Electronic Payment

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

Sylvain Vernois
GREYC Laboratory (ENSICAEN – Université Caen Basse Normandie - CNRS), France

Wilfried Aubry
GREYC Laboratory (ENSICAEN – Université Caen Basse Normandie - CNRS), France

Félix Cuozzo
ENSICAEN, France

INTRODUCTION

Money has two main forms nowadays: the fiduciary money (coins, banknotes…) and the scriptural one (electronic or virtual). To pay goods, both are used. The electronic money, one specific form of the scripting money, is more and more used everywhere in the world. Electronic payment has many particularities: specific infrastructure, equipment, and software, new forms of regulations, technical agreements, normalizations, fraud limitations…

The objective of this chapter is to present a general overview of electronic payment. The background section presents its historical evolution. In the main thrust, the chapter focuses first on the general architecture of electronic payment. Second, different authorization mechanisms for the processing of the banking transaction and for fraud prevention are detailed. Future trends stress the different research topics that should be investigated, especially concerning the SEPA program (Single Euro Payments Area), which will harmonize bank payment systems in Europe through 2012.

Figure 1. Exchange of goods

BACKGROUND

Exchanging goods is the basis of commerce. From the origin with barter (Menger, 1892) to the introduction of a valuable commodity to give the goods a value, men managed to build a trustful organization, creating the money, and later the banks and laws, to protect this new financial structure.

Paper money has been developed since the 17th century as an object without any real value but with a financial value given by trust in the emitter: the bank (see Figure 3).

Nowadays, money is often dematerialized in the payment process (Schafer, Konstan, J.A., Riedl, 2001). This can particularly happen (see Figure 4):

- when the purchase is done: an electronic payment occurs between the customer and the merchant ;
- when banks want to clear the positions they have between each other.

E-payment allows exchanging scriptural money electronically, by the use of an "identifier" that can be associated not

Figure 2. Transaction using social money

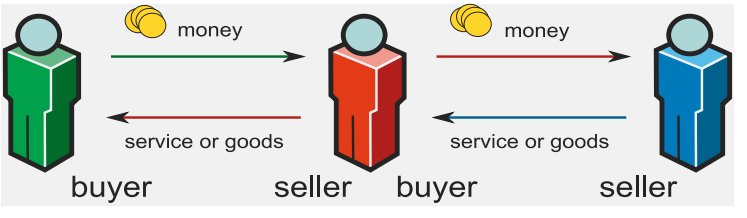


Figure 3. Transaction using paper money

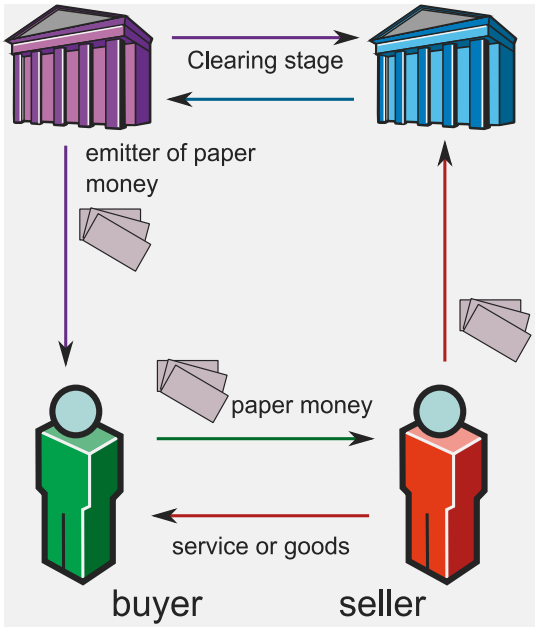
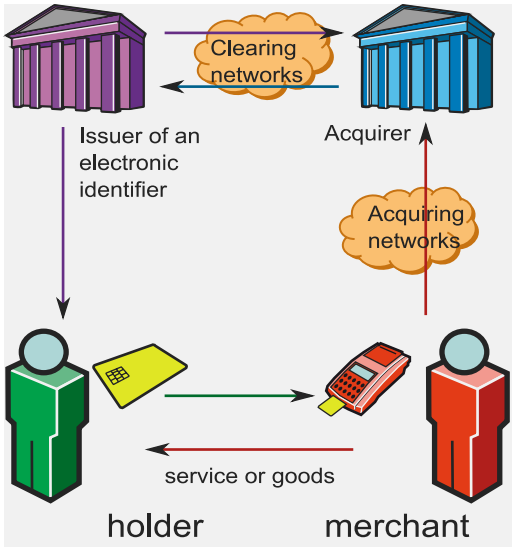


Figure 4. Transaction by electronic payment



only with a bank user or a fidelity account, but also with an electronic purse (off-line or online) or an anonymous account.

The most common media is a plastic card that includes different technologies (magnetic stripe, microprocessor chip, contactless…) allowing different services and security levels. Other objects and technologies can be used, such as customer's fingerprint, thanks to biometrics.

E-payment can be divided into two families:

- Face-to-face payment, where the customer and the merchant are physically in the same place ;
- Distant payment, where the two participants do not meet each other (mail orders, phone orders, and now electronic commerce via Internet) (see Figure 5).

With the development of recent communication technologies, new payment channels have been developed. Multimodality has become a bet for all participants in the payment process, from banks, merchants, to communication network operators.

Gradually, payment cards are allowing more services than their initial function. Open card development platforms (GlobalPlatform, 2006) of specific card specification, such as EMV (**Europay MasterCard and Visa**), are vectors of development of multiapplications cards. That brings new difficulties to solve, like the need of imperviousness between the applications embedded in a smartcard.

Historically, technical and functional payments architectures have mostly been driven by needs and industries. Some are "open" to allow different implementations to be interoperable:

- ISO/IEC norms, such as 8583 (ISO 8583) for message format or 7816 for smartcards (ISO/IEC 7816) ;
- Open specification, such as EMV specification (EMVco, 2006) that proposed an international specification for payment and multiapplication cards.

Others are kept private, to be used only by a restricted number of participants, such as:

- Communication protocols between servers and terminals ;
- French smartcards specification (B4/B0') ;

However, results coming from research have allowed many evolutions. For example, electronic payment is possible thanks to cryptographic advances: the security aspects of payment are very important to accept the way the transaction is concluded. From the elementary algorithm of Lühn allowing checking the validity of card number to DES, RSA (Rivest, Shamir, & Adleman, 1978), or elliptic curves security algorithms, all aspects are interesting in the payment domain.

MAIN FOCUS OF THE CHAPTER

This section presents the state of the art on the way we can create and settle a transaction nowadays. The first part sets out the necessary exchanges for a full electronic transaction between the actors of the transaction. The second section