Yvon Avenel
Journaliste
Éditeur de
SmartcardsTrends

APPLICATIONS BANCAIRES MOBILES

Les environnements multi-émetteurs réclament de nouveaux modèles d'assurance

La "sécurité ouverte", c'est-à-dire celle des applications tournant dans des des environnements ouverts, devient un nouveau défi. Les solutions doivent être rapidement trouvées pour accompagner la montée en volume annoncée du marché des applications NFC prévue début 2010. Pour cela des travaux ont été lancés en avril 2008 au sein et autour du projet EPOMI.

La modernisation des procédures d'évaluation et de certification des niveaux de sécurité et d'assurance des systèmes embarqués, dont le téléphone mobile est un peu devenu le prototype, et celle des cartes à puce, est à l'ordre du jour. La nécessité fait loi car il y a une certaine urgence. Le déploiement annoncé en volumes [1] de cartes SIM non seulement multi-applicatives mais multi-émetteurs, dans les téléphones mobiles, d'une part, et, de l'autre, les exigences en matière de sécurité formulées par les banques [2] pour déployer des applications de paiement dans ces environnements, l'impose. Tirée par la technologie NFC (Near Field Communication) et ses applications dans le domaine du paiement bancaire et privatif ou du transport (*e-ticketing*), mais tirées aussi par de nouvelles applications du "sans fil" comme le développement en Europe du DVB-H et de la TV à péage dans les téléphones mobiles, cette évolution est au cœur de débats qui se poursuivent dans différentes instances entre banques, commerçants, opérateurs de transport, fournisseurs de services de contenus et opérateurs de téléphonie mobile. Les difficultés soulevées par l'émergence de ces nouveaux environnements sont devenues critiques en termes de sécurité. Elles se posent en termes de logistique – qui émet la carte lorsqu'il y a plusieurs émetteurs ? Qui gère les cartes et leurs applications et selon quelles exigences de sécurité ? Mais elles se posent aussi au niveau des procédures d'évaluation et de certification sécuritaires elles-mêmes (*encadré 1*). Évaluer et certifier une mono-application bancaire, mono-émetteur reste un exercice long et coûteux. Utiliser le même schéma pour une plateforme multi-applicative et multi-émetteur devient un véritable défi en termes de complexité, de délais et de coûts.

COMBINER OUVERTURE ET SÉCURITÉ

Comment gérer des applications bancaires et des cartes SIM dont les cycles de vie sont différents et dont on ignore au moment de l'évaluation sécuritaire des cartes (celle du microcontrôleur, du système d'exploitation, de la machine virtuelle s'il s'agit d'une carte Java), les applications (*applets*) qu'elles seront appelées à héberger ? Comment éviter les travaux de réévaluations et les re-certifications longues et coûteuses dès qu'un changement survient dans la cible d'évaluation et de certification ? Ces difficultés sont aujourd'hui identifiées par l'industrie et font l'objet de plusieurs initiatives qui visent à leur trouver des solutions. Les défis qu'elles posent sont à la hauteur des enjeux : il s'agit ni plus ni moins de garantir des niveaux de sécurité élevés (jusque-là établis pour des environnements assez fermés) mais cette fois-ci dans des environnements ouverts dont l'Internet est devenu le modèle. Une première et presque une contradiction dans les termes, si l'on conçoit que la sécurité reste associée à l'image du coffre-fort ou du "mur" (*firewall*). Ouverture et sécurité ont rarement fait bon ménage. Mais il s'agit aussi d'optimiser les procédures d'évaluation et de certification actuelles (de type Critères Communs, *voir l'encadré 2*) qui, si elles étaient transposées aujourd'hui telles quelles aux environnements ouverts des applications NFC ou de TV à péage mobile, pourraient remettre en cause les modèles économiques sur lesquels ces écosystèmes doivent se construire et se viabiliser. La sécurité ouverte devient ainsi un nouveau défi pour l'industrie. Avec un objectif en terme d'échéance : les solutions doivent être trouvées et expérimentées d'ici un an et demi pour accompagner l'augmentation des applications NFC – de paiement notamment – prévue début 2010.

UNE ÉVALUATION MODULAIRE

Le projet d'Évaluation plateforme ouverte modulaire et incrémentale (EPOMI) a été lancé en France en avril 2008 et regroupe plusieurs acteurs importants des futurs marchés du NFC mobile et de la TV à péage. Il représente l'initiative la plus importante qui ait jamais été lancée pour établir les bases

1. RÉACTIVITÉ ET SÉCURITÉ

Applications à la demande et architectures orientées services

Les possibilités offertes par les futures cartes SIM multi-applicatives et multi-émetteurs sont encore loin d'avoir été toutes explorées. La capacité de pouvoir, à la veille d'un week-end à Londres, télécharger sur son mobile l'application de transport Oyster (Mifare) de façon à pouvoir circuler sans encombre dans la capitale anglaise, puis supprimer cette application le lundi et utiliser à nouveau l'application parisienne Navigo (ISO1443 Type B'), créé des usages basés sur la composition de services à la demande dont la richesse peut se décliner à l'infini. Mais ces architectures orientées services supposent des systèmes de confiance éprouvés. C'est tout l'objet du projet EPOMI d'offrir les outils pour les évaluer et les certifier, de façon à pouvoir faire passer dans les usages à la fois la réactivité réclamée par les utilisateurs et la sécurité capable d'assurer la disponibilité et la confiance dont ces services ont besoin.

« Le projet EPOMI représente l'initiative la plus importante qui ait jamais été lancée pour établir les bases d'une évaluation de la sécurité d'environnements ouverts. »

d'une évaluation de la sécurité des systèmes et des environnements ouverts, tablant sur la capacité à mener des évaluations sécuritaires modulaires. Si une application est certifiée de son côté à un niveau d'évaluation donné, et qu'une plateforme l'est également par ailleurs à ce niveau, peut-on affirmer que l'ensemble application et plateforme le sera au même niveau ? "*Les problèmes posés aujourd'hui avec les transactions mobiles viennent du caractère "ouvert" des environnements multi-applicatifs, et de l'évolution rapide des téléphones mobiles*, résume Jean-Claude Pailles, de France Telecom R&D, le chef de file du projet. *De cela, il en résulte une combinatoire « explosive » des configurations possibles entre les différentes applications et leurs versions respectives, les différents types de téléphones mobiles, et les différents types d'éléments sécurisés et leurs fournisseurs, embarqués dans les téléphones mobiles. Cela pourrait conduire à un nombre et une fréquence des évaluations sécuritaires bien trop élevés pour pouvoir être supportés à un coût acceptable par les opérateurs de téléphonie et les fabricants de cartes SIM. La seule solution serait de réduire l'adhérence entre les applications et la plateforme*, poursuit Jean-Claude Pailles. *Il faut pour cela que l'indépendance entre les dispositifs de sécurité et les systèmes d'évaluation d'assurance soit assurée entre la plateforme et les applications qu'elle est susceptible d'héberger et de faire tourner.*"

LES TROIS AXES DE TRAVAIL DU PROJET EPOMI

Trois axes de travail ont été définis au sein du projet EPOMI (*encadré 3*). Le premier vise à définir une approche commune à toutes les applications (paiement, *e-ticketing*, TV à péage), de l'analyse et de la gestion du risque et son assurance, pour l'environnement mobile. Il s'agit d'évaluer – à partir d'architectures matérielles et logicielles définies, d'usages bien spécifiés et de standards établis – les menaces possibles pour établir ensuite des scénarios de parade. Il faut, de plus, quantifier les aspects risques et assurances. Ceci implique la définition de niveaux d'exigences en matière de sécurité. "*Il faudra prendre en compte le fait que le mobile n'est pas seulement une carte à puce, mais que sa connectivité quasi permanente apporte un avantage qu'il reste à mesurer*", souligne Jean Claude Pailles.

Le deuxième axe de travail vise plus directement l'évaluation sécuritaire et la définition de méthodes d'évaluation modulaires et incrémentales qui doivent permettre de minimiser en termes de coûts, de temps et de fréquences, les travaux d'évaluation en dépit du nombre élevé de combinaisons possibles entre les différentes versions de cartes et d'applications qu'un opérateur pourrait avoir à gérer. L'idée est d'évaluer d'un côté une plateforme, qui est aujourd'hui, dans la plupart des cas, une carte SIM Java répondant aux spécifications GlobalPlatform, avec un jeu d'API, et de l'autre des applications de sorte que leur assemblage soit aussi sécuritaire que chacun des éléments évalués séparément. "*Le point critique est de parvenir à s'assurer que les API sont intimement sûres*", indique Jean-Claude Paillés. Mais il faudra aussi réussir à faire coexister des applications sensibles avec des applications qui le sont moins, et pour lesquelles les exigences en matière de sécurité sont moins élevées. "*Il faut pourvoir s'assurer qu'une application peu sensible ne peut pas devenir le vecteur d'attaques en direction d'une application sensible embarquée avec elle dans la même carte*", note Jean-Claude Paillès.

Le troisième axe de travail sera la mise en œuvre des procédures et des outils développés dans les deux autres groupes de travail. Il est prévu qu'un premier niveau d'évaluation de ces travaux soit effectué avec des *applets* déjà disponibles et des plateformes Java qui seront développées par les trois fabricants de cartes à puce impliqués dans le projet. Le projet court sur 18 mois, ce qui signifie que les résultats seront publiés en septembre 2009, et que les premiers produits répondant aux spécifications et au "standard" EPOMI ainsi établis pourraient être commercialisés dès le début 2010. Ce standard n'a pas vocation à se présenter comme une proposition de révision des procédures actuelles d'évaluation et de certification des Critères communs (ISO/IEC 15 408), mais plutôt comme un *addendum* sous la forme d'un profil de protection (PP) accompagné d'outils et de méthodologies d'évaluation.

MODERNISER LES PROCÉDURES D'ÉVALUATION

C'est une approche assez similaire que les laboratoires "sécurité" de Gemalto, le premier fabricant mondial de cartes à puce et fournisseur de services de sécurité, ont adoptée en lançant récemment des travaux pour, eux aussi, proposer de "moderniser" les procédures d'évaluation et de certification des Critères communs afin de surmonter

2. LE SYSTÈME D'ASSURANCE INTERNATIONAL

Les Critères communs : un standard pour des preuves formelles

Les Critères communs sont un standard international (ISO 15 408) établi pour évaluer la sécurité des systèmes d'informations. L'évaluation porte sur une cible (TOE pour *target of evaluation*) qui, dans le cas d'une carte à puce, peut concerner le microcontrôleur et son microcode, le module, la carte, mais aussi l'application et l'environnement d'exécution, ainsi que la personnalisation de la carte impliquant le site où celle-ci est réalisé. La cible peut se restreindre au microcontrôleur ou au contraire, porter sur un système ou un processus complet. Il existe des profils de protection correspondant à des cibles auxquels il peut être fait appel pour conduire une évaluation. Le projet EPOMI vise à l'établissement d'un tel profil. Ces profils établissent des niveaux d'exigences en matière de sécurité et des moyens de les atteindre. Dans l'évaluation, tous les intervenants doivent se mettre d'accord sur la cible et les exigences de sécurité qu'elle réclame (*security target*). L'évaluation est graduée en différents niveaux d'assurance dont le plus élevé est le niveau EAL7 qui correspond à un système d'information qui a été conçu et vérifié selon des méthodes formelles. Gemalto a été le premier à développer une carte qui a reçu ce niveau d'assurance en octobre 2007. Il s'agit d'une carte Java, conforme au profil de protection de Sun Microsystems, dans laquelle l'étanchéité des applications est prouvée formellement.

les difficultés déjà mentionnées à propos des futures cartes SIM multi-applicatives et émetteur. "*La différence de complexité – un facteur 5 – entre une carte SIM et une carte bancaire est telle que si on voulait adopter les procédures d'évaluation et de certification utilisées à ce jour pour la seconde à la première, on risquerait d'atteindre des coûts et surtout des délais prohibitifs*", souligne Philippe Proust, le responsable de la sécurité et de la certification produits de Gemalto. L'idée est donc d'alléger et de simplifier les procédures là où cela est possible. "*Il ne s'agit pas de réduire les niveaux de vulnérabilité, mais tout en conservant, par exemple, le niveau de robustesse défini (VA4 par exemple, pour l'EAL4), d'alléger la démarche de documentation du produit à certifier auprès des Cesti (Centres d'évaluation de la sécurité des technologies de l'information) agréées Critères communs, en remplaçant la documentation papier par des séances de formation interactives, directement auprès des équipes d'ingénieurs chargés d'explorer tous les chemins d'attaque et d'éprouver la robustesse du produit*, précise Philippe Proust. *On compte, de cette façon, diviser par deux les coûts d'une certification EAL4+ et réduire les délais actuellement de 10 mois en moyenne à 5-6 mois.*"

LE RECOURS À DES AUTORITÉS DE CONFIANCE

Les nouvelles procédures d'évaluation sécuritaire et les modèles de sécurité (contre-mesures, gestion des risques et cadre juridique établissant les rôles et les responsabilités) qui leur seront associés supportent par ailleurs des modèles économiques également nouveaux qui valent comme des systèmes de confiance que les acteurs de ces futurs écosystèmes vont devoir construire et partager. Dans le projet EPOMI, le schéma d'émission d'une application par un opérateur de services prévoit la présence d'une autorité capable de valider l'application en question avant qu'elle soit déployée sur telle ou telle plateforme. Cette autorité de confiance relève du domaine bancaire s'il s'agit d'une application de paiement. Elle vient remplir le rôle dévolu à ce jour en France, par exemple, au Groupement des cartes bancaires CB, en collaboration avec Visa et MasterCard, en matière de certification. La question de savoir si ce modèle dans le cas du paiement doit être étendu à l'ensemble de l'écosystème pour reproduire ainsi le modèle d'émission-acquisition (quatre parties et système d'interchange pour les commissions) en pratique, aujourd'hui, pour les cartes bancaires de crédit et de débit, de la pré-personnalisation ou de la personnalisation finale des cartes et la gestion des applications. Dans ce cas, néanmoins, les banques émettrices auraient à payer à l'opérateur une commission pour l'utilisation du réseau de ce dernier.

En dépit de son caractère familier et plutôt satisfaisant du point de vue de la sécurité, ce modèle pourtant paraît difficile à réaliser pour différentes raisons comme le souligne une étude parue en juillet dernier, réalisée par la Smart Card Alliance [3]. Celle-ci souligne la difficulté des banques à investir dans l'émission de téléphones mobiles embarquant le ou les applications de paiement, et celle de trouver avec les opérateurs – qui dans bien des pays subventionnent la vente des téléphones –, des accords sur la valeur des commissions ou du partage des revenus. L'étude qui met en relief de la même façon que le modèle qui confie à l'opérateur le rôle de prestataires de services de paiement, paraît lui aussi peu viable, indique qu'un modèle collaboratif paraît avoir la faveur de la plupart des acteurs. Ce dernier suppose la création d'un nouveau type d'acteurs (*trusted service provider*) capable de fédérer les intérêts de tous les autres en offrant par ailleurs des garanties en matière de sécurité et de disponibilité des services. La seule difficulté de ce modèle est qu'il reste à inventer. ■

3. TOUTE LA CHAÎNE DE LA SÉCURITÉ

Les 12 partenaires du projet EPOMI

- Deux opérateurs de téléphonie mobile : SFR et Orange/France Telecom
- Trois fabricants de cartes à puce : Gemalto, Oberthur Technologies et Sagem Orga.
- Une SSII, spécialiste des logiciels cartes : Trusted Labs
- Un prestataire de services bancaires : Crédit Mutuel
- Un opérateur de transport en commun : RATP
- Une SSII, conseil en systèmes cartes : Galitt
- La Direction centrale de la sécurité des systèmes informatiques (DCSSI) qui contrôle les Cesti français.
- Un Cesti : Serma, un laboratoire bien connu dans le monde des cartes à puce, certifié Common Criteria.

[1] Juniper Research, dans une étude publiée à la mi-septembre, table sur un parc de 700 millions de téléphones mobiles équipés de puce NFC à l'horizon des cinq prochaines années.
[2] Voir Revue Banque N° 705, l'interview de Philippe Gillet, BNP Paribas : "Le paiement mobile a besoin du même niveau d'assurance de sécurité que le paiement par carte".
[3] "Proximity Mobile Payments Business Scenarios : Research Report on Stakeholder Perspectives", http://www.smartcardalliance.org