

AUTHENTIFICATION FORTE

Usurper une identité? Impossible avec la biométrie!

Confidentialité et sécurité. Pour les banques privées, il ne s'agit pas là de vains mots. Mais bien des fondements de leur réputation, de la confiance que leur accordent leurs clients et, partant, de leur croissance. Reste que la sécurité et la confidentialité ne doivent pas empêcher l'efficacité, la compétitivité. Bien au contraire. Plongée au cœur du système mis sur pied par un établissement bien connu sur la place financière genevoise.

Sylvain MARET

CTO e-Xpert Solutions

Sylvain.maret@e-xpertsolutions.com

www.e-xpertsolutions.com

Comment concilier qualité des prestations et intégrité d'informations généralement très sensibles? Comment améliorer la rapidité de certaines tâches grâce à l'informatique, sans risquer de voir des données, relatives aussi bien à la clientèle qu'aux différentes activités de la société, tomber entre de «mauvaises» mains?

Objectif du projet

Pour offrir des services toujours plus performants à une clientèle exigeante et, partant, renforcer sa position face à la concurrence, une banque privée s'est intéressée à la manière qu'elle avait de garantir un accès hautement sécurisé à ses données sensibles. De s'assurer que seules les personnes autorisées puissent les consulter. Si l'authentification forte s'est rapidement imposée comme la solution à retenir, restait encore à définir le système le plus approprié. A déterminer le dispositif à même d'apporter la preuve irréfutable que l'utilisateur est bien le «bon», qu'il est celui habilité à connaître et manier les informations concernées. En d'autres termes, qu'il n'utilise pas le moyen d'authentification d'un autre ou qu'il ne prête pas le sien à un collègue.

Qu'est-ce que l'authentification forte?

Les méthodes classiques pour identifier une personne physique sont au nombre de quatre:

1. Quelque chose que l'on connaît: un mot de passe ou un PIN code;
2. Quelque chose que l'on possède: un «token», une carte à puce, etc.;
3. Quelque chose que l'on est: un attribut biométrique, tel qu'une empreinte digitale;
4. Quelque chose que l'on fait: une action comme la parole ou une signature manuscrite.

On parle d'authentification forte dès que deux de ces méthodes sont utilisées ensemble. Par exemple une carte à puce avec un PIN code.

Pourquoi cette méthode plutôt qu'une autre?

Le mot de passe? Il s'agit là du système le plus couramment retenu pour reconnaître un utilisateur. Il s'avère toutefois que celui-ci n'offre pas un niveau de sécurité optimal. Qu'il ne permet pas d'assurer une protection efficace de biens informatiques sensibles. Sa principale faiblesse réside dans la facilité avec laquelle il peut être identifié. Au nombre des techniques d'attaques destinées à briser un mot de passe, on peut citer l'écoute du clavier par le biais d'un logiciel malveillant (Key Logger) ou plus simplement encore, un Key Logger Hardware.

Quelle technologie choisir?

Un grand nombre de technologies d'authentification forte sont disponibles sur le



La technologie Match On Card permet le stockage d'informations biométriques sur la carte à puce.

marché. Celles de type «One Time Password» (Style SecurID), les cartes à puces et «token» USB cryptographiques ou encore la biométrie. C'est cette dernière qui a été retenue dans le cas qui nous intéresse. Avant tout pour répondre à une exigence fondamentale posée par le client. A savoir, garantir, de manière irréfutable, l'identité de l'utilisateur et rendre le système impossible à manipuler par une tierce personne.

Quel système de biométrie pour le monde IT?

Lecture de l'iris, de la rétine, reconnaissance faciale ou vocale, empreinte digitale. Quand

on parle de biométrie, différentes options sont envisageables. Le choix final a été guidé par le souci de trouver un compromis entre le niveau de sécurité (fiabilité) de la solution, son prix et sa facilité d'utilisation. Cette dernière contrainte était d'ailleurs une des principales clés du succès. L'adhésion des utilisateurs était, en effet, indispensable. Et celle-ci passait par la simplicité de fonctionnement, par la convivialité du dispositif. Le lecteur d'empreinte digitale s'est alors imposé assez naturellement.

Qu'en est-il de la sécurité?

La biométrie peut-elle être considérée comme un moyen d'authentification forte? La réponse est clairement non. Le recours à cette technique comme seul facteur d'authentification constitue certes une solution «confortable» pour les utilisateurs. Il n'en demeure pas moins qu'elle n'offre pas des garanties de sécurité suffisamment solides. Diverses études ont en effet montré qu'il est possible de falsifier assez aisément les systèmes biométriques actuels. Leur utilisation croissante par les entreprises et les gouvernements, notamment aux Etats-Unis, ne fait en outre que renforcer la détermination des hackers à en identifier les failles. C'est un des paradoxes de la biométrie.

Dès lors, il est judicieux de la coupler à un second dispositif d'authentification forte. Dans le cadre de ce projet, un support de type carte à puce a été retenu. Concrètement, l'utilisateur est identifié aussi bien par sa carte que par ses caractéristiques physiques (empreinte digitale, en l'occurrence). La première ne fonctionne que si elle est combinée aux secondes. L'ensemble offre ainsi une preuve irréfutable de l'identité de la personne.

Pourquoi une carte à puce?

La carte à puce présente l'avantage d'être une solution dynamique, évolutive. Elle permet en effet de stocker des identités numériques (certificat digital). Ce qui ouvre la porte à un grand nombre d'applications comme la signature électronique de documents, l'intégrité de transactions, le chiffre-

ment de données, la sécurisation de la messagerie et bien évidemment, l'authentification forte des utilisateurs. Le recours aux certificats digitaux constitue dès lors une base très solide pour construire la sécurité d'un système d'information. Par ailleurs, la carte à puce pave la voie vers d'autres utilisations potentielles, telles que le contrôle d'accès aux bâtiments (badge de proximité - RFID), le porte-monnaie électronique, etc.

Biométrie: où stocker les données?

La biométrie pose la question du stockage des informations relatives aux utilisateurs. Il s'agit là d'une question extrêmement sensible. Nombreux sont en effet ceux qui, à juste titre, s'interrogent sur l'usage qui est

fait sur la carte à puce. A recourir à une technologie qui rend le détenteur de la carte seul propriétaire de ses données biométriques.

Technologie Match On Card

La technologie Match On Card répond parfaitement à la problématique posée. Non seulement, elle permet le stockage d'informations biométriques sur la carte à puce mais elle assure aussi la vérification de l'empreinte digitale, directement sur cette dernière. Donnant ainsi aux utilisateurs un contrôle total sur les données les concernant. Cette approche a le mérite de susciter la confiance des personnes amenées à avoir recours au système. Elle répond, de plus, aux recommandations de Loi fédérale sur la protection des données (LPD 235.1) et de la CNIL (Commission nationale de l'informatique et des libertés) en France.

Retour d'expérience

Les technologies biométriques, à commencer par Match On Card, ont clairement un aspect avant-gardiste. Le développement, mené dans cette banque privée genevoise, a toutefois démontré qu'il est technologiquement possible de mettre en œuvre un système d'authentification forte basé sur la biométrie pour assurer une protection optimale de l'accès à des données extrêmement sensibles.

Reste que la technologie ne fait pas tout. La structure organisationnelle à mettre en place pour soutenir la technologie, pour assurer la gestion des identités, s'est ainsi révélée être un des défis majeurs posés par le projet. Le résultat, c'est une entité spécifique, dont la mission est de gérer l'ensemble des processus qui gravitent autour du système biomé-

trique: enregistrement des utilisateurs, gestion de l'oubli ou de la perte de la carte à puce, formation des utilisateurs, etc. Cette entité constitue un des piliers de la réussite du projet. L'authentification forte n'aurait, en effet, pas pu déployer tous ses effets sans la mise en place, en interne, de cette nouvelle structure. ■

S.M.



Le couplage carte à puce biométrie assure une sécurité optimale.

fait des données les concernant. Où celles-ci vont-elles être conservées? Qui y aura accès? L'information numérique permet-elle de reconstituer une empreinte digitale? Les réticences face à ce procédé sont réelles. Pour surmonter cet obstacle non négligeable à l'acceptation d'une telle solution par les utilisateurs, la formule choisie consiste à stocker les informations directe-