Tiers de confiance : le rôle des banques

Etre tiers de confiance recouvre des attributions variées et plus ou moins étendues. Si les banques ont un capital confiance naturel vis-à-vis de leurs clients, les adéquations du métier bancaire ne sont pas les mêmes avec toutes les formes de tiers de confiance.

PATRICK COILLAND
Expert en sécurité
Groupe Telindus

Le terme «tiers de confiance», réservé initialement aux spécialistes de la sécurité pour désigner les dépositaires de clés secrètes ou privées dans le cadre du respect de la législation cryptographique, est en train de prendre, dans le monde du e-business, de nouveaux sens fondés sur les différents besoins de confiance nécessaires à l'essor des transactions électroniques.

DEUX TYPES D'INTERMÉDIAIRES DANS LE B TO B

En *B-to-B* (*business to business*) entre entreprises se connaissant déjà et recherchant une simple optimisation de leurs processus, les besoins sont au niveau du chiffrement et de l'authentification. Deux types d'intermédiaires sont susceptibles d'intervenir : les dépositaires de clés détiennent les clés de chiffrement pour satisfaire les exigences légales en la matière ; les autorités de certification se chargent de garantir aux parties l'identité de leur correspondant. Les mécanismes techniques sous-jacents relèvent du PKI et de la signature électronique.

LE BESOIN DE CONFIANCE EST PLUS IMPORTANT EN B TO C

En *B-to-C* (*business to consumer*) ou *B-to-B* dans lequel les deux parties ne se connaissent pas avant la transaction, le besoin de confiance est beaucoup plus important et couvre de nombreuses facettes. L'intervention de tiers dans la satisfaction de ces besoins se résume en trois catégories :

- les autorités de certification sémantique poussent la certification au-delà d'une simple garantie d'identité. Le certificat délivré garantit aux yeux du tiers des éléments supplémentaires (existence d'un processus de livraison, rigueur financière, etc). Exemples : programme Verisign Webtrust, offre Chambersign des CCI…
- l'opérateur de paiement global intervient dans le processus de paiement à la place du commerçant qui est déchargé de l'obligation de gérer les différents modes de paiement. Le client, quant à lui, sait que ses informations de paiement ne transitent pas (ni ne résident) chez le commerçant, mais chez un professionnel des transactions de paiement, ce qui améliore la confiance qu'il a dans le processus. Les deux parties y trouvent donc de l'intérêt. Exemples : de nombreuses banques, ATOS…
- l'authentificateur de paiement : ce rôle naissant résulte de l'évolution de la position des banques face au paiement électronique. La gestion du paiement par le commerçant n'est clairement pas souhaitable. La gestion

par un opérateur de paiement global est plus saine, mais il est difficile pour un tel opérateur d'être suffisamment proche de chacune des parties pour emporter leur confiance. Les procédés sans tiers (Set, Cybercomm) souffrent du besoin d'équiper les clients, ce qui sera particulièrement complexe pour les clients légers (PDA, successeurs WAP, etc.). En conséquence, Visa a publié en 2000 un modèle de paiement (3DM : *three domain model*) dans lequel chacune des deux parties (client et commerçant) possède un tiers proche de lui chargé des opérations d'authentification pour le paiement. Des adaptations de SET (3D-SET), mais aussi d'autres technologies (*3D-Secure*) ont été développées pour s'adapter à ce modèle.

Une offre particuliere de tiers de confiance en C to C

Enfin, dans le monde du *C-to-C* (*Consumer to Consumer* : troc électronique, enchères), le concept de «paiement avant la livraison» n'est plus vraiment acceptable, et une offre particulière de tiers de confiance s'est développée : l'intermédiaire de paiement encaisse le paiement (et éventuellement une caution équivalente du vendeur) et attend que les deux parties aient notifié leur accord sur la livraison acceptée pour clore l'aspect financier de la transaction. Exemples : Probatio, Securachat…

Les banques ont une position privilégiée

Dans ce contexte, il est clair que les banques ont une position privilégiée. Elles ont en effet un capital confiance naturel vis-à-vis des clients pour tout ce qui concerne les processus de paiement. Pour autant, les forces et les adéquations du métier bancaire ne sont pas les mêmes avec les différentes formes de tiers de confiance (*encadré*).

Le rôle de dépositaire a été singulièrement entamé lors de l'abandon du dépôt préalable de clés et le marché se cherche encore dans ce domaine ; la législation actuelle permettant le maintien des clés chez le client, il est probable qu'on s'orientera vers un marché de logiciels intégrés plus que de services externalisés.

Le rôle d'autorité de certification reste assez loin des caractéristiques du métier bancaire mais l'ajout d'une sémantique à la certification peut présenter un fort intérêt. On s'approche là des fonctions connues de *rating*. Ce créneau est également convoité par d'autres métiers (les grands cabinets de conseil, par exemple) ; l'enjeu ici serait de disposer l'un label reconnu.

Le rôle d'intermédiaire de paiement, tant qu'il est cantonné au *C-to-C* avec sommes modestes, présente un rapport risque/gains un peu élevé pour les banques établies et intéresse plutôt le créneau des start-up.

Il reste les rôles d'opérateur et d'authentificateur de paiement. Le premier s'accommode assez mal d'une fragmentation du marché, alors que le second s'y prêterait naturellement. Le premier relève donc d'une stratégie offensive, alors que le second s'insère plutôt dans une stratégie défensive consensuelle. On comprendra alors aisément l'engouement actuel du monde bancaire pour le modèle 3DM et le déploiement de fonctions d'authentificateur de paiement.

Le développement des technologies de paiement sans tiers

Quant à l'avenir, l'évolution des technologies devrait toujours laisser une place sérieuse aux autorités de certification «sémantiques». En revanche, la balance opérateur/authentificateur de paiement dépendra de la capacité de déploiement des technologies de paiement sans tiers (type SET/Cybercomm) : si celles-ci réussissent à se déployer, le rôle d'authentificateur de paiement n'émergera pas et celui d'opérateur perdra son aspect «confiance» pour s'orienter vers une fonction d'opérateur «industriel». Si, au contraire, ces technologies échouent au profit de clients allégés à l'extrême, c'est le rôle (défensif) d'authentificateur de paiement qui s'établira. Le monde bancaire est aujourd'hui positionné des deux côtés de l'alternative. A lui de se déterminer.

Les banques et les fonctions de tiers de confiance

	Capital confiance	Proximité du métier	Synergie avec les métiers traditionnels	Commentaires
Dépositaire	***	*	-	Position à reconsidérer avec l'évolution de la législation (passage au tiers de confiance ?)
Autorité de certification	*	*	-	Marché occupé
Autorité de certification sémantique	**	**	**	Synergie avec les assurances, ainsi qu'avec l'audit
Opérateur de paiement global	***	***	**	Naturel
Authentificateur de paiement	***	***	***	Evidemment le plus proche, mais nécessite une adhésion mondiale à 3DM
Intermédiaire de paiement	***	**	**	Risques juridiques, problème de seuil de rentabilité