La sécurisation des échanges électroniques

Fabrice Mattatia (90),
chargé de mission GIP CPS (1)

I. Les principes de la sécurisation

Le développement récent des échanges électroniques révèle aujourd'hui un besoin de confiance. Les exemples sont nombreux. Certes, le client qui passe une commande par Internet en donnant son numéro de carte bancaire est protégé par la loi tant qu'il ne communique pas son code ; par contre le fournisseur de biens ou de services assume, lui, tout le risque de fraude. Autre exemple, les entreprises, qui échangent de plus en plus par des moyens électroniques des informations confidentielles avec leurs différents collaborateurs, leurs clients ou leurs fournisseurs, ne peuvent se permettre de prendre le risque de voir leurs messages interceptés ou falsifiés. L'administration aussi gagnerait à remplacer tous ses formulaires de papier par leurs équivalents électroniques (par exemple pour les déclarations de TVA des entreprises, ou de revenu des particuliers), mais elle ne peut le faire sans garantir la totale sécurité de l'échange, et notamment sans s'assurer de l'identité de ses interlocuteurs et de l'intégrité du message. Or, un échange électronique normal (envoi de fichier ou de message, accès à un serveur) sur un réseau ouvert de type Internet n'offre **aucune garantie** :
– sur **l'identité** des intervenants (n'importe qui peut usurper n'importe quelle identité),
– sur **l'intégrité** des données échangées (elles peuvent être modifiées accidentellement ou frauduleusement pendant le trajet sur le réseau, ou par le destinataire),
– sur la **responsabilité** assumée par l'expéditeur (il peut nier avoir expédié ces données),
– sur la **confidentialité** de l'échange (le message transite en clair sur le réseau).

Afin de **garantir la confiance** dans les échanges électroniques, un **système de sécurisation** doit donc assurer les fonctionnalités suivantes :
– **l'authentification** des intervenants (chacun présente à l'autre une preuve infalsifiable et vérifiable de son identité et de son droit à participer à l'échange),
– **l'intégrité** des échanges (les modifications accidentelles ou frauduleuses des données doivent être repérables),
– **la signature** des données (par cet acte, le signataire assume le contenu de l'envoi),
– **le chiffrement** des échanges (seuls les interlocuteurs peuvent déchiffrer les données).

Une analogie consisterait à faire ressortir le besoin, pour un échange épistolaire, de photocopies certifiées conformes des cartes d'identité, de textes paraphés et d'enveloppes inviolables. Les anciens détenaient une solution originale avec le sceau de cire, à la fois preuve d'identité, signature et moyen de scellement de l'enveloppe.

Toutefois, un sceau, même authentique, n'apporte aucune garantie sur les attributs de son émetteur, par exemple sa fonction, ses diplômes ou sa solvabilité. Il suppose que l'on connaisse personnellement l'interlocuteur, et que l'on détermine ainsi le degré de confiance à lui accorder. Au contraire, dans les échanges électroniques où l'interlocuteur est souvent un inconnu, ces informations sont primordiales pour déterminer s'il a ou non le droit d'entrer dans l'échange.

L'authentification

Revenons donc aux photocopies "certifiées conformes". On voit ici que, pour assurer la confiance, cette certification doit être réalisée par une autorité incontestable. Il en est de même dans les échanges électroniques : la solution pour authentifier les interlocuteurs consiste à faire délivrer par des autorités crédibles et fiables des certificats électroniques infalsifiables, qui précisent leur identité et, si besoin, leurs attributs (fonction, titre, solvabilité, et pourquoi pas classement aux échecs, au golf ou au tennis, etc). Une même personne peut, si besoin, détenir plusieurs certificats délivrés par plusieurs autorités, éventuellement sur plusieurs supports (de même que, dans le monde traditionnel, les certificats papier du permis de conduire et du baccalauréat ne sont pas émis par les mêmes autorités). La crédibilité d'une autorité provient de la garantie qu'elle offre, de ne délivrer ses certificats qu'à bon escient.

(1) GIP CPS, 8 bis, rue de Châteaudun, 75009 Paris. Tél. : 01.44.53.33.91.
E-mail : f.mattatia@gip-cps.fr

Pour les échanges électroniques, on appelle Autorité d'enregistrement (AE) l'organisme chargé de vérifier les dossiers déposés par les personnes demandant un certificat, et de les valider s'ils sont corrects.

Au vu de cette validation, un autre organisme appelé Opérateur de certification (OC) réalise le certificat électronique et le remet à son utilisateur. Il gère également un annuaire des certificats émis et une liste des certificats mis en opposition.

La sécurisation des données

Les techniques permettant de chiffrer, de signer et de garantir l'intégrité des échanges reposent sur les mêmes principes.

Chiffrement

L'émetteur dispose d'une clef électronique de chiffrement Kc et d'un dispositif f de traitement de son message. Il transforme ainsi son message initial Mi en un message chiffré Mc(Mi, Kc), fonction du message initial et de la clef.

Le destinataire dispose aussi d'une clef K et d'un dispositif de traitement g, qui lui permettent de retrouver le message initial Mi à partir du message chiffré Mc(Mi, Kc).

Signature et intégrité

L'émetteur dispose aussi d'une clef Ks et d'un dispositif de signature S, avec lesquels il obtient un code S(Mi, Ks), fonction du message initial et de la clef. Ce code est joint au message expédié.

Le destinataire reçoit donc un message *a priori* suspect Mi' et le code S(Mi, Ks). Il va procéder à la vérification de la signature. Pour cela, il dispose d'un dispositif et d'une clef qui, appliqués au message Mi' et au code S(Mi, Ks) reçus, permettent de vérifier si oui ou non S est bien lié à Mi', ce qui dans l'affirmative prouve à la fois que Mi' est identique au message d'origine, et que son émetteur est bien le détenteur de la clef de signature Ks. La signature et l'intégrité sont ainsi garanties.

Ces démarches supposent évidemment que les clefs soient strictement personnelles, et que les dispositifs de traitement soient suffisamment complexes et sûrs pour interdire une modification non autorisée des données. Ces traitements s'effectuent selon différents algorithmes paramétrables.

Ces algorithmes peuvent être inversibles, ils sont alors dits symétriques. Dans ce cas, une même clef secrète K est partagée par les deux interlocuteurs, et on a à la fois Mc = Mc(Mi, K) et Mi = Mi(Mc, K). Par exemple, le codage trivial consistant à décaler toutes les lettres d'un cran, A étant remplacé par B, B par C, etc. L'inconvénient est que, si l'on tient à la confidentialité, il faut une clef différente pour chaque paire d'interlocuteurs, ce qui devient rapidement ingérable. Pour la signature, en outre, il n'est pas possible en cas de litige d'attribuer un message à l'un plutôt qu'à l'autre.

Il existe également des algorithmes asymétriques. Ceux-ci reposent sur la factorisation des grands nombres. Leur principe est que le traitement subi par les données avec une clef de départ K1 peut être inversé avec une clef d'arrivée K2 différente, liée de façon unique à la clef de départ mais ne permettant pas de la déduire : on a Mc = f(Mi, K1) et Mi = f^{-1}(Mc, K2), avec la fonction f telle que la connaissance de K2, Mi et Mc ne permet pas de retrouver K1 ni de forger de faux couples (Mi, Mc) liés par K1.

En pratique, chaque interlocuteur dispose d'une clef privée, qu'il garde secrète, et de son inverse la clef publique, qu'il diffuse à ses correspondants. Les données traitées au départ avec l'une de ces clefs peuvent être reconstituées à l'arrivée avec l'autre. Pour chiffrer un message, on emploiera donc la clef publique du destinataire. Seul ce dernier pourra le déchiffrer avec sa clef privée. Par contre, l'émetteur signera avec sa propre clef privée. L'application de sa clef publique au message transmis prouvera qu'il en est bien l'auteur. Ce point nécessite à nouveau l'intervention d'une autorité fiable, pour certifier les liens entre clef publique et identité de l'interlocuteur. La clef publique peut ainsi être l'un des attributs contenus dans le certificat électronique.

Avec les algorithmes asymétriques, on n'a plus besoin que de deux clefs par interlocuteur. Par contre leur mise en œuvre est sensiblement plus lente que celle des algorithmes symétriques, ce qui les rend inutilisables en l'état actuel de la technique pour chiffrer toute une session entre deux interlocuteurs. C'est pourquoi en pratique ils ne sont utilisés intégralement que pour la signature et l'intégrité. Par contre, pour le chiffrement, la solution retenue par le marché pour des raisons de performance consiste à utiliser un algorithme asymétrique uniquement pour convenir entre les parties d'une clef de session symétrique et temporaire pour cet échange, ce qui permettra un chiffrement plus rapide.

À partir du moment où un même algorithme est utilisé par une communauté électronique, les clefs peuvent être, soit créées et distribuées par une autorité dite Tierce partie de confiance (TPC), soit générées sur son poste par chaque utilisateur. Dans les deux cas, la clef publique doit être communiquée à l'Opérateur de certification pour insertion dans le certificat. La TPC peut également, à la demande des utilisateurs, disposer d'un moyen de régénérer les clefs pour leur propriétaire légitime en cas d'oubli.

L'infrastructure de gestion de clefs à mettre en place

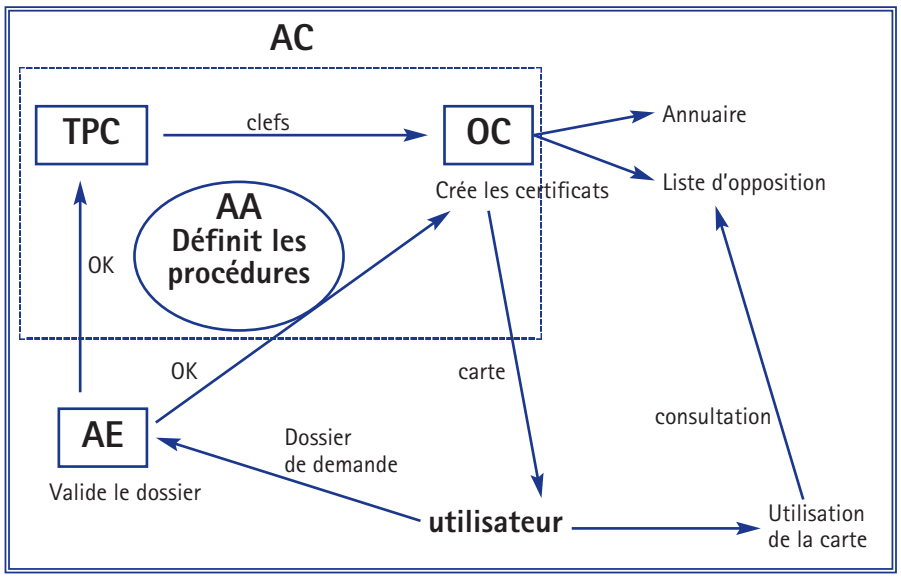
Récapitulons les autorités que nous avons déjà décrites :
– l'Autorité d'enregistrement (AE), qui valide les dossiers des demandeurs et atteste leurs droits,
– la Tierce partie de confiance (TPC), qui génère éventuellement les clefs et peut en garder une trace,
– l'Opérateur de certification (OC), qui au vu de la validation par l'AE, et à la réception des clefs publiques, émet les certificats électroniques.

Les règles de fonctionnement de ces entités doivent être clairement définies afin d'assurer la confiance des utilisateurs. C'est le rôle de l'Autorité administrative (AA), qui rédige et publie les engagements sur les moyens mis en œuvre pour fonder la confiance et garantir la sécurité du système, tant

au niveau des procédures de travail qu'au niveau de la protection physique des infrastructures. Ces documents sont de nature contractuelle vis-à-vis des utilisateurs.

En pratique, pour des raisons d'efficacité et d'économie, l'AA, l'OC et la TPC sont souvent regroupées pour former l'Autorité de certification.

Le fonctionnement de l'infrastructure de gestion de clefs est résumé dans le schéma ci-contre.



Les responsabilités

Les différents acteurs du système d'échanges électroniques ont chacun des responsabilités dans l'application de ces techniques. Par exemple, l'utilisateur qui émet un fichier ou se connecte à une application doit authentifier son destinataire ou cette application.

Inversement, celui qui reçoit un fichier ou permet une connexion à son serveur doit authentifier son partenaire, et vérifier qu'il n'est pas en opposition, avant d'accepter.

Les applications doivent contrôler les certificats de ceux qui veulent se connecter, et vérifier, d'après leurs attributs, que l'accès leur est autorisé (cette décision étant du seul ressort du promoteur de l'application). Enfin, des règles de délégation de signature peuvent être prévues, à charge pour les utilisateurs de les respecter.

Le choix de mettre en œuvre ou non le chiffrement peut être réglementairement obligatoire pour certains échanges. Il est parfois utile que la signature ou le chiffrement nécessitent une activation volontaire supplémentaire par les parties, afin d'imposer un choix conscient.

De son côté, l'opérateur de certification doit tenir à jour les droits des utilisateurs (liste d'opposition, de suspensions, etc.) et permettre leur consultation en permanence.

La confiance dans le système repose sur la sécurité et la rigueur à la fois des procédures de l'Autorité d'enregistrement et des techniques mises en œuvre par l'Autorité de certification.

Dans le cadre de la réalisation pratique d'un réseau, ces diverses responsabilités devront être précisées dans les contrats. La sécurisation n'étant pleinement garantie que lorsque tous les acteurs satisfont à leurs responsabilités, ces derniers devront donc être sensibilisés sur ce point et se conformer systématiquement aux règles qui seront définies.

Les contraintes juridiques

Un système de sécurisation des échanges électroniques doit évidemment respecter la réglementation nationale, notamment en ce qui concerne la cryptographie. La libéralisation des règles en France depuis mars 1999 permettra un plus grand choix de mise en œuvre.

Inversement, il est souhaitable que la législation reconnaisse la valeur de la signature électronique, et lui donne un statut équivalent à celui de la signature manuscrite : cela est sans doute indispensable à son utilisation pour des procédures administratives [2], et en tout cas nécessaire pour créer une confiance des utilisateurs. Un projet de loi en ce sens a été déposé début septembre par le gouvernement. Une directive européenne fixant un cadre de reconnaissance juridique est également en projet et devrait paraître fin 1999.

Enfin, la sécurisation des échanges électroniques devra obtenir un avis favorable de la CNIL, donc garantir la confidentialité (ce qui semble facile à remplir pour un système sécurisé), mais aussi le respect de la vie privée.

Les implémentations

Les clefs et les algorithmes détenus par l'utilisateur peuvent être stockés, soit sur son poste de travail, soit sur une carte à puce.

Le stockage sur le poste présente de multiples inconvénients. Si la clef et l'algorithme sont stockés sur un seul poste, cela empêche l'utilisateur de se connecter au réseau depuis un autre endroit. S'ils sont stockés en plusieurs endroits, cela multiplie les risques de vol, d'utilisation non contrôlée par un tiers en l'absence du responsable, ou de piratage : en effet, il est alors possible à un tiers de copier le disque dur pour s'emparer à la fois de la clef, des algorithmes et de tous les fichiers chiffrés stockés.

Lorsque la clef et les algorithmes de chiffrement sont sur une carte protégée par un code porteur, son détenteur peut l'utiliser n'importe où. S'il la perd, elle reste protégée par son code : il n'est pas possible [3], même en disposant de la carte, de démonter ses mécanismes de chiffrement, car elle effectue ses calculs en interne et agit comme une boîte noire. De même, les fichiers stockés sur le poste sous forme chiffrée ne peuvent plus être lus s'ils sont recopiés illégalement.

En conclusion, comme le note le *Rapport sur la mise en œuvre d'une signature électronique dans le cadre des télé-procédures* publié en novembre 1998 par le ministère de l'Économie, des

Finances et de l'Industrie, "le stockage de certains modules cryptographiques et de la clef secrète dans une carte à puce permet d'optimiser le niveau de sécurité offert". C'est également la solution retenue par le secteur de la santé avec la Carte de professionnel de santé (CPS).

II. Un exemple de système sécurisé : le GIP CPS

Le Groupement d'intérêt public "Carte de Professionnel de Santé" (GIP CPS) a été fondé en 1993. Il rassemble l'État, les Ordres professionnels, les Caisses d'assurance maladie obligatoires et complémentaires et des représentants professionnels. Il a pour objet l'émission, la gestion et la promotion de la carte de professionnel de santé (CPS), carte à puce qui permet aux personnes habilitées du secteur de la santé de **s'identifier**, de **prouver leur qualité**, de **signer** et de **chiffrer** leurs échanges électroniques.

À ce titre, il a défini et mis sur pied les structures nécessaires à une infrastructure de gestion de clefs telle que définie plus haut. Il a élaboré les procédures amont permettant de valider les dossiers en liaison avec les autorités compétentes (État, Ordres, etc). Il définit, émet et gère les cartes, les clefs et les certificats. Le déploiement d'une première tranche de 400 000 cartes est en cours, et le système vise à terme 1 500 000 utilisateurs.

La politique du GIP est d'assurer la compatibilité du système CPS avec les standards en vigueur et en cours de développement.

La carte CPS bénéficie d'un niveau de sécurité homologué ITSec "E3 fort" (c'est-à-dire le même niveau de sécurité que les cartes bancaires, mais en disposant de fonctionnalités plus puissantes).

Le GIP mène une politique de sécurité globale, touchant à la fois à la rigueur des procédures de gestion, à la sûreté des technologies utilisées, et aux garanties de qualité et de disponibilité du système. En rédigeant sa Déclaration relative aux Procédures de certification et sa Politique de sécurité, documents publics, il s'engage sur des objectifs précis de sécurité et sur les moyens à mettre en œuvre pour les atteindre. Il garantit ainsi aux utilisateurs la confiance dans les capacités du système à assurer la confidentialité et la sécurité des échanges électroniques.

Les fonctionnalités de la CPS

Les clefs et les certificats sont stockés dans la carte à puce. Les algorithmes sont mis en œuvre dans la carte, de manière qu'aucun secret ne soit communiqué à l'extérieur.

La signature utilise les algorithmes SHA-1 et RSA (standards) avec des clefs de 768 bits. Le passage à une clef de 1 024 bits est à l'étude.

Le chiffrement s'effectuera aussi, pour la nouvelle version de la carte émise en 2000, avec un algorithme asymétrique standard pour chiffrer des clefs de session symétriques.

Les certificats sont à la norme X509 v3. Ils contiennent l'identité de leur titulaire, ses clefs publiques, sa profession et sa spécialité.

L'intérêt des certificats standardisés est qu'ils peuvent être acceptés par toute infrastructure dont le niveau de sécurité est équivalent à celui de l'autorité émettrice (ici le GIP CPS). On parle alors de "reconnaissance mutuelle" des autorités. Les certificats distribués aux professionnels de santé leur permettront donc de dialoguer électroniquement, non seulement avec leurs pairs en France, mais plus largement, avec toute personne dans le monde utilisant la même norme. L'utilisation des standards devient ainsi un gage d'ouverture illimitée.

Conclusion

Les techniques de sécurisation des échanges électroniques, permettant de répondre aux besoins de confiance des utilisateurs, existent et arrivent à un degré de maturité satisfaisant. De nombreuses administrations, en France et à l'étranger, étudient la mise en place des infrastructures nécessaires. Des réalisations, comme le système CPS, sont déjà en cours. Mais, de même que le téléphone n'est vraiment utile que lorsque tous les abonnés peuvent se joindre, quel que soit leur opérateur, l'interopérabilité des systèmes électroniques sécurisés, quelle que soit l'autorité responsable, représenterait un atout pour leur développement. Il convient donc de veiller à la compatibilité de tous les systèmes. L'adoption de solutions communes à plusieurs acteurs permettrait en outre une économie d'échelle, des gains de temps et une plus grande assurance de la pérennité des produits. La technologie française des cartes à puce détient ici une occasion unique de conforter son avance. ■

(2) En juin 1999, en France, seule la signature des feuilles de soin électroniques par la carte de professionnel de santé était reconnue par la loi.

(3) Sauf à déployer une puissance informatique et un temps de calcul démesurés. Les algorithmes étant tous plus ou moins décryptables (au sens de : déchiffrables illégalement), le principe est en effet de toujours choisir une longueur de clef pour la mise en œuvre de l'algorithme dont la robustesse est telle que son décryptage a un coût disproportionné par rapport au gain espéré.