

INTERVIEW

“L’infrastructure de paiement restera majoritairement off-line”

Selon Yves Randoux, l’architecture IP présente des risques différents du mode actuel ; il faut poursuivre les études et les finaliser pour trouver un bon équilibre entre sécurité et coûts. Cependant, les infrastructures de paiement devront rester off-line.

■ **La monétique IP (Internet protocol) est un nouveau chantier pour le Groupement. Comment a-t-il été lancé ?**

Le chantier de la monétique IP a été lancé au sein du Groupement des Cartes Bancaires “CB” en 2003, au cours des travaux réguliers des comités banques/commerce, créés dans le cadre de l’accord signé en 2001 entre les représentants des banques et du commerce, dans le but d’un meilleur dialogue entre ces acteurs du paiement par carte bancaire. Dans les réflexions sur les évolutions de l’architecture de paiement, les travaux sur l’IP sont particulièrement structurants pour l’avenir. L’aspect le plus délicat reste l’adaptation des structures existantes.

Les enjeux pour les banques et le commerce sont, bien sûr, la prise en compte de l’évolution du monde des télécommunications et les bénéfices à en tirer en termes de qualité et de coûts. Mais l’enjeu majeur reste évidemment l’amélioration constante de la sécurité du système. Il n’est pas envisageable de procéder à des améliorations sans augmenter la sécurité.

■ **Ces travaux peuvent-ils être considérés comme une étape ou une première mise en phase avec les efforts d’harmonisation**



Yves Randoux

Administrateur
Groupement
des Cartes Bancaires
“CB”

de l’espace de paiement européen ?

L’IP présente la particularité d’être ouvert et mondialisé. Ceci est bien entendu un atout dans le cadre d’un espace de paiement européen puisqu’il n’y a plus de notion d’ajustement du coût à la distance.

■ **Peut-on considérer l’avènement de la monétique IP comme un retour du modèle on-line dans le paiement ?**

Le business-model du système de paiement/retrait par carte bancaire CB date des années quatre-vingt-dix et tenait compte des coûts importants des télécoms. Cet élément a déjà beaucoup évolué et connaît une baisse encore plus drastique avec l’IP. Mais recourir au tout on-line aurait un impact majeur sur la taille et la puissance des serveurs bancaires. Aujourd’hui, les pays européens, dans un contexte largement on-line, migrent à la puce. En passant de la piste à la puce, ils mènent une réflexion inverse à celle des banques CB, et souhaitent faire baisser leurs taux de transactions on-line.

Pour le système CB, il n’y aura pas de migration vers un modèle on-line, mais plutôt un équilibre à trouver en utilisant au mieux les facilités qu’offre IP sans induire de coûts supplémentaires sur les suiveurs. Globalement, l’infrastructure restera majoritairement off-line.

■ **La sécurité dans le monde de la monétique IP est-elle un challenge difficile à relever ?**

Dans le système CB, la sécurité est toujours le challenge permanent, et ceci d’un bout à l’autre de la chaîne du paiement et retrait par carte bancaire. Il est donc important que l’univers IP soit capable de répondre aux exigences sécuritaires. Les pilotes mis en place, avec les partenaires du commerce, et particulièrement avec l’aide de Mercatel, montrent bien les efforts qui restent à faire, d’une part avec le grand commerce et d’autre part avec les commerçants équipés de terminaux autonomes.

L’architecture IP présente des risques différents du mode actuel ; il faut poursuivre les études et les finaliser pour trouver un bon équilibre entre sécurité et coûts.

Le Groupement CB revoit aujourd’hui ses exigences sécuritaires pour tenir compte des expériences menées depuis un an sur le terrain, grâce aux échanges avec les représentants du commerce, les opérateurs Télécom, les industriels et professionnels de la monétique.

■ **Quels changements finalement pour les banques ?**

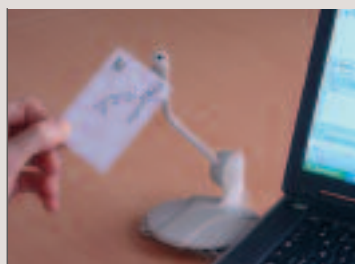
La monétique IP constitue une opportunité également pour les banques. Ces dernières ont déjà investi dans ce protocole pour le nouveau réseau d’autorisation e-rsb exploité en IP. Les banques ont déjà engagé des réflexions sur le meilleur usage de cette technologie de télécommunication pour apporter une valeur ajoutée aux services rendus par leurs clients professionnels, les entreprises et le commerce. ■

Une solution d'authentification audio embarquée dans une carte à puce ISO

■ Les offres d'authentification forte pour sécuriser les accès à des services de banque à distance se multiplient.

Prosodie, un opérateur de services spécialisé dans la gestion des flux de données pour les grands comptes, vient ainsi de commercialiser une solution d'authentification audio qui pour la première fois peut être embarquée dans une carte à puce embossable au format ISO, une carte EMV, par exemple. Jusqu'ici les solutions de ce type, parce qu'elles réclament d'embarquer une pile, un buzzer, et un bouton pous-

soir pour activer la séquence sonore, étaient portées dans des jetons, tokens, ou des cartes à puce dont l'épaisseur interdisait de les utiliser comme de classiques cartes bancaires. "La durée de vie de la carte est de deux ans grâce à l'utilisation d'une pile lithium très fine, ce qui coïncide avec le cycle de vie des cartes bancaires. Du coup, la solution qui permet de combiner les fonctions classiques de la carte bancaire et l'authentification forte pour accéder à des services en ligne, offre des gains de coûts en distribution notamment" souligne l'un des responsables de la société. L'au-



■ **Prosodie** propose une solution d'authentification audio qui pour la première fois peut être embarquée dans une carte à puce embossable au format ISO.

thentification est basée sur un cryptoprocèsseur embarqué dans la carte qui génère une sé-

quence sonore codée, chiffrée (AES) et signée (SHA-1) utilisant une modulation de type FSK (Frequency Shift Keying), compatible avec les micros des téléphones et des cartes son des PC. À chaque pression du bouton poussoir, la carte émet une signature acoustique aléatoire, unique (One Time Password) et non rejouable, qui initie un processus d'authentification qui se poursuit par la frappe de codes sur le clavier du PC ou du téléphone utilisé. Prosodie livre avec cette solution le logiciel serveur correspondant.

Un progiciel dédié à l'accompagnement d'un projet ITIL



■ En offrant un modèle de gestion de la production de services informatiques enrichi par de très nombreuses expériences, l'**ITIL (IT Infrastructure Library)** est de plus en plus utilisé. Pour accompagner cette évolution, la société Nomia,

déjà éditeur d'un progiciel (**OnMap**) dédié à l'accompagnement du changement, axé sur la formation, la communication et l'assistance opérationnelle, vient de s'associer à un autre cabinet de conseil, **CG2 Conseil**, pour commercialiser un pro-

■ la société **Nomia** vient de s'associer à un autre cabinet de conseil, **CG2 Conseil**, pour commercialiser un progiciel dédié à l'accompagnement des projets **ITIL**.

giciel dédié à l'accompagnement des projets **ITIL**. Basé sur OnMap (accompagnement du changement), ce progiciel a pour objectif de faciliter et accélérer le déroulement du projet en proposant des outils d'appropriation des meilleures pratiques, et d'aide à la construction du référentiel ITIL. Il couvre ce référentiel sur la gestion et

le support des services. L'offre qui sera commercialisée courant mai se divise en deux. Une offre "découverte" qui propose notamment des cartographies interactives et des animations. Une offre "boîte à outil" (**Toolkit**) qui comporte l'ensemble du référentiel et la suite d'outils permettant sa personnalisation en fonction du projet de l'entreprise et de l'organisation cible. Il offre en particulier à chaque opérationnel, un bureau "métier" qui lui donne accès à l'ensemble de son environnement de travail en visualisant ses procédures, ses modes opératoires et ses activités dans les processus.

Une plate-forme d'échanges de type EAI pour la zone euro

■ L'harmonisation des instruments de paiements ainsi que l'évolution des systèmes d'échanges et de règlement de la zone euro (TARGET2, et PE-ACH) poussent à une intégration de plus en plus forte du système financier européen. C'est dans cette perspective que la société nantaise **CIBF**, spécialisée notamment dans la gestion de flux et les échanges interbancaires, a développé une plate-forme de

raccordement aux différents systèmes d'échanges et de règlement de la zone euro sur la base d'une infrastructure de type EAI (Enterprise Application Integration). "Ces évolutions vont avoir un impact sur les systèmes d'informations, et elles vont commander des choix de stratégie (plate-forme partageable ou raccordement direct) et de calendrier pour s'adapter. Nous avons donc saisi l'occasion pour bâtir une solution basée sur des infrastructures

EAI, très bien adaptées à un contexte fortement évolutif" souligne l'un des responsables de la société. La plate-forme est construite autour d'un bus applicatif auquel peuvent être raccordées (via des connecteurs) les applications existantes ou nouvelles de la banque. Ce bus orchestre par ailleurs les processus d'échanges par la "greffe" des métiers (fonctions bancaires) sous la forme de services développés en Java. Une

architecture qui offre ainsi la souplesse et la flexibilité souhaitables pour permettre des migrations contrôlées et progressives. L'application d'échanges d'effets de commerce, de chèques et de virements CI-ARC+ de CIBF, peut par exemple, se raccorder telle quelle au bus applicatif ou bien être implémentée directement sous forme de services de paiements pour répondre aux besoins de production bancaire.

Dépôt automatique de documents : encore plus de fonctions

■ La cinquième génération du module (IDM pour Intelligent Depository Module) de sys-



tèmes de dépôt automatique développée et commercialisée tout dernièrement par **Diebold** offre un espace de stockage des documents deux fois plus élevé (jusqu'à 1 000 chèques) que la génération précédente. S'ajoutent à cela la prise en compte des chèques au format européen grâce à une tête de lecture adaptée, la détection de l'insertion

de documents multiples, et un système de vérification de la qualité des images chèques basé sur l'utilisation du logiciel Image Inspector de Carreker Corp. Cette dernière application améliore la qualité de l'archivage des chèques et réduit les risques de fraude. Le IDM accepte les chèques individuels qui peuvent être déposés en vrac. Au cours de la transaction, les deux côtés du chèque sont numérisés, le montant est lu, et la présence de la ligne MICR (Magnetic Ink Character Recognition) reconnue puis lue.

Une plate-forme de services téléphoniques VoIP pour les salles de marchés

■ Nouveau venu sur le marché français, **IPC Information Systems**, fournisseur de systèmes et services de télécommunications à la communauté financière (Barclays, Bank of America, Deutsche Bank), propose désormais une offre de vente, intégration et support de systèmes téléphoniques sur IP (VoIP) à destination des salles de marchés. Ces équipements, basés sur le réseau privé sécurisé de IPC, sont conçus pour répondre aux besoins des applications réclamant des données "interreliées" (voix-données), et d'une manière générale aux exigences de disponibilité et de qualité de service des réseaux de salles de marchés. Ces systèmes ont une capacité de prise en charge de 4 000 utilisateurs et de 16 000 lignes par commutateur. Ils permettent deux appels par seconde et par utilisateur, soit 7 200 tentatives d'appels à l'heure "chargée" par utilisateur.

Première carte EMV DDA à montant pré-authorized

■ La commercialisation depuis fin mars de la carte à puce **Macellia** de **Sagem** marque l'apparition des premières cartes **EMV DDA** (Dynamic Data Authentication) dont la généralisation est prévue en France au cours des prochaines années. Cette carte embarque en outre

l'application OneSmart Mastercard Pre-Authorized qui permet au porteur d'utiliser en mode off-line sa carte de paiement jusqu'au moment où il atteint le montant qu'il a déposé sur son compte "pré-authorized". Il peut alors réapprovisionner son compte. La car-

te Macellia qui utilise un microcontrôleur Risc d'Atmel capable de calculs RSA, est certifiée CAST (Compliance Assessment Security Testing), et a fait l'objet d'une évaluation Critères Communs de niveau EAL4+, le plus haut niveau actuel en matière de sécurité.