

Biométrie: la Vérification se fait maintenant dans la carte Java

(Electronique international Hebdo – 16 décembre 1999 – n° 373)

Oberthur Smart Card et la société française Id3 viennent de démontrer la possibilité d'obtenir un très haut niveau de sécurité et de confort dans la génération d'une signature électronique grâce à un mariage original de la biométrie et de la carte à puce.

Les techniques de la carte à puce et de l'identification biométrique sont à la recherche du mariage idéal. Sagem (Morpho Systèmes) est aujourd'hui le premier à avoir sauté le pas industriel en développant un terminal de paiement combinant la carte à puce (ou une carte magnétique pour le marché américain) et un capteur d'empreinte (*voir notre numéro du 27 mai*). L'industriel français a en effet montré lors du dernier salon Cartes, qui s'est tenu à Paris mi-novembre, l'utilisation d'une carte à puce supportant en mémoire plusieurs applications différentes, ainsi que, l'empreinte digitale (250 octets) du porteur de la carte, utilisée comme clé d'accès à ces applications. Lisible sur différents types de terminaux (terminal de paiement classique ou avec capteur d'empreinte, téléphone mobile), cette carte utilise ainsi l'empreinte à la place du code personnel lorsque le terminal s'y prête (des développements sont en cours pour intégrer ce type de capteur dans un téléphone mobile). La vérification (la corrélation entre l'empreinte stockée et l'empreinte acquise) se fait dans le terminal.

Vers la mise au point d'un circuit spécifique

Employant le même schéma d'utilisation combinée de la carte à puce et des techniques biométriques, Oberthur Smart Card et la société française Id3 ont montré de leur côté, également au salon Cartes, mais sur un prototype cette fois-ci, une autre version de ce mariage de la carte et de la biométrie. Utilisant un capteur thermique d'empreinte (le capteur FingerPrint de Thomson-CSF, qui offre une définition typique de 500dpi), ils ont ainsi démontré la possibilité de réaliser la vérification de l'empreinte (le *matching*) non pas dans le terminal, mais dans la carte elle-même. Un gage supplémentaire de sécurité. Et de surcroît avec des performances acceptables en vitesse de traitement (entre 1 et 2 secondes) et en résultats (1 fausse acceptation sur 100 000 et 1 faux rejet sur 100). Oberthur Smart Card a pourtant développé l'algorithme de vérification sous la forme d'une applet Javat de quelques kilo-octets qui est exécutée dans une machine virtuelle JavaCard, c'est-à-dire avec des performances nécessairement dégradées par rapport à des solutions qui auraient utilisé du code natif et un système d'exploitation propriétaire. La carte utilisée (AuthentIC)(1) était une carte disposant d'un cryptoprocasseur capable d'exécuter des algorithmes à clés publiques. Les performances atteintes avec cette économie de moyens doivent en réalité beaucoup à la qualité de l'acquisition et du traitement des images d'empreintes réalisées par id3, et assurées dans le capteur par deux circuits spécifiques que la petite société, spécialisée dans la conception de circuits dédiés et l'industrialisation de solutions complètes, a développés elle-même. Ce traitement n'est pas, semble-t-il, traditionnel, puisqu'il n'exploite pas les *minutae* (2) des empreintes pour réaliser les extractions significatives qui servent à la vérification, mais d'autres formes caractéristiques. Id3, qui se montre très discrète sur les techniques utilisées, compte porter rapidement son savoir-faire dans un seul circuit, qui sera alors dédié à ce type d'applications.

(1) Cette carte peut supporter JavaCard mais aussi Smart Card for Windows ; elle dispose également d'interfaces PKI (PKCS #11, signature numérique). Dans l'application citée, elle sert à signer des e-mails.

(2) Les "*minutae*" sont des points d'intersection caractéristiques (définis en X, Y et par un angle) de l'empreinte *e*; elles sont utilisées pour caractériser ces dernières sous forme de "*templates*" (extractions de formes caractéristiques).