E-payments in Europe

Oversight of payment instruments

The Banque de France’s approach

Carlos MARTIN
Head of Division
Payment Systems Department
Non-cash Means of Payment Oversight Division
Banque de France
Agenda

◆ Oversight Role
  – Rationale
  – Modus Operandi
◆ Means of payment in France
◆ Examples

Oversight role: rationale

◆ Maintaining public confidence in payment instruments and at the end in currency
◆ Role of payment instruments in the safe and efficient functioning of payment systems
◆ Statutory responsibility
  – The “Everyday Security” Act
    Article L141-4 of Financial and Monetary Code was amended as follow: « The Banque de France shall ensure the security of means of payment, as defined in Article L311-3, ... and the suitability of the relevant standards »
  – The Banque de France is responsible for the security of means of Payment
Oversight role: modus operandi

Principles

- Transparency
- Level playing field
- Co-operation with the issuer
- Coordination with Central Banks of the Eurosystem

Methodology

- Analysis the threats
- Definition of security standards
- Monitoring of compliance
- Enforcement
Means of payment in France

◆ Scope
  – Cheques
  – Bills of exchange
  – Credits transfers
  – Directs debits
  – Card payments (CB, Amex, …)
  – Electronic purse
  – Internet payment (On line communication of card number, virtual card number, P2P, virtual purse, …)
  – Mobile payment (Vocal kiosks, SMS, mobile PKI and electronic signature initiatives, …)

Means of payment in France

◆ Figures for September 2002
Examples: Electronic purse

- Concept

Electronic purse: Moneo
Electronic purse : Evaluation Process

◆ Principles
  – Security requirements
    Use of ISO/IEC 15408 (Common Criteria)
    Drafted in a generic way (Protection Profile)
  – Verification process
    For smartcard product: IT French evaluation and certification scheme to validate the security level
    For the system: the process is under definition

Electronic purse : Evaluation Process

◆ Current situation
  – Security profiles
    e-Purse and Purchase device PPs (for pilot and roll-out)
    e-Purse system
  – Security certification is part of SFPMEI licensing program
  – All the e-purse and purchase device used in the Moneo scheme are certified (EAL4+)
  – A first compliance check for the overall Moneo scheme was done by SFPMEI before roll-out
Examples: Internet Payment

- Analysis conducted in the framework of the e-Economy Initiative of the French Ministry of Economy, Finance and Industry

- Objective
  - Introduce the highest possible level of technical security economically viable

Internet Payment: Fraud

- Potentially high risk of fraud
  - Open network, “virtual” users, high speed with which the attacks can be propagated, ...

- Major vulnerabilities
  - Verification of the identity of parties involved
  - Protection of customer’s personal computer

- User protection et information
  - Unsuitable

- Disparate level of security
  - Between no security (transmission card number) to high security level (payment using smartcard technology)
Internet Payment: recommendations

- **Security Profiles**
  - For each category of payment means
  - Should take into account their nature and potential uses
  - Should serve as a guide for each step of the life cycle of means of payment
  - Could take different forms
  - Compliance with the Common criteria standard

- **Security Label**
  - Visible and understandable by consumers
  - Based on security profiles
  - To be developed and awarded by trade organisations

Internet Payment: recommendations

- **Security verification processes**
  - Independent verification, recognised competence
  - Review
    - Questionnaires, documentation (internal reports, audits), penetration testing
  - Evaluation
    - Co-operation with the French evaluation and certification scheme
    - ISO/IEC 15408 (Common Criteria)
Internet Payment: recommendations

- **Need for a secure dialogue**
  - **Strong and mutual Authentication**
    - Need to avoid transmitting authentication data over the network
    - Use of the “challenge response” technique
    - Development of PKI: Set up of a “root” registration authority to verify the identity for the purpose of generating an identity certificate
  - **Data Confidentiality**
    - during the transactions
    - storage (server, PC, …)
  - **Data Integrity, Replay Prevention of transactions, Non repudiation of transactions**

Internet Payment: recommendations

- **Improvement of user protection**
  - **Suitability, quality and user friendliness of provided products (hardware or software)**
  - **Relevant information, easily accessible and simple**
  - **Minimum security rules to comply with**
    - Sensitive data storage, virus protection, …
Examples: On-line Banking

- Definition of a protection profile for Internet Banking in co-operation with the French banks
- A generic description of the Internet banking system
- A system approach
- A dedicated assurance level

Examples: Cheques

- Exchange of truncated cheques
- Compliance with cheques regulation
- Definition of security requirements for the cheques process in cooperation with the French banks
- Banks are in charge of the verification process
- An annual evaluation report will be sent to Banque de France
Conclusion

Role of Central Banks: support efforts to strengthen security to maintain consumer confidence