Résumé

Pour lutter contre la fraude en ligne, des organismes spécialisés (CNIL en France, APACS au Royaume Uni, FFIEC aux Etats-Unis) encouragent l'utilisation de l'authentification forte, dans laquelle deux facteurs indépendants sont contrôlés pour donner accès à un service : d'une part un couple identifiant/mot de passe, d'autre part un élément matériel (token).

Mobilegov a développé une technologie brevetée pour authentifier n'importe quel élément matériel numérique. Cette technologie est intégrée dans un produit d'authentification forte, *Secured Access Web Service* (SAWS). Il est plus simple à mettre en œuvre que ce qui existait jusqu'ici, tant pour le prestataire de service que pour l'utilisateur, puisque c'est ce dernier qui choisit l'élément matériel de l'authentification forte parmi son propre équipement.

SAWS est engagé dans une procédure de qualification Critères Communs EAL3+.

Table des matières

La menace : la cybercriminalité

Société de l'information et mondialisation

En offrant le moyen d'enregistrer l'information, l'écriture a permis aux civilisations de progresser par accumulation de connaissance. En effet, contrairement au langage qui n'autorise la transmission que d'une génération à la suivante, l'écriture garde la trace d'une connaissance sur une durée qui ne dépend que du moyen de stockage.

Avec l'écriture, l'homme découvre la valeur stratégique de l'information, et met en place des mécanismes de protection, en général liés à une caste d'ayants droit.

L'invention de l'imprimerie ouvre une brèche dans ce mécanisme de protection, en ouvrant l'accès à l'information en dehors de cette caste.

Pendant 500 ans, le support imprimé a été le principal vecteur de transmission et de stockage de l'information, amenant des progrès considérables de la plupart des activités humaines, grâce à la facilité de reproduction de l'information.

Durant cette période, l'amélioration constante des moyens de transport a facilité les échanges des biens, des personnes et des informations, sans apporter pour autant de véritable révolution : la route de la soie existait bien avant l'imprimerie.

C'est l'Internet et les autres réseaux numériques, qui conjuguent la puissance expressive du document multimédia avec la facilité de sa transmission par un réseau de communication qui ont apporté la mondialisation, pour le meilleur et pour le pire.

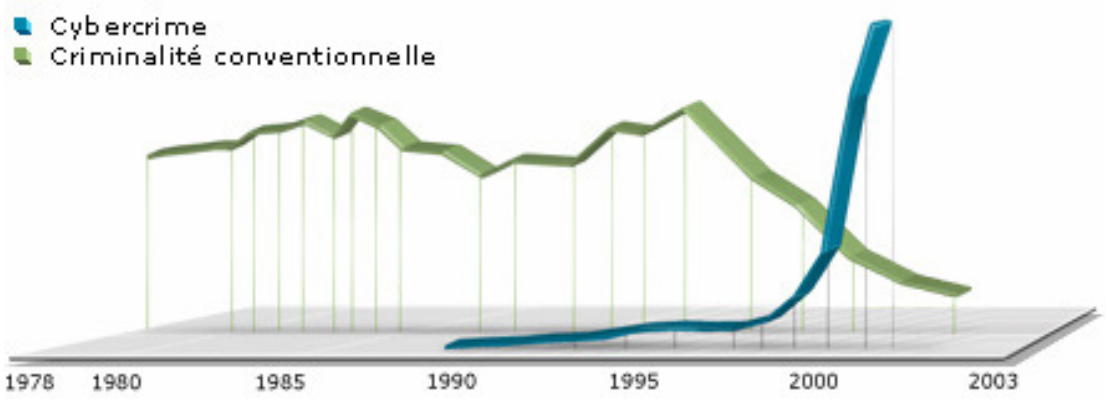
Le meilleur, c'est toute l'information partout, tout de suite, au point que notre société repose désormais sur le web et le téléphone portable de façon difficilement réversible. Le pire, c'est le besoin d'inventer de nouveaux modèles économiques pour tout ce qui touche à l'information, et c'est l'apparition de nouvelles formes de criminalité, nouvelles par leur type ou par leur ampleur.

Une nouvelle criminalité

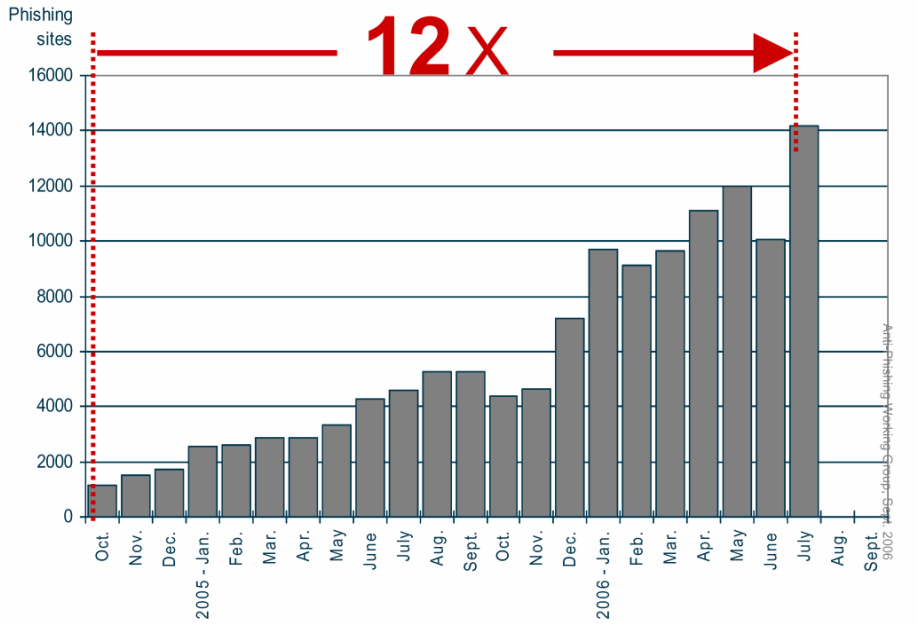
Les faux et leur usage sont aussi vieux que l'écriture elle-même. Ce qui est nouveau avec les documents numériques, c'est la facilité avec laquelle on peut réaliser un faux, et la difficulté à reconnaître un faux dans un document qui circule.

Les exemples de fraude dans le monde numérique sont nombreux, mais la sélection naturelle fait que seules les fraudes à valeur ajoutée financière survivent. Ainsi, les virus ludiques on laissé la place aux logiciels malveillants utilitaires, puis à une criminalité organisée, dont le chiffre d'affaires explose, comme le montre ce diagramme[1] :

[1] Source : IBM, http://www-03.ibm.com/ondemand/ca/fr/pointofview/cybercrime/jul18/ibm_future_crime.html



Le nombre d'attaques par phishing contre les banques double même très régulièrement tous les 4 mois depuis plusieurs années[2] :



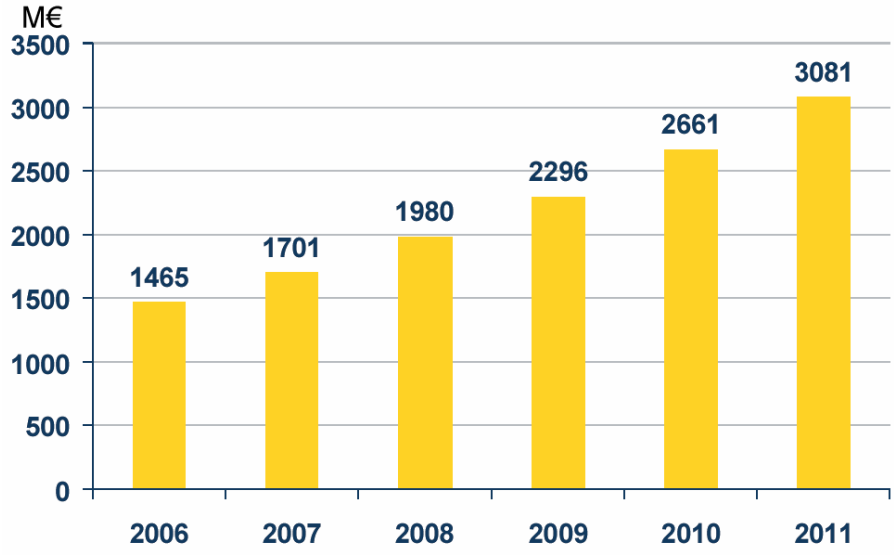
Cette courbe devance même celle des usages des cartes bancaires. Ainsi, en 2007, au Royaume Uni, 145 millions de cartes ont généré 10 milliards de transactions pour un montant total de 354 milliards de £[3].

Dans le même temps, les dépenses en France pour améliorer la sécurité informatique ne doublent « que » tous les 5 ans[4] :

[2] Source: National Bank of Canada, Cybercrime & Identity theft, 5 mars 2007, http://www.pwgsc.gc.ca/recgen/colloquium2007/pdf/panel-discussion-jose-navarro-e.pdf

[3] Source: APACS, http://www.apacs.org.uk/resources_publications/documents/FraudtheFacts2008.pdf

[4] Source: Etude IDC « Le marché français des solutions de sécurité informatique », 2007



Dans une guerre non virtuelle, si les efforts d'un camp doublent tous les 4 mois, alors que ceux de l'autre doublent tous les 5 ans, l'issue du conflit ne fait aucun doute.

Il convient tout de même d'apporter une lueur d'espoir : alors que dans le monde réel, la défense repose le plus souvent sur les mêmes technologies que l'attaque, le monde virtuel dispose d'outils de sécurité difficiles à contourner aujourd'hui. Malgré le nombre croissant d'attaques contre les banques, les revenus générés par ces attaques au Royaume Uni stagnent et même régressent depuis un an. Les revenus de la fraude bancaire sur Internet au Royaume Uni sont ainsi passés de 33 millions de £ en 2006 à 23 millions en 2007, grâce à l'éducation des usagers et aux mesures de sécurité mises en place, et notamment l'authentification forte[5]. En France, où la résistance au changement semble plus forte, les revenus de la fraude liée aux paiements sur Internet sont passés de 13 millions d'Euro en 2006 à 26 millions d'Euro en 2007.

La parade : l'authentification forte

Une authentification forte[6] est une procédure d'identification qui requiert le contrôle positif d'au moins deux éléments ou « facteurs » indépendants d'authentification parmi :

- Ce que l'entité connaît (un mot de passe, un code NIP, une phrase secrète, etc.),
- Ce que l'entité détient (un ordinateur, une carte magnétique ou RFID, une clé USB, un PDA, une carte à puce, etc. , soit un « élément matériel » ou « *token* »),
- Ce que l'entité est, soit une personne physique (empreinte digitale, empreinte rétinienne, structure de la main, structure osseuse du visage ou tout autre élément biométrique), ou ce que l'entité sait faire, (biométrie comportementale telle que signature manuscrite, reconnaissance de la voix, un type de calcul connu de lui seul, etc.).

L'authentification forte est recommandée depuis 2005 par les principales organisations compétentes (CNIL en France, APACS au Royaume-Uni, FFIEC[7] aux Etats-Unis).

---

[5] Source: APACS, http://www.apacs.org.uk/resources_publications/documents/FraudtheFacts2008.pdf

[6] Source : http://fr.wikipedia.org/wiki/Authentification_forte

[7] « The agencies consider single-factor authentication, as the only control mechanism, to be inadequate for high-risk transactions involving access to customer information or the movement of

L'authentification forte, pour quoi faire ?

L'authentification forte garantit que le vol d'un mot de passe ou d'un code NIP ne donne pas à celui qui l'a volé l'accès au service protégé par ce mot de passe.

Les cas d'usage concernent donc aussi bien l'accès à des services internes (contrôle d'accès physique ou problématique des utilisateurs internes en réseau dont on maîtrise le poste de travail) que l'accès à des services distants (utilisateur nomade qui accède à des services internes à son entreprise ou utilisateur qui accède à des services web dont il est le client).

La problématique du contrôle d'accès fait intervenir des solutions de type Role Based Access Control et Role Based Management.

La problématique Réseau concerne le contrôle d'accès aux applications internes à l'organisation, aux bases de données, aux serveurs de fichiers, à l'archivage, aux intranets.

La problématique Web ou réseau local étendu concerne les applications de eCommerce, email et Webmail, applications pour webmaster, eAdministration, extranets, banque en ligne...

C'est donc l'ensemble des usages de la Société de l'Information qui est concerné par l'authentification forte. Encore une fois, il ne s'agit pas d'un problème nouveau, mais notre dépendance croissante aux technologies de l'information en fait un problème critique pour l'ensemble de la société. Pour résoudre ce problème, il est urgent de mettre en place des solutions adaptées aux exigences de sécurité variables des applications concernées et aux compétences diverses des utilisateurs de ces applications.

Principe de l'authentification forte

Adapté non seulement aux échanges électroniques mais aussi à l'économie mondialisée, l'authentification forte permet à un fournisseur de service de vérifier à distance que l'utilisateur du service est bien celui qu'il prétend être, ou bien qu'il a fourni à un tiers (peut-être contre son gré, mais en connaissance de cause) les éléments permettant de se faire passer pour lui. Seul le contrôle biométrique permettrait de renforcer encore la sécurité, mais sa mise en œuvre est limitée à des applications dont les enjeux le justifient, et les associations de défense des libertés veillent à ce que cette situation ne change pas.

Les premiers déploiements, menés en 2006-2007 aux Etats-Unis et en Europe du Nord, montrent déjà une régression de la fraude bancaire et confirment le bien fondé des recommandations des organisations compétentes.

Dans ces déploiements, l'authentification forte repose sur deux facteurs : d'une part le couple identifiant/mot de passe, d'autre part un token, objet matériel propre à l'utilisateur, distribué par le prestataire de service. Pour se connecter au service, l'utilisateur doit avoir en mains son token.

Les tokens d'authentification forte

Le token peut être électronique, connecté ou non à l'ordinateur utilisé dans la transaction. Il délivre alors soit un certificat (PKI) soit un mot de passe à usage unique. Ce mot de passe peut être fonction de l'heure, de la carte bancaire de l'utilisateur, ou d'un compteur.

Le token peut être également un document qui contient des listes de chiffres : liste à biffer ou Bingo Card, et il fournit la réponse à une question posée par le serveur au moment du contrôle d'accès (*challenge-response*).

---

funds to other parties. », Federal Financial Institutions Examination Council (FFIEC), Authentication in an Internet Banking Environment, 2005, www.ffiec.gov/pdf/authentication_guidance.pdf

Enfin, le token peut être le téléphone portable de l'utilisateur. Le serveur lui envoie un SMS au moment du contrôle d'accès, l'utilisateur doit saisir une information de ce SMS.

Tokens électroniques connectés à l'ordinateur

Les tokens connectés à l'ordinateur communiquent avec le serveur afin d'être reconnus à distance. Ils consistent en une carte à puce (qui nécessite alors un lecteur de carte, les ordinateurs en étant le plus souvent dépourvu) ou un token USB plus ou moins « intelligent » (mémoire flash ou microprocesseur). Le token peut intégrer la reconnaissance de « ce que l'on sait » (en exigeant la saisie du code NIP) ou même de « ce que l'on est » (en étant équipé d'un lecteur d'empreintes digitales et exploitant la technologie « match on card », respectueuse de la protection des données personnelles).

L'authentification du token par le serveur met en jeu une technologie de type PKI (Public Key Infrastructure) particulièrement sûre.

Les tokens connectés à l'ordinateur constituent une solution très robuste, la seule résistante aux *key loggers* et autres *screen loggers*, pouvant même garantir la non répudiation des transactions.

Toutefois, la solution est difficilement portable d'un ordinateur à un autre. En effet, l'expérience montre qu'il est difficile de trouver un token qui fonctionne sans installation préalable sur tous les systèmes d'exploitation existants.

D'autre part, le coût des tokens (matériel, logiciel PKI) n'est pas négligeable. Il faut savoir que les lecteurs d'empreintes digitales à bas coût sont en général faciles à tromper : il suffit parfois de les chauffer à la flamme d'un briquet pour augmenter leur taux de fausse acceptation.

Tokens électroniques non connectés à l'ordinateur

Pour améliorer la portabilité des tokens, il suffit qu'ils n'aient pas à être connectés à l'ordinateur. Ces tokens représentent donc l'éventail des solutions les plus courantes. Ils génèrent un mot de passe à usage unique, que l'utilisateur lit sur le token et saisit sur le menu de contrôle d'accès.

Le token partage donc un secret avec le serveur. Ce secret peut être lié au temps (date et heure), ou aux mots de passe précédents (token basé sur un compteur).

Pour être activé, le token peut exiger la connexion de la carte bancaire EMV de l'utilisateur, et/ou la saisie d'un code NIP. Ainsi, le vol ou la perte du token ne permettra pas facilement l'accès au serveur.

Enfin, le token peut être le téléphone portable de l'utilisateur. Lors du contrôle d'accès, le serveur lui envoie un SMS qui contient le mot de passe à usage unique à utiliser pour la connexion en cours.

Les tokens non connectés améliorent certes la portabilité, mais c'est au détriment de la sécurité et de l'ergonomie. Parce qu'ils obligent l'utilisateur à saisir le code affiché sur le token, ils ne sont pas d'un usage très convivial, le contrôle d'accès prend plus de temps, et même un temps imprévisible dans le cas du SMS. Enfin, le coût des tokens (sauf pour le téléphone portable) est sensiblement le même que dans le cas des tokens connectés.

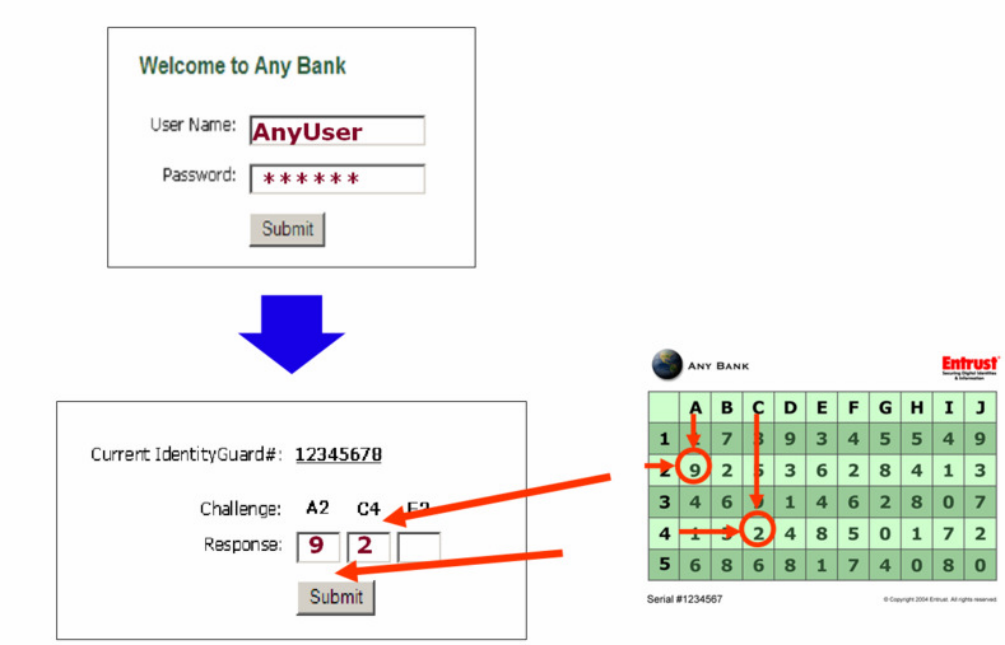
Du fait de la lourdeur du contrôle, ce mode de token ne permet pas facilement d'effectuer une vérification supplémentaire lors d'une transaction importante (virement, ordre d'achat).

Tokens non électroniques

Chaque utilisateur reçoit du prestataire de service un document individuel qui contient des listes de chiffres. Lorsqu'il souhaite se connecter au service, l'utilisateur utilise ce document

pour déterminer le nouveau code à utiliser pour la connexion en cours. Le nouveau code peut être :

- le suivant sur la liste : c'est le cas simple de la « liste à biffer » ou TAN (Transaction Authentication Number)
- fonction d'une question posée par le serveur au moment de la connexion : c'est le cas de la carte matricielle (ou carte à grille ou Bingo Card). Le serveur affiche sur le menu de connexion des numéros de ligne et de colonne. L'utilisateur lit les chiffres en regard de ces numéros sur sa carte et les saisit sur le menu de connexion[8].



Les tokens non électroniques sont certes bon marché. Mais ils ne peuvent être utilisés que pour effectuer quelques transactions. Lorsque la cinquantaine de cases de la carte matricielle ont toutes été utilisées une fois, il est en effet plus sûr de remplacer la carte par une nouvelle. Il en est de même de la liste à biffer.

Conclusion sur les tokens

Le coût des tokens n'est qu'un élément du coût de mise en œuvre de cette authentification forte. En effet, il faut y ajouter le coût de la logistique (fourniture à chaque utilisateur d'un élément matériel unique), et le coût de la gestion des nombreux cas où le token doit être remplacé : perdu, volé, hors service.

Le coût de possession d'un token géré par le prestataire de service est finalement bien plus élevé que le seul prix d'achat du token. Le coût n'est pas le seul facteur : ainsi, lorsque le token doit être remplacé, l'utilisateur est privé pendant plusieurs jours de l'accès au service.

Enfin, le fait que le prestataire de service doive fournir les tokens à ses utilisateurs est contraire à la philosophie des services en ligne totalement dématérialisés : banque directe, vente en ligne, services d'intermédiation tels qu'enchères en ligne.

Pour simplifier la gestion des tokens et réduire les coûts de mise en œuvre de l'authentification sans rogner sur la sécurité, Mobilegov propose avec Secured Access Web Service (SAWS) une solution dans laquelle les tokens sont connectés à l'ordinateur, ce qui

[8] Figure extraite de http://fr.wikipedia.org/wiki/Image:Bingo-Card.png

est un gage à la fois de sécurité et de simplicité d'emploi, et dans laquelle le prestataire de service n'a pas à distribuer ni à gérer les tokens.

Secured Access Web Service (SAWS)

Principe

SAWS permet la mise en place simplifiée de l'authentification forte entre un prestataire de service et un utilisateur du service, connecté par un réseau local, un réseau local étendu ou via Internet. Dans une première étape d'enrôlement, l'élément matériel à utiliser pour authentifier l'utilisateur est défini. Ensuite, pour effectuer une transaction sécurisée, l'utilisateur doit simplement connecter à son ordinateur, au moment où il saisit son mot de passe, l'élément matériel enrôlé.

Première étape : enrôlement

Un accord entre le prestataire de service et l'utilisateur permet à ce dernier de choisir lui-même l'élément matériel qui sera utilisé pour l'authentifier. Ce peut être son ordinateur, un composant de son ordinateur, ou n'importe quel composant amovible, connecté avec ou sans fil à son poste client au moment de la transaction : clé USB, téléphone portable, iPod, etc.

Un protocole défini par le prestataire de service permet d'enrôler l'élément matériel : l'utilisateur peut passer dans une agence ou un bureau du prestataire ou peut effectuer l'opération en ligne : muni d'un mot de passe à usage unique communiqué de façon traditionnelle (SMS, courrier, email), l'utilisateur se connecte au site du prestataire, puis identifie en ligne l'élément matériel qu'il souhaite utiliser. Pour ce faire, il lui suffit de cliquer sur l'un des éléments qui s'affichent au moment de l'opération.

En cas de perte de l'élément matériel, l'utilisateur contacte le prestataire, comme il signale aujourd'hui la perte d'une carte de crédit. En quelques minutes, grâce à l'envoi par SMS ou email d'un nouveau mot de passe à usage unique, il peut définir immédiatement un nouvel élément matériel.

Seconde étape : sécurisation d'une transaction

En général, SAWS est installé en complément de la saisie d'un mot de passe. Au moment de la saisie et du contrôle du mot de passe, le serveur contrôle également la présence de l'élément matériel côté client. Si l'élément matériel est l'ordinateur lui-même, plusieurs composants de l'ordinateur sont contrôlés. Si l'élément matériel est un composant amovible, la présence de ce composant connecté au poste client est contrôlée. L'accès est autorisé seulement si l'élément matériel et le mot de passe sont reconnus.

L'authentification de l'élément matériel met en jeu la technologie d'ADN du Numérique® de Mobilegov : tout composant digital contient une information unique, implantée par le constructeur d'une part pour son usage personnel (n° de série facilitant le suivi des séries de fabrication) et d'autre part par le système d'exploitation (référence constructeur et modèle) pour identifier le pilote nécessaire à l'exploitation du composant.

Pour rechercher la présence de l'élément matériel, le serveur envoie au client une applet Java signée. Cette applet établit la liste des composants présents sur le poste client et renvoie de manière sécurisée (message à durée de vie limitée et crypté) au serveur l'ensemble des informations constructeur-modèle-n° de série pour tous les composants détectés. Le serveur recherche dans la liste la présence de l'élément matériel d'authentification pour l'utilisateur repéré par son identifiant.

En parallèle, le serveur valide le mot de passe saisi pour le même utilisateur. Si le mot de passe et l'élément matériel de l'utilisateur défini par son identifiant sont corrects, l'authentification forte est positive et l'accès au service peut être accordé.

Mise en œuvre

La mise en œuvre de SAWS nécessite une mise à jour du système de contrôle d'accès du prestataire de service.

SAWS est une solution adaptée aussi bien aux configurations de quelques dizaines d'utilisateurs (cas d'un intranet par exemple) qu'aux très grosses configurations de plusieurs centaines de milliers d'usagers (cas de la banque en ligne).

SAWS est donc conçu de façon modulaire et réplicable. SAWS s'interface avec les bases de données comme avec les annuaires d'entreprise (LDAP, X500) et les serveurs Radius.

SAWS peut être géré localement chez le prestataire de services, sur une machine existante ou sur une machine indépendante, ou peut être délocalisé en datacenter (tiers de confiance, fournisseur d'accès Internet).

SAWS peut être associé à un dispositif d'horodatage et de traçabilité pour signer des transactions.

Le logiciel serveur de SAWS fonctionne dans les principaux environnements serveur (MS Windows, Linux) et il peut être adapté à la plupart des plateformes existantes.

SAWS permet d'authentifier des composants matériels connectés à des clients tournant sous MS Windows, Mac-OS, Linux, Symbian. Le principe de SAWS le rend adaptable à n'importe quelle plate-forme sur laquelle se connectent des composants matériels digitaux. Aucune procédure d'installation n'est nécessaire côté client.

Enfin, SAWS comme toutes les solutions qui font intervenir un token connecté à l'ordinateur est à l'abri des *key loggers* ou *screen loggers*.

Compte tenu des applications visées, SAWS a enclenché la procédure de qualification Critères Communs EAL3+[9].

Usages

Le produit SAWS, par sa capacité à supporter de nombreux systèmes d'exploitation, sa facilité de mise en œuvre tant pour le prestataire de service que pour l'utilisateur et son coût de gestion réduit par rapport aux solutions existantes est préconisé dans plusieurs domaines d'application. Sans vouloir être exhaustif, nous en passons quelques uns en revue.

Contrôle d'accès

L'usage principal de SAWS concerne le contrôle d'accès à des applications. Ces applications peuvent être internes à l'entreprise (par exemple, lors de l'utilisation de machines en libre service) ou externes (applications utilisées via le web).

Identity management, Access management

La carte d'identité électronique, biométrique et de préférence de type Match on card sort des placards. Grâce au Match on card, l'information biométrique du porteur est protégée, et il n'est pas facile d'utiliser une carte volée pour usurper l'identité du porteur. Mais une telle carte ne sera pas aisément utilisable pour toutes les transactions de la vie quotidienne : pour

[9] Pour une explication sur niveaux d'assurance d'évaluation selon les Critères Communs, voir par exemple http://fr.wikipedia.org/wiki/Evaluation_Assurance_Level

des raisons de résistance mécanique, de connectique (y compris sans contact) et de rapidité, un objet relais, à plus courte durée de vie, pourra en revanche être préféré pour certaines applications. Dans la philosophie de SAWS, cet objet sera défini de façon sécurisée à l'aide de la carte d'identité, requise au moment de l'enrôlement. Différentes applications pourront utiliser différents objets, ou le même, à la convenance de l'utilisateur. La sécurité ne sera pas la même que celle obtenue par le contrôle biométrique multimodal et la signature électronique de la carte d'identité, mais elle sera néanmoins suffisante pour de nombreuses applications, complétée ou non par la saisie d'un mot de passe. C'est le cas notamment du contrôle d'accès, où dans bien des cas la vitesse du contrôle prime sur son infaillibilité.

Cette solution est retenue pour la Chancellerie Autrichienne.

Banque en ligne

Le besoin de sécurité, généralement partagé par le client et le prestataire de service dans le cas de transactions bancaires, a vu la mise en place, notamment en Europe du nord, de solutions d'authentification forte. Bien que le même élément matériel puisse parfois être utilisé par plusieurs banques, et que les erreurs de manipulation soient peu nombreuses, cette solution est en général considérée comme une contrainte pesante.

SAWS apporte à la banque en ligne une solution d'authentification forte, conforme aux directives des organisations compétentes, plus simple à gérer pour la banque comme pour son client.

eCommerce

La saisie répétée des codes de carte bancaire (numéro de carte, date d'expiration, nom et prénom du porteur, numéro de contrôle) est fastidieuse mais n'apporte pas réellement la sécurité nécessaire à des transactions de plus en plus fréquentes et qui engagent des montants de plus en plus importants.

De même, la multiplication des comptes ouverts chez différents fournisseurs, impose à l'utilisateur de mémoriser ses nombreux codes et mots de passe. Ce n'est pas ici un problème relevant du Single Sign-On, les informations échangées étant en général peu sensibles. Et puis, si les informations échangées jusqu'ici sont peu sensibles, c'est aussi parce que les mécanismes de sécurité disponibles sont insuffisants.

SAWS apporte une solution simple et sûre à ces applications, facilitant la portabilité et donc la mobilité.

Digital Rights Management (DRM, Gestion des droits numériques)

La lutte contre la copie illégale et la transmission de documents protégés par un copyright est passée par plusieurs étapes. On a d'abord fait porter la responsabilité sur les fournisseurs d'accès, puis sur leurs abonnés, enfin, devant le manque de succès, sur l'ensemble des usagers de dispositifs de stockage de données. La raison en est la difficulté de faire la preuve de l'identité des fraudeurs : rien ne prouve en effet que l'abonné à un accès Internet est bien celui qui télécharge des données protégées ou illégales.

Il faut donc agir en amont de la mise en circulation des faux et apporter la traçabilité des échanges qui inquiète les fraudeurs sans compliquer la vie de la majorité d'usagers honnêtes. SAWS est une telle solution, compatible également avec la protection de la vie privée.

Single Sign On

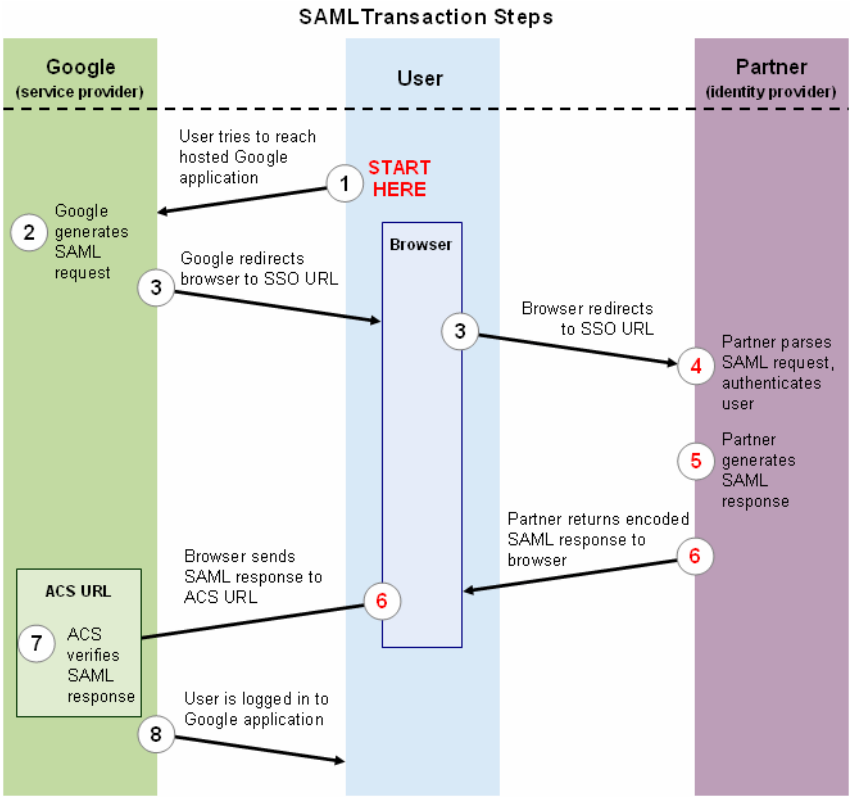
La multiplication des applications protégées par un mot de passe puis la nomadisation des collaborateurs a encouragé les solutions permettant à chacun de ne plus retenir qu'un seul mot de passe : c'est le Single Sign On (SSO).

Si les premières solutions, qui définissaient le même mot de passe pour chaque application, ont eu un effet négatif sur la sécurité (car en craquant le mot de passe d'une application mal protégée, on connaissait tous les mots de passe d'un utilisateur), les solutions récentes améliorent au contraire la sécurité et permettent notamment de définir des politiques de gestion des mots de passe (longueur, complexité, durée de vie) en conformité avec les réglementations (SOX, HIPAA, GLBH, CFR). Il est alors facile d'implémenter les procédures de sécurité requises par les nouvelles réglementations métiers, ainsi que d'auditer et de prouver (grâce aux outils de rapport et d'audit) que celles-ci sont respectées.

Toutefois, le cœur de la sécurité demeure le mot de passe. Plusieurs solutions de SSO complètent donc cette sécurité par une authentification forte.

SAWS apporte ici aussi une solution simple et efficace d'authentification forte. Cette approche est particulièrement efficace dans un environnement distribué, où différents systèmes d'exploitation coexistent.

SAWS s'intègre naturellement au standard SAML (Security assertion markup language) et au SAML Single Sign-On (SSO) Service for Google Apps[10] :



[10] Figure extraite de http://code.google.com/apis/apps/sso/saml_reference_implementation.html