Security for Electronic Commerce

Marc Pasquet
GREYC Laboratory (ENSICAEN – Université Caen Basse Normandie - CNRS), France

Christophe Rosenberger
GREYC Laboratory (ENSICAEN – Université Caen Basse Normandie - CNRS), France

Félix Cuozzo
ENSICAEN, France

INTRODUCTION

E-commerce permits a dematerialized financial transaction between a customer and a merchant (Schafer, Konstan, & Riedl, 2001). It uses a complex architecture involving many aspects in computer science (security, database management) and in electronics (smartcards, tokens) (Tang, Waichee, & Veijalai, 2004). E-commerce is in a constant growth (Herrmann & Herrmann, 2004). To be used by the majority of individuals, electronic transactions must be secured to increase the confidence in the e-commerce. Security is necessary in commercial relationships for many reasons. First, the customer must be sure that the goods he/she is buying will be the expected ones, and will be well delivered at his/her address. Second, the merchant must be sure to be paid. If the customer uses banknotes or electronic payment, two or more partners are involved in that transaction: the customer's bank and the merchant's one. The two banks must be sure of the customer's identity and of the merchant's one in order to avoid banking frauds.

In the transaction process, many security systems are used to ensure the confidentiality, authentication, and integrity of exchanges. The security is guaranteed by using specific procedures and hardware. The objective of this chapter is to present how the classical security concepts are applied for an electronic payment and especially to limit the fraud.

The background section first gives a general idea of the problem generated by the electronic commerce. Second, we present briefly the public key infrastructure approach that is generally used for authentication within this context. The main thrust introduces two protocols that have been developed: SSL (secure sockets layer) and TLS (transport layer security), to create a secure channel where all transactions are encrypted by using specific architectures and algorithms. For the payment part of the transaction process, banks have been considered that SSL and TLS are not sufficiently secure. The main reason is that the cardholder is not authenticated by the issuer bank and the responsibility stays on the merchant side. Banks have so tried to implement different architectures to meet these requirements. These different methods, use of token with SET (secure electronic transaction) or a smartcard such as C-SET developed in the last fifteen years, began to converge to the 3D-secure (three domains security) protocol. These methods to secure the distant payment was adopted together by the card scheme Visa© and MasterCard©. The last, but not the least problem, concerns the distant authentication of the client by its bank, which is described in the future trends.

BACKGROUND

We first make a brief description of the e-commerce issues.

E-Commerce Description

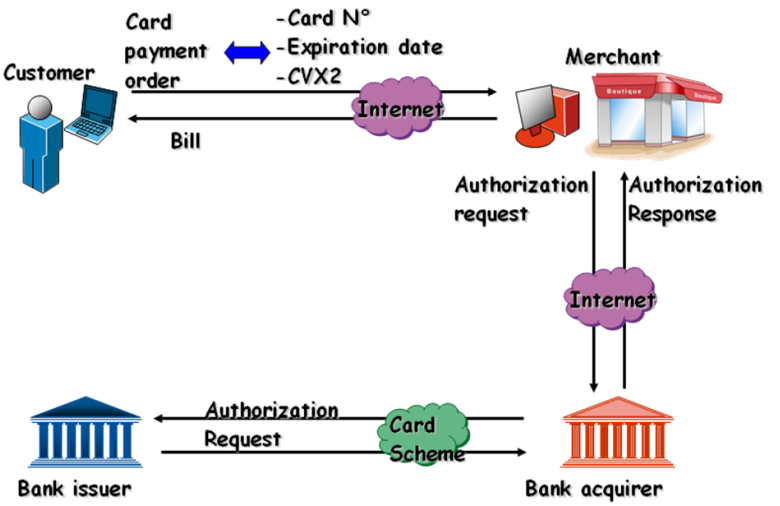
In order to better understand how the e-commerce works, Figure 1 shows the different partners and the different exchanges between them. A financial transaction between a customer and a merchant is, in fact, a transaction between the issuer and the acquirer banks. The payment is achieved through many authorization requests (customer authentication, bank transfer authorization) involving many security and cryptographic concepts.

In order to help the e-commerce development, some good practices are necessary to be applied:

- *The risk control*. The risk is partly taken by:
  - The merchant to not finally be paid;
  - The consumer to not receive the goods or the services;
  - The consumer bank in case of a systemic attack.

This risk, assumed by these different partners, must be as low as possible. The risk is as much loss of confidence in the system, as waste of money.

Figure 1. The different partners and flux in e-commerce payment



- *The facility of use for the consumer.* The reference model is the face-to-face commerce, and an ideal solution for the e-commerce must not create more constraints;
- *The use of international standards*. In one hand, Internet protocol is the base for e-commerce and in the other hand, the banking payment systems with chip or/and stripe cards, should also be used for e-payments;
- *The deployment of the different measures with a communication between banks and merchants.* The constraints and the added value must be studied with a great attention. If one of the four partners of the transaction (the customer and his/her bank and the merchant and his/her bank) is not interested in one architecture implementation, the system will have much more difficulties to be developed.

As conclusion, it is necessary to:

- Well balance the responsibilities between the four partners;
- Adapt the security level to the risk level;
- Integrate the legal constraints.

The Security Problematic

Additionally, in order to help the electronic commerce development, banks have to implement different solutions (Furnell & Karweni, 2000):

- *Visual cryptogram:* To improve the identification process, the EMV (Eurocard MasterCard Visa) cards include, on the back, a three figure code called CVX2, that the consumer must give to complete a payment transaction;
- *Authorization:* More than 7% of authorizations come from the e-commerce, and that part increases every year;
- *Individual supervision of frauds*: Coming from consumers or merchants;
- *PKI (public key infrastructure) for data protection*: To create the better possible protection for the different exchanges between all the transaction partners;
- *Authentication services*: To avoid the risk at the consumer level (CAP (chip authentication program ©MasterCard), SET, 3D-secure).

The Public Key Infrastructure

A public key infrastructure (PKI) includes a set of physical components (computers, cryptographic algorithms and equipments, smartcards), human procedures (verifications, validations), and software (systems and applications) to manage the life cycle of electronic keys or certificate. A certificate can be considered as proof of the existing relation between the identity of a customer or merchant and a public key. The major element is the certifying authority (CA) that signs the certificate, the registration authority (RA) that creates the pairs of keys, and the repository that stores the certificates.

Figure 2 shows the different transactions in a PKI infrastructure (Chanson & Cheung, 2002). There exist many certifying authorities (EuroPKI, E-certify Corporation, ID.Safe, Identrus, E-Commerce PKI CA, SwisSsign…).

A public key infrastructure delivers a set of services for its users (Critchlow & Zhang, 2004). The main services are: