Keynectis porte le certificat électronique sur clé USB

« Le certificat est la base de l'identité numérique », proclame Pascal Colin, directeur général de Keynectis, entreprise spécialisée dans l'émission de certificats électroniques. Poussé par l'administration (notamment la télédéclaration des revenus imposables sur laquelle s'est développé Keynectis), l'industrie, les services et les banques, le certificat électronique est en voie de démocratisation. *« La certification électronique est un vrai marché »*, insiste le dirigeant.

Mais pour que son usage se démocratise, notamment auprès des particuliers, il restait à le rendre simple à utiliser et peu onéreux. C'est tout l'enjeu de K.Access, une solution de certification développée en juin 2009 et en cours de tests en phase pilote. Elle vise notamment à répondre simplement aux directives de la Banque de France qui pousse les établissements financiers à mettre en œuvre des solutions d'authentification forte (au-delà du simple login/mot de passe habituel) pour sécuriser les opérations en ligne.

Création instantanée du certificat

Solution brevetée, K.Access permet d'inscrire un certificat électronique sur un périphérique de stockage USB (clé, téléphone portable, baladeur numérique, etc.). La solution permet ainsi à l'utilisateur de s'authentifier (de manière forte, donc) en connectant simplement sa clé USB (ou son téléphone…). Pour l'heure, K.Access ne fonctionne que sur Windows et Mac OS. Son portage sous Linux est *« une question de marché plus que technique »*. Et son développement sur les smartphones est une question de temps.

La richesse de la solution tient notamment dans la création immédiate du certificat. Pour cela, il suffit à l'émetteur du certificat (la banque par exemple) d'adresser un « code de retrait » ou « d'initialisation » à l'utilisateur. Code à saisir, en ligne, lors de la demande du certificat K.Access. Lequel est ensuite livré dans un container sécurisé bâtit à partir de « l'ADN » du support d'enregistrement (le numéro de série de la clé USB, par exemple). Un code PIN, laissé au choix de l'utilisateur, permet de valider l'utilisation du certificat contenu sur la clé USB.

Choix du support et code PIN laissé à l'utilisateur

Outre sa simplicité d'usage, K.Access présente l'avantage de laisser à l'utilisateur le choix du support (ce qui évite la distribution des produits physique et de leur support par l'entreprise), le choix du code pin (qu'il n'est donc pas nécessaire d'envoyer) et la possibilité de révoquer rapidement (en ligne) un certificat en cas de perte ou vol du support et d'en demander un nouveau dans la foulée. Par ailleurs, il ne nécessite aucune installation sur le poste client qui ne conserve aucune trace de l'opération une fois la clé retirée. Enfin, la connexion au site émetteur du certificat est automatique ce qui préviendra toute tentative de détournement en ligne (phishing, man in the middle, etc.).

« K.Access va répondre aux besoins du monde bancaire en particulier et Internet en général », assure **Bernard Delbourg**, P-dg de Mediscs, la société partenaire de Keynectis à qui il fournit le container

numérique. La solution pourrait en effet se décliner pour les sites de e-commerce comme PriceMinister ou Ebay qui seraient alors en mesure de confirmer les transactions en authentifiant leurs utilisateurs. Une authentification qui pourrait également intéresser les sites de réseaux sociaux. Twitter, par exemple, commence à proposer l'authentification de comptes, pour le moment limitée aux personnalités publiques.

Un concurrent de SMS OTP

« K.Access est le premier étage de solutions plus complètes à venir », souligne **Anne Murgier**, directrice commerciale de Keynectics qui évoque l'intégration possible d'autres services comme la signature électronique, le paiement en ligne 3DSecure, le coffre fort électronique…

Enfin, le coût d'accès rend la solution très accessible. Il est de **2 euros par utilisateur et par an pour 50 000 certificats** et 1 euro à partir de 500 000 émissions. *« La banque ne paie que pour les certificats réellement créé »*, précise Pascal Colin. Dans ce cadre, **K.Access vient concurrencer les solutions de sécurité SMS OTP** (code envoyé par SMS) et autres token générateurs d'OTP. Mais sans prétendre atteindre le niveau de cryptographie de la carte à puce. *« K.Access vise le marché de la sécurité par SMS mais en moins cher et plus sécurisé »*, résume Pascal Colin.

Depuis son lancement en 2004, Keynectis assure avoir émis 25 millions de certificats. Une goutte d'eau par rapport au 10 millions de certificats que l'entreprise déclare pouvoir émettre quotidiennement. K.Access l'y aidera-t-elle?

K.Access, une certification hautement sécurisée K.Access repose sur des certificats électroniques **X509 V3** sur infrastructure à clés publiques (**PKI**). Le container du certificat est généré depuis les serveurs de Keynectis lors de l'initialisation du support. Ce qui rend le container unique et non duplicable. L'authentification utilise des clés **RSA 2048** (génération sur **matériel HSM certifié EAL4+**). Keynectis précise que *« le paquetage client virtualise les fonctionnalités d'une **Smart Card** avec des mécanismes de protection de la clé privée spécifiques »*. Une virtualisation lgociel qui ne prétend pas encore atteindre le chiffrement matériel. L'industrie de la carte à puce a encore de beaux jour devant elle…

—

CARTES & IDentification 2009. Venez participer au rendez-vous mondial de la carte à puce, de la sécurité numérique, de l'identification et des technologies intelligentes. Pour vous inscrire, consultez le programme, les dates et lieux de ce rendez-vous.