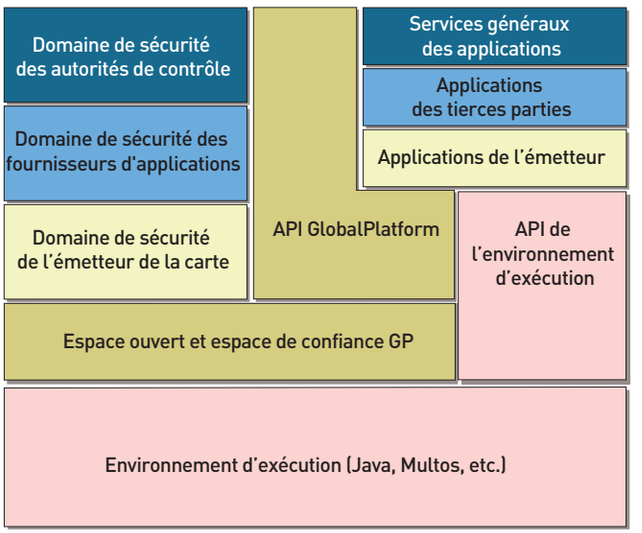
OS et standards logiciels : la nouvelle donne

Les marchés émergents du sans-contact, de l'identité et de l'authentification forte pèsent sur l'évolution des grands standards de la carte et favorisent l'entrée de nouveaux acteurs.

Le salon Cartes a été l'occasion d'un certain nombre d'annonces clés qui confirment l'adoption, par l'industrie de la carte, de systèmes de plus en plus ouverts, dont JavaCard était jusque-là la plus emblématique des illustrations. La présentation par Gemplus d'une implémentation de la plate-forme .Net *(voir encadré)* sur une carte à puce au format " clé USB ", récompensée par le Sésame du meilleur logiciel, confirme aujourd'hui cette tendance lourde initiée avec le JavaCard Forum dès 1997 et confortée depuis 1999 par les travaux de GlobalPlatform, en y apportant une dimension supplémentaire : des standards reconnus du monde du PC peuvent être implémentés tels quels dans une carte à puce. Une tendance à laquelle l'Académie (le Cnam et l'ENST en France) apporte aussi sa contribution pour explorer de nouvelles voies en utilisant des standards établis dans le monde du PC ou du mobile, futurs piliers d'un monde complètement ouvert à tous les développeurs et offrant une interopérabilité entre les différents fournisseurs de cartes, de lecteurs et de systèmes. Les développements conduits à l'ENST Paris (Open EAP SmartCard) par Pascal Urien, autour des protocoles du monde du Wi-Fi et Wimax (EAP-TLS, AKA, PSK), en sont ainsi une autre illustration. Ces développements s'accompagnent en outre d'une démarche inédite de type Open Source, puisque le code source de ce projet est accessible sur Internet (1), et peut être téléchargé et installé sur la carte à puce de son choix pour sécuriser ses accès sans fil. Une première dans l'industrie de la carte. Ces évolutions s'inscrivent dans le droit-fil des futures cartes IP et USB, embarquant des serveurs Web (Axalto, Gemplus, Oberthur Card Systems, G&D) et offrant une connectivité Internet similaire à celle du petit PC. Avec la sécurité en plus.

Une architecture pour les multiapplications



La Card Specification v.2.2 de GlobalPlatform offre pour la première fois des services de PKI pour authentifier la carte, et surtout une gestion dynamique des droits et privilèges attachés aux domaines de sécurité de l'émetteur et des fournisseurs d'applications.

Ouverture au monde du PC et du mobile

Ces développements tombent à pic. Ils ouvrent le monde de la carte et de ses arcanes (les APDU), jusque-là très spécifiques, à une population de développeurs familiers de la plupart des langages évolués (Java, Visual Basic, C, C++, C#, etc.) du monde du PC ou du mobile. A un moment où, précisément à cause de l'extension prise par les applications de la carte dans le domaine de l'identité et du sans-contact notamment, le besoin en développement d'applications se fait sentir avec une acuité inédite. Les marchés émergents dictent désormais la donne en matière de systèmes d'exploitation, de standards et de spécifications logicielles.

La version 2.2.2 des spécifications JavaCard, annoncée par Sun Microsystems au salon, répond ainsi au besoin des marchés émergents de l'identité et du sans-contact, et prépare la version 3.0 " full Java " annoncée pour la mi-2007 (2). C'est également le cas de la version 2.2 de la " Card Specification " de GlobalPlatform, encore en discussion, et dont la publication est prévue en début d'année. Outre le fait qu'elle soit très orientée comme la dernière version de JavaCard sur le sans-contact (compatibilité avec les cartes à interface double, contact et sans-contact), et pour la première fois intègre des mécanismes pour utiliser de la cryptographie à clés publiques (PKI), elle offre une plate-forme très sécurisée de gestion d'applications issues d'horizons divers sur la même carte. En renforçant son concept de " domaine de sécurité " *(voir schéma)*, elle pourrait ainsi permettre à une carte d'identité d'accueillir en téléchargement des applications développées par une autre autorité que celle du ministère qui aurait émis la carte, par exemple. Ou à une carte SIM d'accueillir des applications de banque en ligne.

Enfin, ultime et importante conséquence de l'émergence des marchés de l'identité et du paiement sans contact notamment portés par des travaux de spécifications et de standardisation de plus en plus ouverts, la chaîne de la valeur de la carte à puce s'ouvre à de nouveaux acteurs. Les banques américaines se tournent vers leurs fournisseurs traditionnels de cartes magnétiques pour évoluer vers le sans-contact grâce aux spécifications PayPass, tout comme les gouvernements se tournent vers leurs imprimeries nationales, des intégrateurs systèmes ou des encarteurs locaux pour émettre des cartes d'identité. Quand ils ne se tournent pas directement vers les fabricants de cartes. Le marché s'élargit donc, mais il entraîne avec lui des fournisseurs de modules (circuit plus son OS) et de systèmes d'exploitation " sur étagère " que ces encarteurs ou ces intégrateurs n'ont ni le temps ni les ressources de développer. D'autres scénarios dans le monde du GSM favorisent l'entrée de ces acteurs, dont la visibilité était jusque-là réduite. Les Trusted Logic, Aspects Software, Inseal, SC2, EDSI et IBM deviennent du coup autant de " Microsoft " de la carte à puce.

YVON AVENEL

(1) http://www.infres.enst.fr/~urien/openeapsmartcard/.

(2) Une version qui sera pour la première fois un vrai Java (fichiers .jar et non .cap, ramasse-miettes, multithreading, etc.), un sous-ensemble du J2E ou J2ME, comparable au .net kernel par rapport à sa version desktop.

L'IMPLANTATION LA PLUS COMPACTE DE LA PLATE-FORME .NET DE MICROSOFT

→ A l'occasion du salon Cartes 2005, Gemplus a présenté des prototypes de "dongles" USB et de cartes à puce embarquant une implantation particulièrement compacte d'un environnement d'exécution .Net, implantation néanmoins en totale conformité avec la norme ISO/ECMA-335, qui caractérise l'environnement pour services Web de Microsoft.

→ La solution présentée offre un ensemble de fonctions qui garantissent une intégration transparente et aisée d'objets sécurisés communicants dans une infrastructure informatique existante. Elle devrait également contribuer à préparer les infrastructures du futur, basées sur la gestion d'identité numérique, les services Web et les architectures orientées services (SOA).

→ Parmi les principales caractéristiques de l'implantation logicielle, on notera la connectivité TCP/IP, le support du format de fichier .Net standard (sans convertisseur externe donc), la prise en charge de l'exécution simultanée de plusieurs applications et la libération automatique de la mémoire. P.A..