The implementation of E-signatures in payment systems: open issues and possible solutions

Paola Masi
Payment System Oversight Office
Banca d'Italia

ECB Conference on e-payments
Frankfurt 19 November 2002

Introduction

- E-signature represents a key element of security management in open networks like Internet. It can grant legal validity to an electronic authentication attached to or logically associated with electronic payment transactions
- According to the *ECB Issues Paper on e-payments*, "the conditions applying to electronic signatures could strengthen confidence in and general acceptance of the new technologies" (par. 3.2.2)
- Hence, e-signature is essential to provide e-payment services with the same level of certainty and security as face-to-face transactions and traditional electronic payments on "closed networks"

- Despite the robust legal framework governing e-signature in Europe (the Directive 1999/93/EC), the full development and adoption of electronically-signed financial transactions on open networks are still lacking

Legal framework

- Being technologically neutral, the e-signature Directive defines qualified electronic signatures in a functional but not in a technical way
- Every kind of electronic authentication attached to or logically associated with the data to be signed gets legal validity: such a general authentication method is an "electronic signature". An "advanced electronic signature" is an electronic signature that meets some specific requirements set by the Directive
- Member States are allowed to have voluntary accreditation schemes for the purposes of different levels of security in certification services and are obliged to establish a supervisory system to control certification service providers

E-signature for the security of e-payments

- Compared to traditional payment systems, the use of the open network has allowed more convenient financial services but has also made the nature of risks more complex (e.g. unauthorised access, illegal acquisition of PINs, theft of data, etc.)
- There is an increasing demand for security services by banking customers, above all by firms, confirmed by the vast economic literature and surveys on e-commerce and e-business
- Financial institutions are requested to supply on-line payments on open networks with the same security levels as traditional payment instruments (including e-signature, time-stamping, receipts, warranty systems, attribute of the sender, etc.)

E-signature for the security of e-payments

To win the challenge of the new technological environment, e-signature must be regarded as an enabling platform, or an essential device, to offer a complete set of trust services. These might be grouped in three levels:

a *basic services* related to validation of identity and issuance of certificates

b *complementary services* to e-signature, typically developed by the banking community, such as electronic documents management systems, attribute management, "Quality of Service" (QoS) dynamic warranty systems, secure/certified mail

c *value added services*, tailored to individual customers, like "escrow services" in business-to-business environment

Open issues

With a view to creating secure European e-payment services, the adoption of e-signatures requires the solution of the following open issues:

• ***supervision of certification-service providers***

Some European countries have already established a centralised supervision scheme; others preferred a decentralised one; others are envisaging mixed solution. The possible drawbacks of not-harmonised national schemes should be carefully analysed

• ***security certification***

A number of countries subscribed an agreement on the recognition of Common Criteria Certificates (May 2000). This is a valuable result but is effectively applicable only if the main processes – evaluation, certification and accreditation - are defined in a clear and harmonised way

Open issues

• ***interoperability of certificates***

Interoperability has been tackled at national level by public bodies and authorities; in some cases single business initiatives have been undertaken (e.g. the case of *Identrus*). Some form of incentive might be studied to foster the use of a common structure for qualified certificates and for certificate revocation lists (CRLs) and the adoption of common standards produced by the European Telecommunications Standards Institute

• ***business requirements***

The lagging process of defining the business requirements might be due to network externalities. Single market operators are not big enough to internalise the costs needed to develop a widespread, cheap, secure and reliable e-signature. The achievement of critical mass is linked to a variety of factors (from the quality of telco infrastructure to long-term consumer's risk aversion)

Solving the open issues

According to the *ECB Issues Paper on e-payments*:

> central banks can play a catalyst role in the adoption of e-signature in the banking sector, trying to remove obstacles, to identify constraints, to devise policies that should help to overcome "the co-ordination failures" within the financial and banking communities and with the other economic agents involved in monetary transactions

Suggestions from the Italian case

The interoperability issue

- The Italian overseer strongly supported the adoption of "Interoperability Guidelines" among Italian Certification Service Providers
- The guidelines were developed by a working group constituted under the chairmanship of the Authority for Information technology in the Public Administration (AIPA)
- The basic level functions defined in the "interoperability guidelines" are open and compatible with most software packages available today
- Although the guidelines are not mandatory for Italian Certification Service Providers, the Public Administration accepts only certificates compliant with these technical rules

Suggestions from the Italian case

Business requirements

- The Italian overseer is actively promoting the development of procedures and protocols for on-line public payments based on e-signature: expanding public demand will serve as a catalyst for the diffusion of digital signature for private companies
- A recent project, devised by the Ministry of Economy, the Banca d'Italia, the AIPA and the banking system, is aimed at:
  - building a new information system on cash flows and economic data from the Public Administration
  - connecting central and local government entities (e.g. regions, provinces, universities, the local health service, schools, etc.) to Treasurer Banks using electronically signed documents. This is expected to be the "killer application" of e-signatures

Conclusions

- The delay in adopting e-signature in banking applications and procedures for e-payment services is due neither to lack of technical solutions nor to the legal aspects of mutual recognition.

- The slowdown factors seem to be related to the following difficulties: i) defining an institutional and organisational framework to manage "fully-dematerialised" payments and ii) solving network externality problems preventing market operators from integrating e-signature into business applications.

- Obstacles may be overcome through the dialogue between competent authorities and market operators

Conclusions

Drawing on the Italian experience, some issues seem to have priority:

- finding a solution to the interoperability problem at EU level, which must complement the mutual legal recognition of e-signatures in various countries
- a common definition of e-payments security features necessary to the integration of e-signatures into banking applications
- co-ordination of the national plans of e-government for *e-Europe 2005* in order to foster the use of e-signature within the Public Administration across Europe