LE DIGIPASS: UNE TECHNOLOGIE BREVETÉE PAR VASCO

El Baaboua Florentina
Adresa: Str 9 Mai, Nr 49, Sector 6, Bucureşti Universitatea Româno – Americană Facultatea de Management – Marketing Email: pav_florentina@yahoo.com Telefon: 0766 301 547
Titrade Cristina
Adresa:Bld Lacul Tei, Nr 71, Bl 18, Sc B, Et 2, Ap 55, Sector 2, Bucureşti Universitatea Româno –Americană Facultatea de Informatică Managerială Email: cristina_titrade@yahoo.com Telefon: 0740 043 030
Sion Beatrice
Adresa:Str Aghireş, Nr 4, Sc B, Ap 17, Sector 2, Bucureşti Universitatea Româno –Americană Facultatea Economia Turismului Intern şi Internaţional Email: beatrice_sion@yahoo.com Telefon:0767 345 394
Mihalcescu Cezar
Adresa: Calea 13 Septembrie, Nr 104, Bl 48, Et 7, Ap 21, Sector 5, Bucureşti Universitatea Româno Americană Facultatea Economia Turismului Intern şi Internaţional Email: cezar_mihalcescu@hotmail.com Telefon:0722 387 162

VASCO Data Security lancement du Digipass un lecteur de cartes à puce offrant des fonctions d'authentification multiples en combinant la fonction "ce que vous voyez est ce que vous signez". Le DIGIPASS peut être utilisé pour de l'authentification, la signature digitale, et l'accès au réseau de l'entreprise. Il offre une authentification forte pour la banque en ligne, la banque par téléphone et les environnements de e-commerce. Le DIGIPASS peut être utilise tant en mode connecté que non connecté. En mode non connecté, le lecteur devient EMV-CAP et offre les fonctionnalités de mot de passe dynamique et de signature électronique du DIGIPASS.

Mots clée: accès sécurisé, authentification, signature digitale, crypté.

Présentation

VASCO Data Security International Inc., la société leader mondial en programmes de sécurisation spécialisé en produits d'authentification fait partie des leaders mondiaux de l'authentification forte avec plus de 10 millions de Digipass vendus.

VASCO conçoit, développe et commercialise des solutions « d'authentification de l'identité des personnes » basées sur l'utilisation de mots de passe dynamiques, à usage unique, générés par un token toutes les 36 secondes et modifiés à chaque utilisation, donc virtuellement impossible à pirater ou à forcer.

VASCO sécurise les réseaux d'entreprises et permet l'authentification forte DIGIPASS pour l'accès à distance (firewall, protocole Radius et serveurs d'accès) et aux utilisateurs de réseaux VPN ainsi qu'aux applications Web et personnalisées.

Le logiciel d'authentification de VASCO est intégré sur la "calculette" DIGIPASS de l'utilisateur final, ou sur son PC, son GSM ou d'autres appareils portables.

Côté serveur, les produits VACMAN de VASCO limitent l'accès de l'application à l'utilisateur DIGIPASS désigné.

Le marché cible de VASCO couvre les applications –et leurs centaines de millions d'utilisateurs- ayant recours aux mots de passe statiques.

Avec plus de 3.65 milliards d'utilisateurs de téléphones mobiles au niveau mondial, ces petits appareils sont devenus omniprésents dans la vie quotidienne. Les banques sont également conscientes de l'étendue de l'impact qu'a le téléphone mobile au niveau mondial et veulent tirer avantage de cette situation pour offrir de nouveaux services à leurs consommateurs. En conséquence, les applications de banque mobile sont devenues des solutions de plus en plus souvent mises en avant pour le retail banking. Avec le déploiement d'applications pour la banque mobile, un certain nombre de challenges sont mis en places. Parmi ces challenges, la sécurisation de l'application ou la facilité d'utilisation, permettant d'obtenir à la fois un niveau élevé d'acceptation auprès du consommateur et en même temps, générer un revenu suffisant pour la banque.

Avec le Digipass pour Mobile et le Digipass pour Java C API, VASCO offre une réponse aux questions de la sécurité d'acceptation par l'utilisateur des opérations de banque mobile. Le Digipass pour Mobile offre deux applications d'authentification. Le première est le code d'authentification «response only», la seconde application peut être un code d'authentification «Challenge/response» ou la signature électronique. VASCO est la première société qui offre une gestion du temps complète et automatique dans un système d'authentification mobile. Le Digipass pour Mobile se synchronise avec le server sur base de l'horloge, offrant ainsi une authentification encore plus sécurisée que les solutions d'authentification basées uniquement sur l'évènement. Le Digipass pour Mobile offre également une fonction d'adaptation automatique aux changements d'heures et une synchronisation automatique, facilitant l'utilisation de l'authentification forte pour les voyageurs chevronnés.

La facilité d'utilisation est un élément clef pour l'acceptation par l'utilisateur de l'application de banque mobile. A travers les années, VASCO a développé une large expérience en déploiements de grandes quantités pour les utilisateurs finaux. Cette expérience se traduit par les meilleures solutions disponibles. L'installation (disponibilité)

est rapide (moins de 2 minutes), sécurisée (totalement crypté) et peut être fait dans un univers en ligne (utilisant le HTTP ou SMS) ou en mode non connecté (manuel).
Les banques peuvent customiser le Digipass pour Mobile et le Digipass pour Java & C API à leurs propres couleurs. Les logos, couleurs, icônes, caractéristiques, et menu peuvent être facilement adaptés afin d 'augmenter la reconnaissance de la marque aux yeux de l'utilisateur final. De plus, le Digipass pour Mobile et le Digipass pour Java & C API supportent toutes les langues ? La customisation offerte offre à l'utilisateur final une expérience mobile riche et facile d'utilisation.
Le Digipass pour Mobile permet l'authentification à deux facteurs et les fonctions de signatures électroniques pour les combinés Java, Palm et Blackberry et supporte plus de 400 types différents de téléphones mobiles. L'utilisation du Digipass pour Mobile ne requiert aucun déploiement ou programme additionnel côté utilisateur final et peut être utilisé en combinaison avec d'autres solutions Digipass afin de mieux servir les besoins et désirs des clients.
Le Digipass pour Java & C API a été développé pour les banques et intégrateurs. Il offre la possibilité d'intégrer la technologie bien connue du Digipass dans quasi tout environnement. Le Digipass pour Java & C API intègre de manière totalement transparente les fonctions d'authentification forte et de signature électronique dans les applications de banque mobile tout en se basant sur l'infrastructure «backend» existante et en la maintenant.
Le Digipass pour Mobile et le Digipass pour Java &C API sont des produits qui se basent sur la technologie côté server qui a déjà fait ses preuves de VASCO, le VACMAN Controller. L'utilisation du Digipass pour Mobile ne requiert que peu ou prou de mise à jour du server.

Grâce au VACMAN et au DIGIPASS, vous bénéficiez d'un accès sécurisé à diverses applications Internet, de l'entreprise et du VPN (Virtual Private Network).
Le VACMAN Middleware est une gamme de programmes qui rendent l'authentification possible. L'utilisateur s'enregistre avec son nom d'utilisateur et le mot de passe généré par le DIGIPASS. Le VACMAN vérifie la requête d'authentification de l'utilisateur avant de lui accorder l'accès. Avec le VACMAN vous pouvez également gérer l'administration centrale des différents utilisateurs. Simple et facile d'utilisation donc!

Le VACMAN Middleware: une plateforme, plusieurs applications différentes
- Une authentification sans histoire;
- Un développement tenant compte des demandes des petites, moyennes et grandes enterprises;
- Une integration, une maintenance et un contrôle facile;
- Pas d'installation de programme nécessaire sur le PC des utilisateurs;
- Des coûts extrêmement bas pour l'intégration et l'utilisation;
- Une seule plateforme d'au thentification pour différentes applications;

Le principe du DIGIPASS: un mot de passe dynamique unique
Presque la totalité des applications dans l'environnement professionnel quotidien exigent une authentification. La plupart de ces applications utilisent encore toujours un mot de passe statique simple (p.ex.: le nom de votre animal familier préféré). Ce type de mot de passe peut être facilement cracké par des hackers et rendent donc votre information non sécurisée.
Le DIGIPASS en fini totalement avec ce problème. Il calcule pour vous un mot de passe dynamique qui ne peut être utilisé qu'une seule fois. Vous utilisez le mot de passe pour vous enregistrer. Votre nom d'utilisateur et votre mot de passe sont ensuite vérifiés par le programme placé sur le server, le VACMAN. Si les données sont correctes, vous pourrez accéder à vos applications sécurisées.
Le DIGIPASS fonctionne sur le principe du temps. Toutes les 36 secondes, un nouveau mot de passe est généré. Cette combinaison entre le principe du temps, le mot de passe dynamique utilisable une seule fois et la vérification par le server des codes générés par le DIGIPASS, rendent l'accès à vos informations confidentielles, aussi vrai qu'impossible.

Jeton de l'authentification basée sur la plate-forme
DIGIPASS est une authentification à deux facteurs plate-forme qui permet aux utilisateurs de s'authentifier eux-mêmes à des systèmes (tels que les permis DIGIPASS-bancaires sur Internet ou E-commerce sites) en utilisant les identifiants générés par les appareils de poche. Le système est basé sur la combinaison de matériel jetons possédés par l'utilisateur et des outils logiciels d'authentification sur le serveur du côté de reconnaître que la génération des clés d'identification généré par l'utilisateur jetons.
En bref: un utilisateur d'authentifier un DIGIPASS-système de permis en fournissant leur nom d'utilisateur, en combinaison avec une seule fois le mot de passe qui est généré à la volée par le matériel qu'ils possèdent symbolique.
Autre identification comprennent défi / les mécanismes de réponse, lorsque le serveur génère un code qui est inscrit sur le matériel, avec un code de réponse a ensuite présenté sur l'appareil que l'utilisateur retourne à la salle d'attente du serveur, ou une signature numérique dans lequel le processus de utilisateur entre de multiples pièces

d'informations sur les transactions relatives à la tâche qu'ils exécutent (tels que le numéro de pièce, la quantité et le montant en dollars dans une transaction de commerce électronique) et du matériel périphérique génère un code unique qui peut être confirmé par le serveur.
Dans tous les cas, le logiciel serveur est capable de reconnaître que la condition ID généré par le matériel périphérique comme faux ou authentiques, permettant l'identification basée sur l'ID utilisateur est connu et le matériel qu'ils possèdent. Acès par l'utilisateur de l'appareil lui-même peuvent aussi être protégés par un utilisateur PIN.
Les jetons eux-mêmes - appelés jetons Digipass - sont offertes par le vendeur dans une variété de saveurs, de petits seule touche keychain dispositifs qui génèrent une seule fois les mots de passe, à la pleine taille de poche avec clavier alphanumérique complet et un soutien pour les cartes à puce. En outre, le vendeur propose un Pocket PC, Palm, JavaPhone, Windows et des logiciels basés sur les implémentations de logiciels permettant la génération d'un temps de clés d'identification sur les PC ou ordinateurs de poche, un "Virtual Digipass" processus dans lequel le composant serveur envoie les identifiants de l'utilisateur via SMS et le Digipass pour WEB (DP4WEB), dans lequel l'utilisateur registres en ligne et reçoit un login sécurisé applet (Java-based) et un cookie qui stocke leur DIGIPASS secret sur leur PC lui-même.

Qu'est ce qu'un eID?
Votre eID est votre carte d'identité téléphonique. Cette carte contient les mêmes informations que celles qui se trouvent sur votre ancienne carte d'identité. Mais l'eID est bien plus que ça!

Que fait l'eID?
La carte d'identité électronique à 2 grandes applications:
L'Authentification: vérifier que la personne qui s'annonce est bien celle qu'elle prétend être. L'eID vous permet donc de vous identifier (à distance) et vous donne accès à différentes applications à l'intérieur de votre entreprise, organisation ou commune.
La signature digitale: grâce aux certificats présents sur votre eID, vous pouvez signer de manière électronique des documents électroniques sans vous déplacer physiquement. Cette signature digitale a le même poids légal que la signature traditionnelle écrite.
Le processus suivi lors du passage des transactions: a chaque fois que vous effectuez une transaction, vous devez passer par plusieurs étapes qui représentent autant de contrôles :
-tout d'abord, vous devez remplir le premier écran qui est un **écran de saisie**. Après l'avoir complété, vous avez le choix : soit vous annulez l'opération, soit vous envoyez vos données;
-vous vous trouvez maintenant devant un **écran de confirmation** qui vous offre le choix entre trois options : annuler, modifier et confirmer
-si vous confirmez, le système vous demandera de valider votre opération en encodant le ID. A ce stade, vous pouvez soit encore annuler l'opération, soit l'envoyer pour qu'elle soit exécutée.
Après envoi, vous recevrez un **écran de notification** reprenant la référence sous laquelle la transaction a été enregistrée. (Si la communication a été interrompue avant l'apparition de ce dernier écran, votre transaction n'a peut-être pas été enregistrée. Pour vous assurer si votre transaction a été enregistrée ou non, contrôlez votre Order Book (en cours) pour voir si votre transaction a été enregistré ou non.

Les avantages du Digipass:
Une sécurité accrue: le Digipass offre une solution d'authentification forte, d'accès et de transactions sécurisées. Il est parfaitement adapté pour protéger l'accès aux ordinateurs de bureaux et pour sécuriser les données par le biais de la signature digitale. Chaque opération de signature demande un code PIN. Ce petit appareil personnel génère pour vous une signature électronique qui vous permet de vous connecter, de signer vos opérations. Il calcule une nouvelle signature à chaque utilisation, ce qui vous garantit une sécurité optimale.
Réduire les coûts: le Digipass offre les mêmes capacités qu'une carte à puce avec l'avantage de ne pas avoir à investir dans un lecteur de cartes à puce. De plus, il a été développé pour les déploiements de masse. Il suit les standards en matière d'envois postaux ce qui rend les envois postaux plus faciles dans les cas de déploiements de masse.
Facilité: le Digipass a été développé pour simplifier les opérations dans la complexité des environnements PKI; le Digipass est facile d'utilisation. C'est un Digipass de petite taille et léger ce qui le rend ultra-portable, et ainsi, améliore la mobilité de l'utilisateur. Il peut également être utilisé par des utilisateurs sur différents postes de travail.

Bibliographie

1.www.vasco.com
2. http://fr.wikipedia.org/wiki/Accueil
3.www.toolinux.com
4. www.mag-securs.com