Résumé de « The concept of security and trust in electronic payments »

1. The need for security in electronic environment

Les transactions dans le commerce électronique peuvent se produire sans un contact humain auparavant ou sans établir une relation interpersonnelle. Auparavant, les longues relations dépendaient toujours de la confiance. Les entreprises sont forcées de développer l'intimité du client mais également d'assurer que les besoins de sécurité font partie la stratégie de la relation avec le client. Les trois briques du mécanisme de sécurité utilisé sont :

- l'encryptage : fournit la confidentialité, l'authentification et l'intégrité
- les signatures digitales : fournissent l'authentification, l'intégrité et la non-répudation
- les algorithmes de hash : fournissent l'intégration et peuvent authentifier

Une transaction de commerce électronique peut être catégorisée en un processus en trois étapes :

- chercher et négocier
- le chemin de la confiance
- engagement et suivi

La première étape peut identifier tous les besoins de sécurité qui peuvent être appliqués à l'environnement que nous avons besoin pour établir le concept de confiance et de sécurité. Les besoins sont l'identification, l'authentification, le contrôle d'accès, la confidentialité, l'intégrité, la non-répudation, la disponibilité. La sécurité dans le cadre du payement électronique est catégorisée en trois domaines:

- la sécurité du système (infrastructure technique et implémentation)
- la sécurité de la transaction (un payement sécurisé en accord avec des règles spécifiques et bien définies)
- la sécurité légale

2. Identification of trust

La phase du payement électronique est confidentielle si toutes les phases du processus sont capables de satisfaire les besoins des participants et leurs attentes sécuritaires. Tous les participants doivent avoir une confiance absolue dans le système. La confiance et le risque doivent être considérés comme des déterminants importants pour adopter un comportement. La confiance exige de prendre une décision rationnelle basée sur la connaissance de possibles récompenses de confiance ou de non confiance. Un environnement de confiance est caractérisé par :

- le fait que chaque entité est identifiable uniquement
- qu'il y a un nombre minimum d'entité de confiance à priori
- que ces entités ont une confiance incontestable en les autres entités participantes

3. Electronic payment (e-payment) phase

Le système de payement électronique fait deux choses à savoir : imiter les framework existants dans le mode réel et schématiser de nouveaux chemins pour exécuter les payements

des transactions. Le paiement électronique compte trois participants : le client, le marchand et la banque. La première caractéristique distincte du système de paiement est le « money model » :

- Token (quand le moyen d'échange représente de la valeur)
- Notational (que une valeur est stockée et changée avec une autorisation)

Il y a trois modèles de protocole de paiement à savoir : cash, chèque et carte.

Une autre caractéristique distinctive est le temps auquel la valeur monétaire est prise du payeur :

- les systèmes à prépaiement (le compte du client est débité avant le paiement)
- les systèmes « pay-now » (le compte du client est débité au moment du paiement)
- les systèmes « post-pay » (le compte du marchand est crédité avant que le compte du client soit débité)

4. Security evaluation approach: properties and requirements

Les besoins sont l'intégrité, l'authentification, la prévention de la fraude et la tolérance, et l'intimité.

Les propriétés sont la divisibilité (la possibilité de multiples coupures), la transmissibilité, la prévention de la double dépense (prévention de la copie de monnaie pour être dépensés plusieurs fois), la confidentialité du paiement, l'anonymat du paiement et l'intracablilité du payeur. Aucun système de paiement électronique ne possède toutes ces propriétés.

5. Cryptography and PKI

Une question logique est quel mécanisme peut établir et implémenter efficacement la sécurité et la confiance sur Internet. La cryptographie représente le seulement moyen avec lequel le business peut travailler comment les mécanismes basés sur le papier. Il y a deux formes de cryptographie, la symétrique et l'asymétrique. La transmission d'information digital entre les parties doit être sûre que des garanties sont offertes pour :

- l'identité des parties
- les informations transmises ne sont pas modifiées
- la confidentialité de l'information transmise
- la protection contre le déni de la transaction (non-répudation)

6. Conclusion

La création d'un nouveau système de paiement ou d'une infrastructure de confiance pour des transactions sécurisé nécessite un investissement signifiant. Pour qu'un système de clés publiques fonctionne correctement dans le domaine public, la clé publique doit être accessible et les expéditeurs et les destinataires doivent avoir une manière d'être sûr que les clés publiques sont bien les clés publiques de ceux avec qui ils veulent avoir un contact. Il y a deux solutions : le web de confiance (basé sur une relation préexistante) et les autorités de certification.