 33 de la loi pour la confiance dans l'économie numérique qui transpose l'article 6 de la directive européenne du 13 décembre 1999 et par là, la présomption de responsabilité pour les P.S.C.E. qui délivrent des certificats présentés comme qualifiés ne donne lieu qu'à quelques modifications qui se retrouvent notamment dans le régime de responsabilité du P.S.C.E.

Ainsi, lorsqu'il entend délivrer un certificat qualifié, le P.S.C.E. ne pourra pas exonérer sa responsabilité en cas d'inexécution ou de mauvaise exécution.

Cet article prévoit :
« *Sauf à démontrer qu'ils n'ont commis aucune faute intentionnelle ou négligence, les prestataires de services de certification électronique sont responsables du préjudice causé aux personnes qui se sont fiées raisonnablement aux certificats présentés par eux comme qualifiés dans des conditions fixées par décret en Conseil d'Etat lorsque :*

1° Les informations contenues dans le certificat, à la date de sa délivrance, étaient inexactes ;

2° Les données prescrites pour que le certificat puisse être regardé comme qualifié étaient incomplètes ;

3° La délivrance du certificat n'a pas donné lieu à la vérification que le signataire détient la convention privée correspondant à la convention publique de ce certificat ;

4° Les prestataires n'ont pas fait procéder à l'enregistrement de la révocation du certificat et tenu cette information à la disposition des tiers.»

Par conséquent, pour les certificats présentés comme qualifiés par le P.S.C.E., le lien de causalité est présumé entre la faute (l'inexécution d'une obligation essentielle) et le préjudice (un manque à gagner pour le tiers qui se fie ou le signataire), sauf à démontrer qu'il n'a commis aucune faute intentionnelle ou qu'il n'a pas été négligent. Il en va de même pour les P.S.C.E. qui ont fait l'objet d'une qualification volontaire. **La seule différence se situe dans la difficulté technique pour le demandeur de démontrer la faute commise par un P.S.C.E. qualifié.**

Selon ce même article 33, « *les prestataires ne sont pas responsables du préjudice causé par un usage du certificat dépassant les limites fixées à son utilisation ou à la valeur des transactions pour lesquelles il peut être utilisé, à condition que ces limites figurent dans le certificat et soient accessibles aux utilisateurs*.». Le terme « *accessible* » pourrait être interprété en mettant en avant le fait que les limites d'utilisation ou de valeur du certificat doivent être perçues de façon à éviter toute confusion (par exemple : engageant l'entreprise à l'exclusion de son employé en son nom personnel). En pratique, il pourrait s'agir d'une indication permettant à la personne qui reçoit un certificat et un message signé de remarquer les limites d'utilisation du certificat, sans qu'il soit nécessaire que ce soit tout le contenu de cette limite lui-même qui soit affiché. Actuellement, les certificats électroniques ne contiennent pas de champs prévus pour inscrire les limites d'utilisation et de valeur – et cela

[117] V. E. Caprioli, *Loi du 6 août 2004 : commerce à distance sur Internet et protection des données à caractère personnel*, Comm. Comm. Elect., Février 2005, n°2, p. 24-28.

n'est pas sans incidence sur les risques qui pèsent sur les P.S.C.E. Il faut donc que ce tiers puisse contrôler de manière simple et systématique la liste des certificats révoqués qu'aura émis le P.S.C.E, vérifier la signature (ce qui sous entend l'intégrité du message) et le certificat électroniques.

Enfin, il devra archiver l'ensemble de ces éléments, pour pouvoir apporter la preuve de ces diligences dans le cadre d'un éventuel contentieux.

Le dernier alinéa de l'article 33 dispose également que le P.S.C.E devra justifier d'une garantie financière ou d'une assurance « *garantissant les conséquences pécuniaires de sa responsabilité civile* ». Cette exigence, peut être d'une application pratique délicate dès lors que le risque financier est relatif au montant et à la nature spécifique à chaque préjudice ainsi qu'aux limites contenues dans le certificat. C'est donc une appréciation *in concreto* qui devra être effectuée.

En ce qui concerne les signatures qui se fondent sur des certificats non qualifiés ainsi que pour toutes les autres obligations, c'est le droit commun qui s'applique : les articles 1382 et suivants du code civil pour la responsabilité délictuelle et le droit des obligations contractuelles pour les rapports entre le P.S.C.E. et son client (son abonné).

La signature électronique dans la sphère publique

Les télé-procédures à l'égard des usagers, professionnels ou particuliers, se sont développées tout au long de la dernière décennie (on pense ici aux déclarations de la TVA[118], auprès des URSSAF ou encore, pour le grand public, à celle de l'impôt sur le revenu). Leur essor s'effectue également dans les relations entre l'Etat et les collectivités locales, notamment dans le cadre du « *contrôle de légalité par voie électronique* »[119].

La facture électronique signée a été introduite par l'article 17 de la loi de finances rectificative pour 2002[120], qui transpose la directive n°2001/115 du 20 décembre 2001 modifiant la directive n°77/388/CEE en vue de simplifier, moderniser et harmoniser les conditions imposées à la facturation en matière de taxe sur la valeur ajoutée et pose le régime des factures électroniques, notamment le recours aux dispositifs de signature électronique.
Les modalités d'application de la facturation électronique ont été précisées dans l'instruction du 7 août 2003[121]. Il s'agit ici d'une signature électronique utilisant un certificat de serveur (signature de la personne morale) et non d'une signature électronique (certificat de personne physique) au sens juridique de signer un acte.

Le recours à la signature électronique se diffuse également dans d'autres pans du droit. Ainsi, l'Arrêté du 28 août 2006 pris en application du I de l'article 48 et de l'article 56 du code

---

118 Loi n°2002-1576 du 30 décembre 2002, J.O. n° 304 du 31 décembre 2002, p. 22070.

119 V. pour une analyse de la problématique, Anne Cantéro, *Des actes unilatéraux des communes dans le contexte électronique, Vers la dématérialisation des actes administratifs ?,* PUAM, Coll. Collectivités locales, 2002. V. également pour les textes adoptés : la loi n°2004-809 du 13 août 2004 relative aux libertés et aux responsabilités locales, J.O. du 17 août 2004, p. 14545 et s. ; le décret n° 2005-324 du 7 avril 2005 relatif à la transmission par voie électronique des actes des collectivités territoriales soumis au contrôle de légalité et modifiant la partie réglementaire du code général des collectivités territoriales, J.O. du 8 avril 2005, p. 6340 et s. ; l'arrêté du 26 octobre 2005 portant approbation d'un cahier des charges des dispositifs de télétransmission des actes soumis au contrôle de légalité et fixant une procédure d'homologation de ces dispositifs, J.O. du 3 novembre 2005, p. 17289 et s.

120 Loi n°2002-1576 du 30 décembre 2002, JO du 31 décembre 2002.

121 Instruction de la Direction générale des impôts n° 136 du 7 août 2003, 3CA.

des marchés publics et relatif à la dématérialisation des procédures de passation des marchés publics formalisés[122] fait une référence explicite aux articles du Code civil.

L'article 7 de l'ordonnance n° 2005-1516 du 8 décembre 2005 sur les échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives[123] a consacré la possibilité de signer électroniquement tout acte administratif qui requiert une telle signature dans les textes de droit commun[124]. Ce texte prévoit, en outre, l'adoption de deux documents : le Référentiel général de sécurité (qui devrait reprendre les principes de la PRIS en ce qui concerne les signatures électroniques) et le Référentiel Général d'Interopérabilité (RGI)[125].

Certaines questions prospectives ont fait jour concernant la responsabilité de l'Etat en cas de manquement dans la délivrance de certificats (erreur dans les champs du certificat) contenus dans la future C.N.I.E, le cas échéant. A cet égard, les principes classiques de responsabilité administrative pour faute devraient trouver à s'appliquer. Les conditions entourant la responsabilité de l'Etat en qualité d'autorité de certification seraient donc :

- la preuve par la victime de la faute de l'Etat dans le cadre de la procédure de délivrance du certificat (erreur manifeste dans les champs du certificat) ;
- la preuve par la victime du préjudice subi du fait de cette faute. Pour ouvrir droit à réparation, la jurisprudence administrative exige que le préjudice soit certain (comme en droit civil). Certains préjudices matériels qui se traduisent en général par une perte pécuniaire et les préjudices moraux qui sont plus difficilement appréciables sont susceptibles d'ouvrir droit à réparation.
- La preuve du lien de causalité entre la faute et le préjudice. Le fait imputé à la personne publique doit être la cause directe du préjudice subi par la victime pour engager sa responsabilité.

Ces premiers éléments de réflexion devront être complétés d'une étude plus précise en fonction de l'architecture retenue pour le déploiement de la CNIe et des textes spécifiques adoptés en la matière qui pourraient établir un régime de responsabilité particulier.

3- L'identification dans le domaine bancaire

A la suite des attentats intervenus en 2001 et en 2004 aux Etats-Unis et en Europe, la lutte contre le terrorisme et le blanchiment d'argent s'est intensifiée. Afin de combattre cette nouvelle forme de guerre, des règles permettant de lutter efficacement contre le développement de ces réseaux criminels sont élaborées[126]. Elles portent notamment sur le contrôle des flux financiers entre les différents Etats. Le Règlement (CE) n°1781/2006 du Parlement européen et du Conseil du 15 novembre 2006 relatif aux informations concernant le donneur d'ordre accompagnant les virements de fonds a été adopté dans un contexte de lutte contre le blanchiment des capitaux et le financement du terrorisme. Le « *financement du terrorisme* » (défini à l'article 2-1) est le fait, par quelque moyen que ce soit, directement ou indirectement, de fournir ou de réunir des fonds au sens de l'article 1er §4 de la directive 2005/60/CE, c'est-à-dire dans l'intention de les voir utilisés ou en sachant qu'ils seront utilisés, en tout ou en partie, en vue de commettre l'une quelconque des infractions visées

122 V. J.O. du 29 août 2006 p. 12766 et s.

123 J.O n° 286 du 9 décembre 2005 p. 18986.

124 E. A. Caprioli, *Des échanges électroniques entre les usagers et les autorités administratives d'une part, et entre ces dernières d'autre part*, JCP éd. A et CT, 2006, n°1079, p. 432 et s.

125 Décret n° 2007-284 du 2 mars 2007 fixant les modalités d'élaboration, d'approbation, de modification et de publication du référentiel général d'interopérabilité, J.O. du 3 mars 2007 p. 4060 et s.

126 Qui ne seront pas développées ici.

aux articles 1er à 4 de la décision cadre 2002/475/JAI du Conseil du 13 juin 2002 relative à la lutte contre le terrorisme[127]. L'objectif de ce règlement est, selon l'article premier, d'établir « *les règles relatives aux informations sur le donneur d'ordre qui doivent accompagner les virements de fonds, aux fins de prévention, de l'enquête et de la détection des activités de blanchiment de capitaux et de financement du terrorisme* ».

La traçabilité et l'identification des clients par les établissements bancaires sont deux éléments essentiels dans la lutte contre le blanchiment et le financement du terrorisme au niveau communautaire. Cette exigence est reprise au niveau national.

Ainsi l'article L. 563-1 du Code monétaire et financier dispose :

« *Les organismes financiers ou les personnes visées à l'article L. 562-1 doivent, avant de nouer une relation contractuelle ou d'assister leur client dans la préparation ou la réalisation d'une transaction,* ***s'assurer de l'identité de leur cocontractant par la présentation de tout document écrit probant.*** *Ils s'assurent dans les mêmes conditions de l'identité de leur client occasionnel qui leur demande de faire des opérations dont la nature et le montant sont fixés par décret en Conseil d'Etat. Les personnes visées au 8 de l'article L. 562-1 satisfont à cette obligation en appliquant les mesures prévues à l'article L. 565-1.*

Ils se renseignent sur l'identité véritable des personnes avec lesquelles ils nouent une relation contractuelle ou qui demandent leur assistance dans la préparation ou la réalisation d'une transaction lorsqu'il leur apparaît que ces personnes pourraient ne pas agir pour leur propre compte.

Les organismes financiers et les personnes mentionnés à l'article L. 562-1 prennent les dispositions spécifiques et adéquates, ***dans les conditions définies par un décret, nécessaires pour faire face au risque accru de blanchiment de capitaux qui existe lorsqu'elles nouent des relations contractuelles avec un client qui n'est pas physiquement présent aux fins de l'identification ou lorsqu'elles l'assistent dans la préparation ou la réalisation d'une transaction.*** ».

L'article R. 563-1 du Code monétaire et financier (introduit par le décret n°2006-736 du 26 juin 2006 (JO du 27 juin 2006) est à cet égard encore plus explicite :

« *I. - Est considérée comme client occasionnel pour l'application de l'article L. 563-1 la personne qui s'adresse à un organisme financier ou à une personne mentionnés à l'article L. 562-1 dans le but exclusif de réaliser une opération ponctuelle. Ces organismes financiers et ces personnes vérifient l'identité de leur client occasionnel avant de réaliser une opération ponctuelle lorsque son montant excède 8 000 euros, qu'elle soit effectuée en une seule ou en plusieurs opérations entre lesquelles un lien semble exister.*

Cependant, lorsqu'ils réalisent une opération de transfert de fonds pour un client occasionnel, lorsqu'ils ouvrent un compte ou un livret ou offrent des services de garde des avoirs ou lorsqu'ils concluent tout contrat d'assurance ou de capitalisation donnant lieu à la constitution d'une provision mathématique, les organismes financiers procèdent à la vérification d'identité quel que soit le montant.

Les personnes mentionnées au 9 et au 13 de l'article L. 562-1 ne procèdent à l'identification qu'en cas de règlement en espèces d'un montant supérieur à 3 000 euros.

Pour les sommes ou opérations mentionnées à l'article L. 562-2, la vérification d'identité a lieu même si le montant de l'opération ponctuelle est inférieur au seuil.

127 J.O.C.E. L. 164, du 22 juin 2002, p. 3.

II. - Pour l'application de l'article L. 563-1, les organismes financiers et les personnes mentionnés à l'article L. 562-1 ***vérifient l'identité d'une personne physique par la présentation d'un document officiel en cours de validité portant sa photographie. Ils conservent la copie de ce document ou ses références. Les mentions relatives à l'identité à vérifier comprennent les nom, prénoms ainsi que les date et lieu de naissance. Outre ces mentions, les références à conserver incluent la nature, le numéro, les date et lieu de délivrance du document ainsi que le nom de l'autorité ou personne qui l'a délivré ou authentifié.***

[…]

*III. - La vérification de l'identité des personnes physiques peut ne pas avoir lieu en présence de la personne à identifier. Dans ce cas****, outre l'obtention d'une copie du document exigé au II,*** *les organismes financiers et les personnes mentionnés à l'article L. 562-1 prennent les dispositions spécifiques et adéquates nécessaires, en adoptant des mesures parmi l'une au moins des quatre catégories de mesures suivantes :*

1º Obtenir des pièces justificatives supplémentaires permettant d'établir l'identité du cocontractant ;

2º Mettre en oeuvre des mesures de vérification et de certification de la copie de la pièce officielle d'identité mentionnée au II par un tiers indépendant de la personne à identifier ;

3º Exiger que le premier paiement des opérations soit effectué par un compte ouvert au nom du client auprès d'un organisme financier établi dans un Etat membre de la Communauté européenne ou dans un autre Etat partie à l'accord sur l'Espace économique européen ;

4º Obtenir une attestation de confirmation de l'identité d'un client de la part d'un organisme financier établi dans un Etat membre de la Communauté européenne ou dans un autre Etat partie à l'accord sur l'Espace économique européen. L'attestation mentionne les éléments d'identification cités au II, est adressée directement par cet organisme à la personne demandant l'identification et précise le nom et les coordonnées du représentant de l'organisme l'ayant délivrée. Cette attestation peut également être obtenue d'un organisme financier établi sur le territoire d'un Etat figurant sur la liste établie conformément aux dispositions du quatrième alinéa du IV, qui est en relation d'affaires suivie avec l'organisme financier ou la personne mentionnés à l'article L. 562-1 établis en France et qui déclare avoir procédé à des mesures d'identification équivalentes à celles applicables en France. ».

→ Ainsi, la présentation (ou la transmission) d'un document d'identité officiel en cours de validité est un préalable nécessaire à la conclusion de tout contrat bancaire. On voit ici l'intérêt d'une CNIe pour les établissements financiers : l'utilisation d'un certificat permettrait une vérification d'identité à distance et faciliterait le développement des services bancaires en ligne, autorisés depuis l'ordonnance n°2005-648 du 6 juin 2005 relative à la commercialisation à distance de services financiers auprès des consommateurs[128].

[128] J.O. du 7 juin 2005, p. 10 002 ratifiée par le décret n°2005-1450 du 25 novembre 2005, p. 18634 et s.

VI- Etude sur la signature électronique dans le contexte de l'identité numérique : bases normatives

Le lecteur trouvera dans ce chapitre **les bases normatives** sur lesquels s'appuient un certain nombre d'éléments ressortis des interviews réalisés. Il ne prétend pas fournir une information exhaustive, ni se substituer à la documentation largement disponible, en particulier sur le site web de la DCSSI et de l'administration électronique.

1- Norme versus spécification

Selon la Cour de Cassation, une norme consiste en « une codification écrite des règles de l'art » [129]. Elle détermine et décrit un socle de règles techniques sur lequel les acteurs économiques peuvent s'appuyer. Une norme n'a donc pas de pouvoirs directement contraignants. En revanche, elle offre un certain nombre de repères (modalités, conditions, moyens) pour arriver à la finalité qu'elle s'est fixée. On utilise d'autres appellations telles que spécification à caractère normatif ou standard pour tout autre document de référence.

2- Le cadre technique de la signature électronique

Les documents les plus importants fixés par le cadre réglementaire présenté au précédent chapitre portent sur :

1. les éléments de sécurité (profils de protection) des différents composants des outils de création de certificats et des produits de signature électronique : accords d'ateliers CEN sous les références CWA 14167-1, CWA 14167-2 et CWA 14169
2. les politiques de sécurité requises pour les différents opérateurs de l'infrastructure PKI : tiers de confiance émetteurs de certificats notamment et connu sous la référence TS 101456 v1.2.1.

En outre, ce dispositif repose sur l'application de normes fondamentales de sécurité, notamment :

- des spécifications relatives aux algorithmes de cryptage (norme internationale ISO)
- la structure du certificat : la recommandation de l'UIT connue sous la référence X509V3, qui est également une norme internationale ISO.

Les références précises des textes indispensables à la signature électronique sont explicitées dans un mémento édité par la DCSSI et disponible en téléchargement sur le portail de la Direction Centrale de la Sécurité des Systèmes d'Information :
http://www.ssi.gouv.fr/site_documents/sigelec/signature-memento-v0.94.pdf

La lecture de ce document est recommandée pour toute personne souhaitant mettre en place un dispositif de signature électronique.

De ce fait, les documents définis par l'EESSI n'ont pas le statut de normes, mais représentent une collection de documents de référence dont quelques-uns seulement ont été référencés au JOCE. La version transposée du standard ETSI TS 101456 en accord AFNOR sous la référence AC Z74-400, a été référencée par décret dans la réglementation française.

[129]) Cass. Civ3 du.4 février 1976; N° de pourvoi : 74-12643.

Authentification

La recommandation X509 définit 2 niveaux d'authentification : l'authentification simple et l'authentification forte. Suivant cette recommandation, l'authentification impose un chiffrement des informations. Elle ne fournit cependant aucune préconisation concernant l'algorithme de cryptage à mettre en œuvre.

La spécification RFC 3039, établie par l'IETF (organisation de standardisation de l'Internet), précise quant-à-elle un profil de certificat de signature électronique qualifié en conformité avec l'usage dans le cadre de la directive signature électronique. Elle exige la remise en face-à-face du certificat.

Par ailleurs, il est généralement admis que l'authentification forte impose un support physique pour le certificat (type carte à puce), mais cette assertion ne repose pas sur une base normative.

Code PIN ou NIP

Le NIP Numéro d'Identification Personnel également appelé Code PIN (Personal Identification Number) est défini par la norme européenne ETSI « Global System for Mobile communications » en 1991. Pour le domaine bancaire, la norme internationale ISO 9564 traite spécifiquement de la gestion et la sécurité du numéro personnel d'identification (PIN)

Valeur des transactions financières

La réglementation sur la signature électronique autorise qu'une valeur limite de transactions financières puisse être attribué à un certificat.

La spécification européenne ETSI TS 101 862 V1.1.1 indique comment coder la limite sur la valeur des transactions financières dans laquelle le certificat qualifié peut être utilisé.

Enfin, la spécification RFC 3280 établie par l'IETF, est un profil de la recommandation X509 pour l'usage d'une infrastructure à clé publique sur l'internet.

➔ compte tenu de ces éléments, il ne nous semble pas opportun de retenir une suggestion qui viserait à modifier la façon de coder la valeur limite de transaction financière.

Niveau d'évaluation pour les certificats

La norme ISO/IEC 15408 fixe des critères communs pour l'évaluation des produits de sécurité. Il s'en déduit une classification en 7 niveaux "*Evaluation Assurance Level*" : EAL 1 à EAL 7. Des sous-niveaux ont été établis, le caractère +, par exemple EAL2+ signifiant que le niveau 2 a été renforcé.

➔ Il faut faire attention car la notion de "classe (ou catégorie) de certificat" à laquelle font pourtant référence certains guides, des ouvrages, ou les documentations commerciales de plusieurs produits, ne repose de fait sur aucune base normative.

3- La politique de référencement de sécurité de l'administration PRIS

L'administration française a établi pour ses besoins propres, et pour les organismes étant amenés à travailler dans le cadre de commandes publiques, une politique de référencement de sécurité PRIS version 2.1 de novembre 2006. Cette politique s'applique en particulier à la dématérialisation des échanges électroniques.

Les préconisations de la PRIS concernent l'usage d'architectures à clé publique (PKI). La PRIS définit 3 niveaux de sécurité qui vont de une étoile à trois étoiles. Le niveau 3*** impose l'authentification forte.

Le tableau ci-dessous[130] précise bien le mécanisme de mise en œuvre des certificats,

PSCe	***	**	*
Enregistrement	Face à face	Face à face	-Envoi d'un dossier papier ou électronique - ou communication par le porteur d'un élément permettant de l'identifier dans une base de données administrative
Remise/acceptation d'un certificat	-Remise en face à face si non fait lors de l'enregistrement - Si l'AC ne génère pas la bi-clé, vérification que le certificat est bien associé à la clé privée correspondante (chargement à distance sur une carte à puce). - Acceptation explicite du certificat par le porteur.	-Remise en face à face si non fait lors de l'enregistrement - Si possible, acceptation explicite du certificat par le porteur, au minimum, acceptation tacite à partir d'une date de remise suffisamment fiable.	- Remise par message électronique ou téléchargement. - Acceptation tacite.

et leur positionnement élevé dans le contexte de la future CNIe, notamment leur acceptation explicite par le porteur via la génération d'un code secret et leur consignement sur une carte à puce.
La carte d'identité hébergera deux certificats, donc deux couples de bi-clés, l'un servant à s'authentifier, avec présomption de fiabilité, l'autre, à valider une transaction en marquant son consentement. Il est appelé certificat de signature dont la valeur juridique découle de la Directive Européenne 1999/93.

Notons qu'actuellement, la réglementation précise que la durée de validité d'un certification 3 étoiles est de 3 ans, et que son renouvellement la première fois peut se faire sans face à face. Le second renouvellement, après 6 ans, exige de nouveau le face à face.

La CNIE de son coté, envisage des certificats d'une durée équivalente à la carte, soit 5 ans.

➔ En ce qui concerne les services de confiance, et donc en particulier les prestataires de Services de certification électronique, la PRIS impose pour les niveaux 2étoiles et 3 étoiles un contrôle de l'identité en face-à-face pour la validation initiale de l'identité du porteur ou

130 http://synergies.modernisation.gouv.fr/IMG/pdf/070125_presentation_PRIS.pdf Présentation PRIS V2.1 Ministère du Budget et de la Réforme de l'Etat.

une méthode équivalente, par exemple une signature avec un certificat et un outil de niveau 3 étoiles.

➔ Un certificat PRIS à 3 étoiles, dès lors qu'il sera utilisé dans le cadre d'une infrastructure de sécurité adéquate, aura un niveau de sécurité équivalent à une signature électronique sécurisée.

4- Conséquences pour l'usage des titres délivrés par différentes sphères de confiance

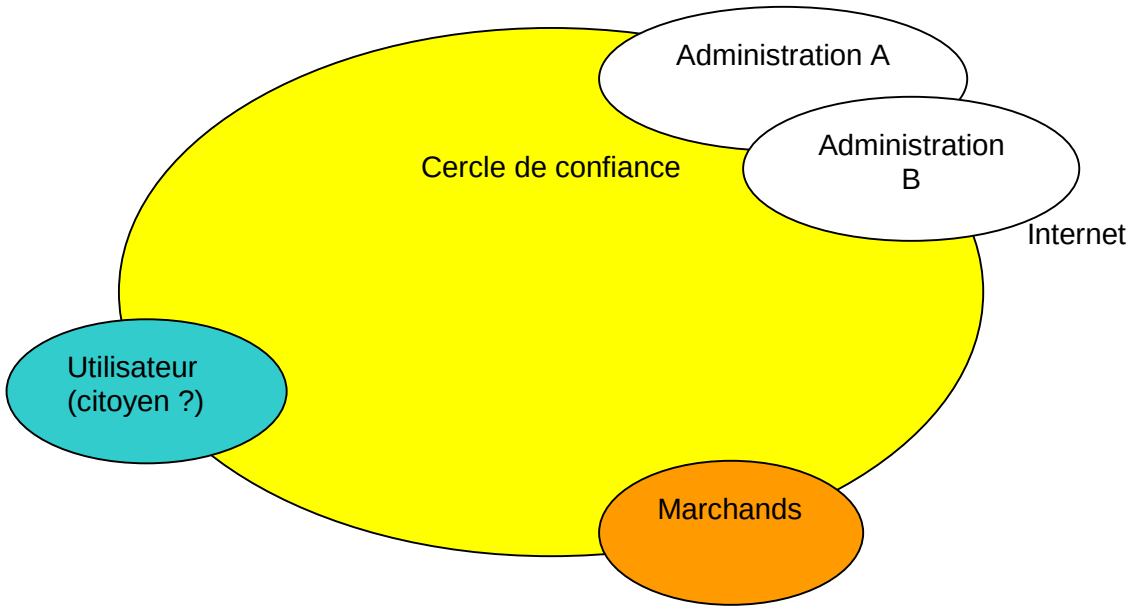
Les exigences relatives à la procédure de délivrance des certificats ont des conséquences importantes en terme d'impact sur les marchés :

➔ Une carte d'identité avec certificat électronique est un document délivré en face-à-face et peut prétendre au niveau PRIS ***. Elle pourra donc être utilisée dans le cadre d'une procédure mettant en œuvre une signature électronique sécurisée, dès lors que cette procédure intègrera les autres éléments de sécurité requis au niveau de l'infrastructure PKI : dispositif sécurisé de création de signature électronique et dispositif de vérification de signature électronique.

➔ Une carte Sésame Vitale, même avec certificat électronique, serait remise par la Poste. N'étant pas délivrée en face-à-face, elle ne pourra être utilisée à elle seule dans un processus de signature électronique sécurisé.

➔ Les cartes de transports type NAVIGO comportent souvent des éléments de biométrie, notamment la photo de l'abonné. Cependant, leur procédure de délivrance ne suppose pas aujourd'hui le face à face. En conséquences, elles ne sont pas appropriées pour être utilisées dans un processus de signature électronique sécurisé, même si elles comportent un certificat électronique.

Cercles de confiance
Les spécialistes de la sécurité utilisent cette notion pour désigner un ensemble de services auquel on donne accès dès lors que l'on dispose des droits nécessaires. Concrètement, il peut s'agir du système d'information d'une entreprise, de services bancaires, d'un portail de l'administration, d'un ensemble de commerçants fédérés sur l'Internet, etc.



Pour accéder à un cercle de confiance, il faut donc s'authentifier et disposer des droits nécessaires. Bien évidemment, les droits attribués se limitent à l'usage au sein du cercle de confiance considéré et ils ne sont pas exploitables à l'extérieur du cercle de confiance.

L'étanchéité entre différents cercles de confiance peut être exigible pour différentes raisons et notamment pour limiter le risque de propagation des données personnelles au delà de ce qui est nécessaire. Le chapitre protection des données personnelles revient sur ce point avec le projet « Liberty Alliance » pour indiquer comment cette architecture répond à cette exigence.

5- Normalisation des cartes d'identité

La plupart des titres émis par les états font l'objet de travaux de normalisation internationaux et/ou européens: passeport, visa, permis de conduire, etc.

Plusieurs pays ont mis en place ou envisagent de mettre en place des cartes d'identité nationales.

A la différence d'autres titres comme le passeport ou le visa, la normalisation des cartes d'identité nationale ne se fait pas à l'échelon international.

Sous l'impulsion d'acteurs français, le Comité européen de Normalisation a mis en chantier une spécification technique ECC European Citizen Card au sein de son comité technique TC 224 qui s'occupe de cartes à puces, et également de signature électronique. Cette spécification, dont la référence est CEN TS 15580 et dont les deux premières parties sont en cours de publication, couvre les champs suivant :

- Cartes avec Identification, Authentification et Signature électronique (IAS),
- Carte avec contact, mais option sans contact possible,
- Évaluation de sécurité conforme au CWA 14169,
- Garantie de durabilité,
- Biométrie optionnelle.

Dans une seconde étape, il est envisagé de lui donner le statut de norme européenne.

➔ Une carte d'identité conforme à la TS 15580 répondrait aux critères exigibles pour la délivrance de certificats de signature électroniques qualifiés. Il sera également possible d'utiliser cette carte dans d'autres contextes avec signature électronique, par exemple des cartes de vie quotidienne.

Le Comité CEN TC 224 normalise par ailleurs les résultats du groupe Area K de l'EESSI qui concerne l'utilisation de signature électronique sur des supports cartes à circuits intégrés. Ce travail concerne notamment la reprise en normes, des accords d'atelier de la série CWA 14180.

La spécification IAS

En France, le groupement GIXEL a travaillé avec l'administration DGME à une spécification d'exigence pour un socle commun Carte qui permettait l'Identification, l'Authentification, et la Signature électronique (IAS).

Le socle IAS est conforme aux standards suivants :

- Normes ISO 7816 , spécification générique pour les cartes à circuits intégrées
- CWA 14169 : PP Secure Signature Creation Device
- CWA 14890 E-Sign Area K : Application Interface for Smart Card used as Secure Signature Creation Device, Part 1 et 2
- ISO 7816-15, PKCS#15 pour certificats X509 V3, PRIS V2 et objets cryptographiques PRIS V2

Actuellement dans la première version, seul le mode contact est pris en compte.

La spécification IAS 1.0.1 Premium est disponible sur le site du Gixel Onglet Cartes à puce.

Cette spécification IAS a servi de base à la spécification technique ECC European Citizen Card.

Autres travaux de standardisation

Par ailleurs, d'autres efforts de normalisation sont à signaler en raison de leur connexion avec ce sujet, bien qu'il présente une moindre importance pour cette étude :

- Pour le secteur santé, l'ISO a publié sous la référence ISO 20301 une spécification de carte santé. L'Europe vient d'engager avec l'impulsion de la Commission Européenne un projet de carte santé pour travailleur migrant (atelier eHIC).

- Un atelier CEN (WS eAuthentification) a développé une spécification de carte à puce visant l'authentification forte dans un contexte d'usage en réseau (CWA15264 : 2005)

- Un atelier CEN (WS WS/MMUSST) a développé une spécification de carte à puce multi-applications pour des applications urbaines (CWA 15535:2006). Toutefois, cette spécification ne prévoit pas l'usage de la signature électronique.

6- Protection des données personnelles

La protection des données personnelles est réglementée en France par la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés qui institue la CNIL (Commission Nationale de l'Informatique et des Libertés). En Europe, la protection des données personnelles est régie par les directives suivantes : 95/46/CE, stockage des données, 2002/58/CE, communications électroniques de ces données.

L'application de cette législation impose un contrôle strict de l'usage des données à caractère personnel susceptibles d'être collectées. Au plan normatif, on distinguera les approches suivantes :

- **Management et bonnes pratiques**

Cet axe de normalisation est cité pour une bonne compréhension des enjeux et de l'étendu des travaux, mais ne s'applique pas directement à l'identité numérique et à la signature électronique.

- Etablir un système de management des données personnelles : seuls le Canada et le Japon ont choisi cette approche qui s'apparente aux systèmes mis en place pour la qualité (ISO 9000) ou l'environnement (ISO 14000).
Une tentative pour établir une norme internationale de management des données personnelles a échoué à l'ISO à la fin des années 1990. En effet, une telle approche ne semble pas généralisable. Dans les pays, qui, comme la France, ont mis en place une réglementation spécifique, l'autorité de contrôle (la CNIL en France), apparaît assez réticente à cette approche.

- Plusieurs guides de bonnes pratiques ont été développés par le Comité Européen de Normalisation dans le cadre d'un atelier traitant de ces questions. Ces guides ne présentent pas un caractère technique et visent à aider les organisations dans des démarches telles que l'audit de données personnelles. En France, le correspondant CNIL dans les organisations pourrait trouver intérêt à cette approche.

L'ISO (JTC 1 /SC 27) vient de décider de reprendre ces questions sous l'angle de la sécurité de l'information.

- **Standards techniques**

Cet axe de normalisation concerne directement les questions d'identité numérique et de signature électronique.

- Des systèmes déclaratifs relatifs à une politique en matière d'utilisation de données personnelles ont fait l'objet d'efforts de standardisation et, en particulier, la spécification P3P du consortium W3C.
Dans sa version initiale, P3P permet à une entreprise de déclarer à travers son serveur Web sa politique, en matière de protection des données personnelles, de façon codifiée. L'utilisateur peut indiquer ses préférences en matière de gestion de ses données personnelles, par exemple dans son navigateur internet.

Le modèle P3P devrait migrer vers un dispositif plus sophistiqué pour intégrer les évolutions des usages et la sophistication croissante des échanges sur l'Internet. Par exemple il pourrait s'agir d'y adjoindre des langages de négociation de politiques de protections de données personnelles entre serveurs.
En matière de réseau, l'IETF a développé un standard (statut RFC) spécifique au transport d'information à caractère personnel. Un tel standard pourrait être utilisé dans le cadre de l'exploitation de réseaux téléphoniques de nouvelles générations.

➔ cette approche ne prend pas en compte la notion d'identité ni de certificat électronique.

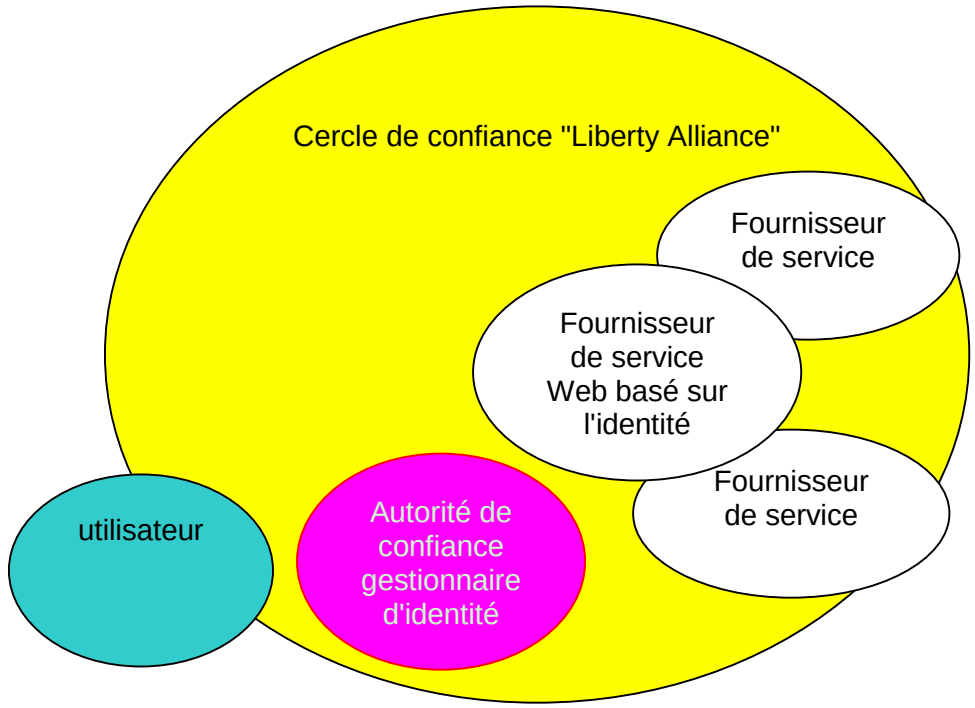
- Des documents relatifs à des techniques d'anonymisation ont été produits dans certains secteurs (santé), et visent à limiter les risques de propagation de données à caractère personnelles.

- Des techniques de pseudonymisation, visant à substituer des données non signifiantes à des données à caractère personnel.

➔ ces approches sont utilisables dans le contexte de l'identité sur les réseaux

- **La fédération d'identité**

A la différence d'un modèle propriétaire d'accès à un cercle de confiance comme Microsoft Passeport, le consortium Liberty Alliance propose un cadre standardisé pour une architecture de services Web visant à permettre l'établissement de cercles de confiance à travers une fédération d'identité.



Ce modèle nous semble actuellement l'approche la plus aboutie en terme de standardisation pour la gestion de données d'identité[131] sur l'internet,[132].

Le modèle décrit par Liberty Alliance met en œuvre des techniques d'anonymisation et de pseudonymisation et s'appuie sur les standards les plus courants de services Web : la spécification SOAP développé par le W3C et les protocoles standardisés au sein du consortium OASIS tels que SAML.

Un profil particulier LECP (Liberty-Enabled Client or Proxy) intègre un modèle de protocole de Web services visant un faible transfert de connaissance au sein d'un même cercle de confiance.
Cette architecture fait appel à un tiers de confiance qui détient pour l'utilisateur, certaines données personnelles et fait un lien entre le propriétaire de ces données et un demandeur ; par exemple, un commerçant qui propose un service qui requière que l'utilisateur soit majeur pour consommer.

---

131 A l'opposé de la fédération d'identité, la société Microsoft a développé un modèle propriétaire de cercle de confiance sur les réseaux, dans le cadre de son initiative Microsoft Passport.

132 sachant que d'autres modèles existent : par exemple, en entreprise, la gestion des droits d'accès au sein de cercles de confiance repose souvent sur un annuaire conforme aux recommandations X500 ou au standard LDAP d'IETF.

Dans l'architecture Liberty Alliance, il est possible d'autoriser une personne à utiliser un ou plusieurs pseudonymes et de signer électroniquement les informations d'identité fournies par le tiers de confiance. Toutefois, autoriser un particulier à faire usage de plusieurs pseudonymes ne fait pas l'unanimité.

➔ L'utilisation de certificats X509 en possession d'un utilisateur ou d'un tiers (par exemple une banque), est compatible avec ce modèle d'architecture.

A l'avenir, un cadre tel que celui proposé par le consortium Liberty Alliance, aura besoin d'être complété : des travaux sont notamment proposés pour interconnecter plusieurs cercles de confiance et permettre, par exemple, à un utilisateur reconnu par un premier cercle de confiance, d'accéder à un deuxième cercle de confiance avec le même niveau de sécurité quant à la gestion de ses données.

7- Biométrie

La biométrie est une technique d'identification d'une personne à partir d'une correspondance entre certaines caractéristiques biologiques et leur codage dans un fichier logique. Les mesures prises à la suite des évènements du 11 septembre 2001 ont conduit à développer une normalisation de ces techniques au sein de l'ISO/CEI JTC1/TC 37.

Par ailleurs, l'Organisation Internationale de l'Aviation Civile (OACI) spécifie les éléments biométriques à intégrer sur les passeports et les visas. Ces spécifications sont intégrées dans les normes développées au sein du comité ISO/CEI JTC 1 SC 17/ WG 3.

les sujets traités par la normalisation en matière de biométrie sont les suivants :

- Interfaces logicielles :
  - ✓ CBEFF
  - ✓ BioAPI
  - ✓ Protocole d'échanges de données

- Formats d'échanges de données :
  - ✓ Empreintes digitales
  - ✓ Visage
  - ✓ Iris
  - ✓ Signature (scripturale)

- Profils d'application
- Méthodes de tests et d'évaluation

Comme il a été dit, la carte d'identité devrait intégrer des éléments de biométrie qui sont ceux définis par l'OACI.

➔ Il n'est pas envisagé en France[133] de pouvoir exploiter à fin d'authentification, au sein de cercles de confiance, les données intégrées dans la carte. Leur usage sera strictement limités aux autorités de contrôle dans les conditions prévues par la loi.

[133] Dans certains pays, par exemple la Grande Bretagne, il est envisagé d'ouvrir à leur demande la biométrie à certains acteurs tels que les banques.

8- Autres travaux

- **Signature XML**

Le consortium W3C a publié un ensemble de recommandations sous l'appellation XML signature. Elles visent à permettre l'usage de signature électronique dans un contexte XML pour authentifier des transactions électroniques sur une longue période. Cette technique s'appuie sur des certificats X509 et sur une architecture de type PKI.

Ces travaux peuvent s'avérer intéressants dans le cadre des télé-procédures.

VII - Glossaire des technologies mises en œuvre

Il convient de bien distinguer 3 fonctions clés **: l'identification, l'authentification et la signature.**

- *Identification*

L'identification est une opération courante du monde réel qui permet à un individu de faire état de son origine sur la base d'un élément externe. La CNI n'étant nullement obligatoire en France, l'identification peut être réalisée par le biais de tout document pouvant attester de l'origine d'un personne, extrait de naissance, permis de conduire, passeport, mais également sur la base du témoignage d'un tiers.
Par contre, cette identification n'exige pas que soit constitué un lien physique entre la personne et l'élément externe qui atteste de son origine. Il s'agit donc d'un rapport de confiance entre la personne qui témoigne de son identité et celui qui la requiert, sachant que les preuves mises en œuvre – photographie, date de naissance, couleur des yeux, nationalité, témoignage d'un tiers – ne constituent nullement une relation univoque.

- *Authentification*

Dans l'univers de l'économie numérique, il existe rarement un contact physique entre internautes et prestataires de services. Leur relation étant totalement dématérialisée, l'identification traditionnelle basée sur la confiance et les témoignages de bonne foi des parties n'est donc plus réalisable.
L'authentification des parties prend alors le relais sur l'identification physique traditionnelle avec, pour finalité, de vérifier l'identité dont une entité (personne ou machine) se réclame. Généralement cette authentification est précédée d'une identification qui permet à cette entité de se faire reconnaître du système par un élément dont on l'a doté.
S'identifier c'est communiquer une identité préalablement enregistrée, s'authentifier, c'est apporter la preuve de cette identité.

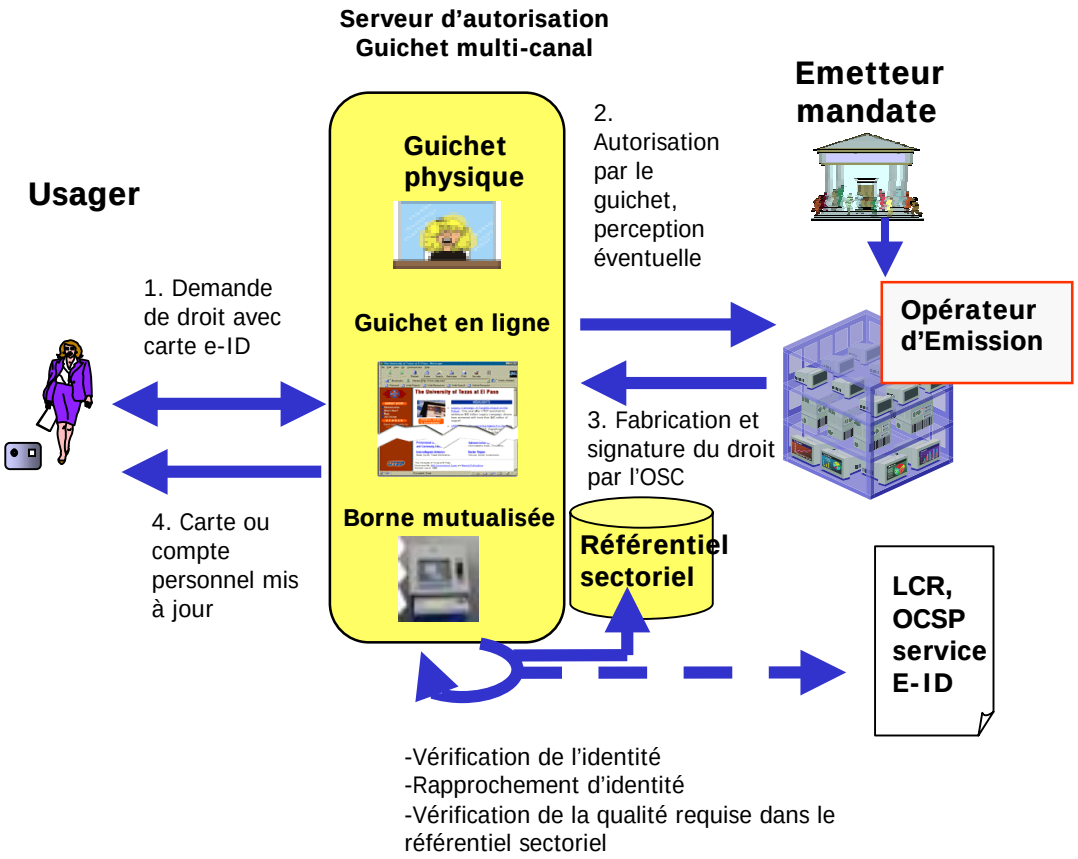
Lorsqu'il accède à un télé-service basé sur des mécanismes cryptographiques asymétriques – architecture de certificats et de bi-clés - le demandeur applique une transformation cryptographique, par sa clé privée, à la requête d'authentification ; le lien entre cette phase d'authentification et les échanges suivants ("ouverture du canal de communication") étant réalisés avec une sécurité équivalente.
Ainsi, la clé privée est-elle stockée et mise en œuvre dans un dispositif d'authentification qui reste sous le contrôle exclusif de l'usager détenteur de cette clé.

Pour pouvoir s'authentifier, l'internaute doit d'abord connecter, s'il en possède un, son dispositif matériel d'authentification (ex : carte à puce ou clé USB avec puce), dans lequel sa clé privée est confinée et protégée en confidentialité, puis saisir son code d'activation. L'application transmet au dispositif les données secrètes du demandeur, qui confirme son identité si le calcul cryptographique de sa valeur d'authentification est exact.

Durant cette transaction, l'internaute génère un certificat électronique que lui a préalablement délivré un prestataire de service de certification électronique (PSCe), liant son identité à sa clé publique. Son accès au service est ainsi légitimé sur la base d'un module de vérification d'authentification.

➔ La CNIe, pourrait être un dispositif d'authentification forte si elle stocke une bi-clé et un certificat d'authentification de niveau ***.
➔ Il faut retenir que l'authentification est une notion associée à l'instantané, et n'assure pas une pérennisation de l'information dans le temps, même si le mécanisme d'authentification forte utilise des technologies à base de clés cryptographiques et de certificats électronique.

Procédure de demande de droit
(exemple : registre du commerce pour les mandataire sociaux, liste électorale, certificat de majorité, permis de chasse, accès e-banking, ...)



Dans le monde dématérialisé de l'économie numérique, les certificats constituent véritablement la procédure la plus efficace d'authentification des internautes, par contre dans le contexte du monde physique et lorsque les individus doivent faire preuve de leur identité – contrôle de police, passage aux frontières – les états planifient des moyens plus poussés faisant appel à des technologies numériques.
Il s'agit généralement de mettre en œuvre un mécanisme de comparaison entre les constantes physiques de l'individu et leur relevé numérique, stocké sur un serveur distant ou le titre d'identité lui-même.
Il s'agit de biométrie, basée soit sur des images (c'est-à-dire une photographie de cette constante physique comme le visage, la main, les doigts, l'iris ou la rétine) soit en un synoptique de cette constante physique. Aujourd'hui ces synoptiques sont produits par des algorithmes propriétaires qui diminuent le volume des donnée sur les puces ou facilitent leur transmission sur réseaux distants. Mais par souci d'interopérabilité, les états préfèrent stocker les images des empreintes.

➔ Il faut retenir qu'en France, l'usage des moyens poussés d'identification mis en œuvre dans les titres (biométrie) sera strictement réservé aux fonctions régaliennes dans des conditions sévèrement contrôlées : forces de police et de gendarmerie.

- *Signature électronique*

Bien que l'authentification forte sur la base de certificats atteste l'identité d'un internaute, elle ne témoigne nullement de son consentement sur un acte donné. Ici intervient la fonction de signature électronique qui, elle aussi, fait appel à une notion de bi-clé et de certificat électronique.

Ce service de confiance permet de garantir l'identité du signataire, l'intégrité du document signé ainsi que la **manifestation du consentement du signataire** quant au contenu des données électroniques ainsi signées.

L'internaute devant signer électroniquement un message ou un fichier, utilise une clé privée asymétrique qu'il détient et met en œuvre dans un dispositif qu'il doit garder sous son contrôle. Une signature électronique peut aussi être requise et activée lorsque l'usager est en relation avec une application d'échange dématérialisé depuis son ordinateur personnel ou une borne d'accès dans un lieu public.

Pour pouvoir signer un message ou des données, l'internaute doit connecter, s'il en possède un, son dispositif matériel de création de signature (ex : carte à puce ou clé USB avec puce), dans lequel sa clé privée est confinée et protégée en confidentialité.
L'application de création de signature, intégrée ou non au télé-service, calcule sur l'ordinateur, ou sur la borne, un condensat du message ou des données à signer et le transmet au dispositif de création de signature par activation du code PIN.
Le calcul cryptographique générant la signature électronique du message ou des données à signer, est ainsi réalisé dans le dispositif de création de signature. Le condensat signé, intitulé signature électronique, est ensuite retourné à l'application.

Pour attester de la légitimité de sa signature électronique, l'usager génère un certificat, préalablement délivré par un prestataire de service de certification électronique (PSCe) qui lie son identité à sa clé publique. Cette vérification s'effectue à l'aide d'un module de vérification de signature.
➔ La CNIe, pourrait devenir un dispositif de signature qualifiée si elle stocke une bi-clé et un certificat de signature de niveau PRIS*** ou qualifié.

- *Certificats et signatures*

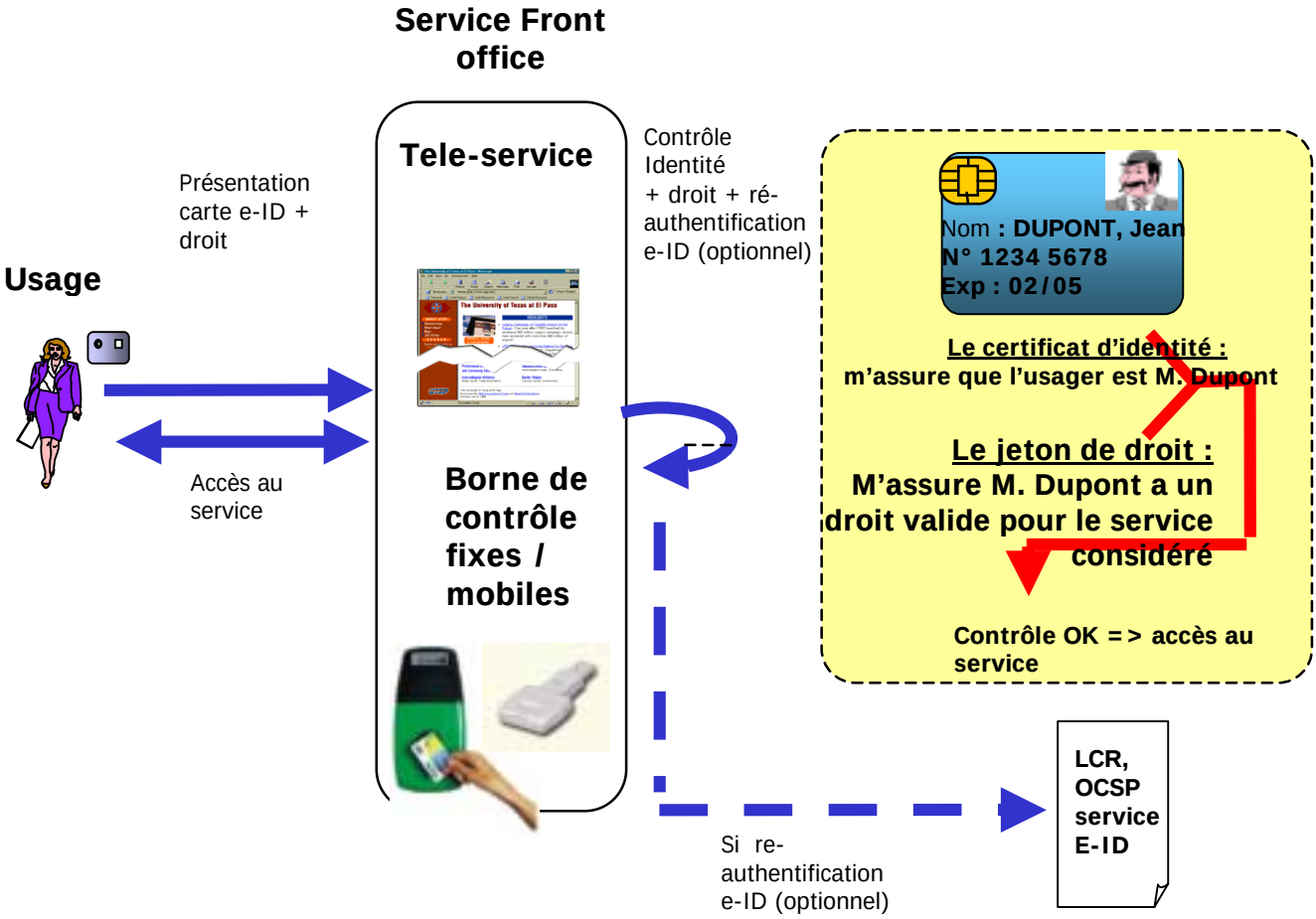
Il est important de bien distinguer le certificat de la signature[134]. Le premier consiste en une fourniture à la fois logicielle et matérielle permettant d'activer un mécanisme de bi-clés. Il s'agit donc d'un fichier électronique attestant qu'une clé publique appartient à l'entité qu'il identifie (personne physique ou morale ou entité matérielle). III est délivré par une autorité de

[134] Garantir l'identité du signataire, l'intégrité du document signé ainsi que la manifestation du consentement du signataire quant au contenu des données électroniques ainsi signées.
Dans le cadre de la PRIS, l'utilisation de la clé privée de signature du porteur et du certificat associé est strictement limité au service de signature électronique.
La mise en œuvre d'un procédé de signature électronique respectant les exigences définies pour le niveau *** de la PRIS permet de bénéficier de la présomption de fiabilité du procédé de signature telle que prévu dans l'article 1316-4 du Code Civil.

confiance appelée l'Autorité de Certification. En signant le certificat, elle valide le lien entre l'entité et la bi-clé pendant une durée donnée précisée dans celui-ci.

Utilisation d'un droit

(exemple : télé-déclaration sociale, vote en ligne, jeux en ligne, contrôle du permis de chasse, service e-banking, ...)



La nature du média est primordiale dans la mesure où il conditionne l'intégrité de la bi-clé. Généralement les bi-clés et les certificats sont stockés dans des cartes à puces ou des clés USB cryptographiques protégées par PIN.

- *Biométrie*

Le rôle de l'Etat se limite à une garantie de moyens mis en œuvre pour confirmer l'intégrité du titre (clé publique) et la légitimité de l'ayant droit à s'en prévaloir (clés privées et identifiant biométrique) tout en se réservant l'usage exclusif du contrôle biométrique, comme si la fraude à l'identité était considérée comme la plus élevée dans l'échelle du risque et que seule la puissance publique s'autorisait ce contrôle ultime.

Un distinguo fort mal perçu par les internautes, des débats de 2005 qui ont largement communiqué sur le contrôle biométrique, sans réaliser qu'il serait strictement réservé aux forces de police et à aucune autre autorité de la sphère publique.
Un dérapage pas nécessairement condamnable si l'on sait que plusieurs pays ont autorisé le contrôle biométrique par la sphère privée, notamment les banques anglaises pour des accès aux coffres ; ou simplement un contrôle local de la propriété de la carte[135] (MOC) comme dans le cas récent du Portugal ; une approche non retenue par les autorités françaises, mais que regrettent certains représentants de nos banques[136].

En résumé, dans le contexte de la CNIe, le certificat est délivré par la puissance publique, il atteste de l'identité du porteur de titre, sur la base d'un couple de clés.
PIN code et empreintes biométriques sont intimement liés au détenteur de titre : le PIN, par sa connaissance du code secret, la biométrie, comme un condensé de sa nature physique.

Le code active la bi-clé par une frappe du clavier ou un pointage de l'écran, mais sans transiter sur le réseau. L'authentification biométrique peut être réalisée sur la carte ou transiter sur le réseau, suivant le type de recherche effectuée.

Mais dans tous les cas, elle est restreinte aux représentants de l'état.

135 MOC : Match On the Card, tel que proposé par le Portugal dans son récent projet de Carte d'Identité Cartao de Cidadao . Cette authentification biométrique sera utilisée dans les cas où un lien fort entre la personne physique et l'identité numérique est requise (e.g. ouverture d'un compte bancaire, obtention d'un prêt, etc.) avec le consentement du porteur.

136 Cette opinion ressort de nos entretiens avec le CFONB.

Conclusion :

Les signatures électroniques constituent l'un des enjeux majeurs du programme d'identité de l'Etat pour que ce projet participe pleinement au développement de l'économie numérique et des échanges sur internet. Les gains de productivité et chiffres d'affaires rapidement suggérés ici sont à prendre avec précaution ; ce sont au plus des ordres de grandeur, forcément approximatifs, qui tablent sur une croissance accélérée de secteurs déjà portés par le web.

Par contre, ne sous-estimons pas l'impact de cette rupture technologique que constituent l'identité forte et la confiance sur le web. Même s'il ne peut être possible de l'évaluer sur la base des services existants, rappelons que le déploiement de projets d'infrastructure à l'échelle nationale peut générer des retombées importantes.

Née en France, la carte à puce constitue un formidable marché dont nos industriels sont les leader mondiaux. Le « Minitel », autre incongruité hexagonale, a fait de notre pays un pionnier mondial de l'économie numérique alors que les PTT voulaient simplement diminuer le coût de l'annuaire.

La gratuité des certificats proposés avec les CNIe peut pareillement conduire à l'éclosion d'offres originales, inédites, nullement pressenties à ce jour, et vraissemblablement passées sous silence dans cette étude.

Certains acteurs, dont nous ressentons ici la nervosité et l'intérêt, sont déjà à l'affût de nouveaux services financiers. Des intermédiaires de confiance, dont nous décelons encore mal le positionnement dans le contexte de l'économie sur le net généralisée, sauront certainement tirer partie d'offres basées sur le Web 2.0 et les certificats électroniques.

D'une manière générale, l'une des caractéristiques du secteur numérique, est que chaque innovation a le potentiel de révolutionner les usages, et son cycle de vie est conditionné par l'émergence d'autres innovations.