EUROPEAN CENTRAL BANK
EUROSYSTEM

The European Forum on the security of retail payments

Pierre Petit

Payment Forum
Helsinki, 10 May 2012

Outline

I. **Origin and mandate**

II. **Recommendations for the security of internet payments**

III. **Future work**

1. Origin and mandate

The Forum: a platform for cooperation between central bank overseers and supervisors

- The role of the central bank
- The role of the supervisor
- The role of the market

1. Origin and mandate

The role of the central bank

- The payment system function is one of the three basic functions of the central bank
- Its objective is to promote safety and efficiency of the payment system
- The role of the overseer is to monitor systems and instruments, assess them against standards or recommendations, and foster change (when necessary)

1. Origin and mandate

The role of the supervisor

- Protection of depositors

The role of the market

- Level playing field in security of retail payments

1. Origin and mandate

Mandate of the Forum

- Facilitate common understanding among authorities of issues relevant to the security of retail payments
- Develop recommendations

II. Recommendations for the security of internet payments

- **Scope**
- **Addressees**
- **Implementation**
- **Three domains**

II. Recommendations for the security of internet payments

First domain:

- Governance
- Risk identification and assessment
- Monitoring and reporting
- Control and mitigation
- Traceability

Second domain:

- Initial customer identification
- Strong authentication

II. Recommendations for the security of internet payments

- Transaction monitoring and authorisation
- Protection of sensitive payment data

Third domain:

- Customer education and communication
- Notifications, limits
- Verification of payment by customer

III. Future work

Future work includes

- **Access to payment accounts**
- **Mobile payments**

III. Future work

Why look at access to payment account?

- EC Green Paper
- It is a market reality, not yet covered by the legal framework (Payment Services Directive)
- Security and efficiency of payments are key concerns of the Eurosystem

III. Future work

	Technical access channel	
	Customer's online banking interface	**Dedicated interface provided by the account issuer**
for information purposes	Account aggregation service*)	
for payment transaction purposes	Overlay payment service	Online banking e-payment service

*) Some account aggregation services use a dedicated interface as well.

III. Future work

Objectives of the work on payment account access

- Identification of threats to confidentiality, integrity, and availability of information, which may put privacy and money of the customer in danger
- Identification of possible mitigation measures

Annex I: Recommendations for the security of internet payments

Governance	• *Internet payment services security policy.*
Risk identification and assessment	• *Thorough risk identification and vulnerability assessments*
Monitoring and reporting	• *Central monitoring and follow-up of security incidents, incl. customer complaints* • *Reporting to management and competent authorities*
Risk control and mitigation	• *Implementation of multiple layers of security defences measures mitigating the identified risks*
Traceability	• *Appropriate tracing of all transactions*

ECB-UNRESTRICTED

Annex I: Recommendations for the security of internet payments

Initial customer identification, information	• *Customer identification prior granting access to the services.* • *PSPs should provide adequate "prior" and "regular" information to the customer about the necessary requirements (e.g. equipment, procedures) for performing secure internet payment transactions and the inherent risks.*

Strong customer authentication	• *Internet payment services should be initiated by strong customer authentication.*
	Examples for exemptions:
	  • *trusted beneficiaries included in "white lists"*
	  • *purely consultative services, with no display of sensitive customer or payment information*
	  • *For cards based on a fraud risk analysis and the usage of CVx2*

Enrolment for & provision of strong authentication tools	• *Enrolment in a safe and trusted environment (e.g. face-to-face, secure website)* • *Secure delivery of personalised security credentials or related devices and software* • *Card holders should have the option to register for strong authentication independently of a specific internet purchase.* • *Bypassing of enrolment only in exceptional cases*

ECB-UNRESTRICTED

Annex I: Recommendations for the security of internet payments

Log-in attempts, session time-out, validity of authentication	• *limit the number of authentication attempts,* • *define rules for payment session "time out"* • *set time limits for the validity of authentication*
Transaction monitoring and authorisation	• *Real-time fraud detection and prevention systems to identify suspicious transactions* • *Card payment schemes in cooperation with acquirers should elaborate a harmonised definition of e-merchant categories and require integration in the authorisation message.*
Protection of sensitive payment data	• *Sensitive payment data should be protected when stored, processed or transmitted.* • *Acquirers should encourage e-merchants not to store any sensitive card payment data or require them to have the necessary measures in place to protect these data.*

Customer education and communication

Customer alerts and notifications, setting of limits for internet payment transactions

Annex II: Oversight of electronic retail payments

Existing oversight expectations		Access channel			
Expectations in development /under consideration		Terminals		Remote	
Out of scope		contact technology	contactless technology	via internet	via other communication networks
Payment instrument	Credit transfer	*Oversight framework for CT*	*e.g. proximity mobil payments*	*access by the account holder directly and in person* *access to the payment account involving a third party provider*	*(e.g. voice)*
	Direct debit	*Oversight framework for DD*		*E- mandate issued in the online banking environment* *Creditor based E-mandate flow*	*(e.g. voice)*
	Cards (physical, virtual)	*Oversight framework for cards*		*All cards, including the charging of wallet solutions; except business cards*	*(e.g. voice)*
	E-money (physical, virtual)	*EMSSO, Harmonised approach &standards for PI* *Review ongoing (adjustments for virtual e-money)*		*only for charging of e-money accounts* *no harmonised standards for transfers of e-money between two e-money accounts)*	
	Other (e.g. closed loop, billing systems, consultative services)		*e.g. ticketing, transport*	*e.g. account aggregation*	*e.g. SMS*

Annex III: Retail payment systems and payment instruments oversight – relevant frameworks*

- **Aug 1998:** Report on electronic money
- **May 2003:** Electronic money system security objectives according to the common criteria methodology (EMSSO report)
- **Jun 2003:** Oversight standards for euro retail payment systems
- **Jun 2006:** Business continuity oversight expectations for systemically important payment systems (SIPS)
- **Jan 2008:** Oversight framework for card payment schemes – standards (CPS)
- **Feb 2009:** Eurosystem oversight policy framework
- **Feb 2009:** Harmonised oversight approach and oversight standards for payment instruments
- **Oct 2010:** Oversight frameworks for direct debits and credit transfer schemes
- **Mar 2012:** Oversight expectations for links between retail payment systems *(Consultation)*
- **Apr 2012:** Recommendations for the security of internet payments *(Consultation)*

** http://www.ecb.europa.eu/pub/pub/paym/html/index.en.html*