EUROPEAN CENTRAL BANK

EUROSYSTEM

ECB-UNRESTRICTED

Stephanie Czák
Market Infrastructure Expert

European Forum on the Security of Retail Payments (SecuRe Pay)

Recommendations for the security of internet payments vs. Draft recommendations for payment account access services

Frankfurt, 5 March 2013

Presentation overview

1. Public consultation
2. Scope and addressees
3. Relationship between both
4. Outlook
5. Questions /Discussion
6. Background information

EUROPEAN CENTRAL BANK ©
www.ecb.europa.eu

a. Recommendations for the Security of Internet Payments **("Internet Recommendations")**

Public consultation:

- Mid-April to June 2012
- 59 respondents from 17 EU Member States
- European and national associations and authorities

b. Draft recommendations for "Payment account access" services **("PAA Draft Recommendations")**

Public consultation:

- Launched on 31 January 2013
- Response by 12 April 2013

a. Internet Recommendations

Main concerns and issues raised during public consultation:

- Rationale for the internet recommendations (extent of oversight/supervision)
- Balance of security and customer convenience (risk based approach, minimum requirements)
- Definition of strong customer authentication (some misunderstandings)
- Reference to existing standards (technology neutral)
- Implementation issues (level playing field, geographic scope, date)
- Consistency with other EU legislation (e.g. AML, data protection)
- Functional scope (business cards, e-mandates, e-money)
- Application of recommendations to customers and e-merchants

EUROPEAN CENTRAL BANK ©
www.ecb.europa.eu

Main changes to the recommendations 1/3

Rec		Type of change	Main aspects
1	**Governance**	Scope; clarifications	Added: payment schemes, Clarified: independent risk management function
2	**Risk assessment**	Scope; clarifications	Added: payment schemes, reference to incident management
3	**Incident monitoring and reporting**	Scope; clarifications; KC	Added: payment schemes, New: merchant's cooperation on data breaches and other security incidents with their acquiring PSPs and relevant law enforcement agencies
4	**Risk control and mitigation**	Scope, clarifications	Added: payment schemes, Clarification: "data minimisation", man in the middle & man in the browser attacks
5	**Traceability**	Scope	Added: e-mandate reference
6	**Initial customer identification, information**	Clarifications	References to anti-money laundering

Main changes to the recommendations 2/3

Rec		Type of change	Main aspects
7	**Strong customer authentication**	Major, new KCs and BP	Revised: exemptions for strong customer authentication Removed: reference to 3D secure and CVX2 New: bilateral authentication when communicating with e-merchants. New: elements linking the authentication to a specific amount and payee Revised: definition of safe and trusted environment
8	**Delivery of authentication tools & software to the customer**	Clarifications	Delivery of payment-related software to customers, safe and trusted environment Removed: reference to CVX2
9	**Log-in attempts, session time out, validity of authentication**	Deletion	Reference to specific number of minutes

Main changes to the recommendations 3/3

Rec		Type of change	Main aspects
10	**Transaction monitoring**	Clarifications, new KC, BP upgraded to KC	Added: e-mandate Replaced: real-time by prior the execution New: separate reference to Acquiring
11	**Protection of sensitive payment data**	Scope, clarifications	Added: reference to e-mandate Clarified: secure encryption is applied between the communicating parties
12	**Customer education and communication**	New KC, card BP becomes general	New: Clear separations of payment related processes (e.g. redirections) from the merchants' online shop
13	**Notification, setting of limits**	Clarifications	editorial
14	**Customer information on payment initiation /execution**	Clarifications	KC 14.1 only for CT/e-mandate

EUROPEAN CENTRAL BANK ©
www.ecb.europa.eu

Presentation overview

1. Public consultation
2. **Scope and addressees**
3. Relationship between both
4. Outlook
5. Questions /Discussion
6. Background information

EUROPEAN CENTRAL BANK ©
www.ecb.europa.eu

a. Internet Recommendations

Scope:

- the execution of **card payments** on the internet, including ***virtual card payments***, as well as the registration of card payment data for use in "***wallet solutions***".
- the execution of **credit transfers** (CTs) on the internet.
- the issuance and amendment of direct debit **electronic mandates.**
- transfers of **electronic money** between two e-money accounts via the internet.

b. PAA Draft Recommendations

Scope:

- Account information services.
- Payment initiation services.

EUROPEAN CENTRAL BANK ©
www.ecb.europa.eu

a. Internet Recommendations

Addressees:

- All **PSPs**, as defined in the Payment Services Directive, providing internet payment services.
- **Governance authorities** of payment schemes
- E-Merchants (indirectly via the PSPs and in form of best practices)

b. PAA Draft Recommendations

Addressees:

- **Third party service providers** providing internet-based payment account access services.
- **Account servicing payment service providers**.
- **Governance authorities** of schemes providing payment account access services.
- E-Merchants (indirectly via the TPs and in form of best practices)

Presentation overview

1. Public consultation
2. Scope and addressees
3. **Relationship between both**
4. Outlook
5. Questions /Discussion
6. Background information

EUROPEAN CENTRAL BANK ©
www.ecb.europa.eu

Guiding principles:

- Addressees should perform specific assessments of the risks.
- Strong customer authentication.
- Effective processes for authorising transactions, as well as for monitoring transactions and systems should be implemented in order to identify abnormal customer payment patterns and prevent fraud.
- Customer awareness and education programmes on security issues should be provided.

Structure and content:

- Formulated as generically as possible to accommodate continual technological innovation. Recommendations constitute minimum expectations.
- Each recommendation is specified through key considerations (KC). Addressees are expected to comply with both the recommendations and KCs or need to be able to explain and justify any deviation from them upon the request of the relevant competent authority (“comply or explain” principle).
- Some best practices (BP) are included, which addressees and other relevant market participants are encouraged to adopt.

EUROPEAN CENTRAL BANK ©
www.ecb.europa.eu

PAA Draft Recommendations

Specific issues 1/2

- Implementation: The Forum would welcome an extension of the scope of the PSD to cover payment account access services and their providers.
- Aims: Maintaining the same level of security as in the internet recommendations.
- Account servicing PSPs should be able to differentiate between payment account access by third parties (TPs) and access by account owners without TP involvement.
- Active customer opt-in for account information services & payment initiation services.
- TPs (where applicable) should perform strong customer authentication for the customer's access to payment account access services. (TP could agree with account servicing PSPs to rely on the latters authentication methods).

PAA Draft Recommendations

Specific issues 2/2

- A TP should only access the payment account upon the customer's specific instruction and on a case-by-case basis.
- Cooperation in case of ex post dispute /fraud between e-merchants, TPs and account servicing PSPs.
- Storage, use, access to sensitive payment data by TPs
- TP should have a transparent liability regime to the customer
- Payment account access services should not compromise the possibility for the account servicing PSP to send security-related messages alerts to the customer.

EUROPEAN CENTRAL BANK ©
www.ecb.europa.eu

Presentation overview

1. Public consultation
2. Scope and addressees
3. Relationship between both
4. **Outlook**
5. Questions /Discussion
6. Background information

EUROPEAN CENTRAL BANK ©
www.ecb.europa.eu

Outlook SecuRe Pay Work

- Review of the recommendations on Payment account access" services until end of 2013
- Integration of the recommendation in the supervisory and oversight expectations, common Assessment Guide
- Mobile payments
- Options to improve information sharing on major security incidents

Presentation overview

1. Public consultation
2. Scope and addressees
3. Relationship between both
4. Outlook
5. **Questions /Discussion**
6. Background information

EUROPEAN CENTRAL BANK ©
www.ecb.europa.eu

Questions and comments from your side?

EUROPEAN CENTRAL BANK ©
www.ecb.europa.eu

Presentation overview

1. Public consultation
2. Scope and addressees
3. Relationship between both
4. Outlook
5. Questions /Discussion
6. **Background information**

EUROPEAN CENTRAL BANK ©
www.ecb.europa.eu

European Forum on the Security of Retail Payments (SecuRe Pay):

- Established in 2011.
- Voluntary cooperative initiative between authorities (in particular between supervisors of PSPs and overseers.
- Facilitation of common knowledge and understanding on issues related to the security of electronic retail payment services and instruments.
- Geographic scope: European Union/European Economic Area.
- Functional scope: whole processing chain of electronic retail payment services (excluding cheques and cash), irrespective of the payment channel.
- Recommendations to address major weaknesses and vulnerabilities.
- Mission: Foster the establishment of a harmonised EU/EEA-wide minimum level of security.

SecuRe Pay Members:

BE	Nationale Bank van België/Banque Nationale de Belgique
BG	Българска народна банка (Bulgarian National Bank)
CZ	Česká národní banka
DK	Danmarks Nationalbank Finanstilsynet
DE	Deutsche Bundesbank Bundesanstalt für Finanzdienstleistungsaufsicht
EE	Eesti Pank Finantsinspektsioon
IE	Central Bank of Ireland
GR	Bank of Greece
ES	Banco de España
FR	Banque de France Autorité de Contrôle Prudentiel
IT	Banca d'Italia
CY	Central Bank of Cyprus
LV	Latvijas Banka Finanšu un kapitāla tirgus komisija
LT	Lietuvos bankas
LU	Banque centrale du Luxembourg Commission de Surveillance du Secteur Financier
HU	Magyar Nemzeti Bank Pénzügyi Szervezetek Állami Felügyelete
MT	Central Bank of Malta
NL	De Nederlandsche Bank
AT	Oesterreichische Nationalbank Österreichische Finanzmarktaufsicht
PL	Narodowy Bank Polski Komisja Nadzoru Finansowego
PT	Banco de Portugal
RO	Banca Națională a României
SI	Banka Slovenije
SK	Národná banka Slovenska
FI	Suomen Pankki – Finlands Bank Finanssivalvonta
SE	Sveriges Riksbank Finansinspektionen
UK	Financial Services Authority
	European Banking Authority
	European Central Bank

SecuRe Pay Observers:

IS	Central Bank of Iceland Fjármálaeftirlitið
LI	Liechtensteinische Landesbank 1861 Finanzmarktaufsicht Liechtenstein
NO	Norges Bank Finanstilsynet – The Financial Supervisory Authority of Norway
	European Commission
	Europol

Selected terminology 1/2

Virtual cards:

- A card-based payment solution where an alternative, temporary card number with a reduced validity period, limited usage and a pre-defined spending limit is generated which can be used for internet purchases.

Wallet solutions

- Solutions that allow a customer to register data relating to one or more payment instruments in order to make payments with several e-merchants.

Account information services (AIS)

- Internet-based aggregation/visualisation services that collect information on different accounts held by an account owner with one or more account servicing payment service providers (PSPs) and which can be accessed via the internet. The consolidated information of these accounts is presented to the account owner in a user friendly way via a single website.

Payment initiation services (PIS)

- Internet-based services to initiate payment transactions via payment accounts. The technical implementation of this service can differ based on whether or not the payee is actively involved in the payment initiation and whether the TP's software is used by the account owner to transmit his/her credentials to the account servicing PSP.

EUROPEAN CENTRAL BANK ©
www.ecb.europa.eu

Selected terminology 2/2

Governance authority:

- Accountable for the overall functioning of the scheme that promotes the payment instrument in question and ensuring that all the actors involved comply with the scheme's rules. Moreover, it is responsible for ensuring the scheme's compliance with oversight standards.

Third party service provider (TP):

- Service providers offering internet-based AIS and/or PIS for payment accounts for which they are not the account servicing PSP are qualified as TPs. Focus is on the legal entity offering the AIS and/or PIS and which enters into an agreement with the account owner. Outsourcing agreements are considered to be under the outsourcer's responsibility. Both licensed PSPs and non-licensed service providers can offer services as a TP.

Account servicing PSP

- Issue (and maintain) payment accounts on behalf of customers (account owners). An account servicing PSP can decide to outsource certain functionalities to other companies (e.g. IT data processing centres, network providers), however, any outsourcing must be based on a contractual agreement defining the parties' respective rights and responsibilities.

EUROPEAN CENTRAL BANK ©
www.ecb.europa.eu

Recommendations for "payment account access" services

Invitation to comment

- All interested parties are invited to comment on the draft "Recommendations for payment account access services".
- The respective national central banks and national supervisors of payment service providers (PSPs) will serve as contact points for national PSPs and other actors in their country and provide further information and/or answer questions regarding these recommendations.
- Any comments received will be published on the internet, unless it is clearly indicated that the author does not consent to such publication. Comments should only be made using the response template provided and be submitted to the ECB in English, or in the relevant official EU language.

Deadline: 12 April 2013

Download:

- Response template
- Recommendations for "payment account access" services. Draft document for public consultation.

Address for submission:

- European Central Bank
  Secretariat Division
  Kaiserstrasse 29
  D-60311 Frankfurt am Main
  Germany
  Fax: +49 69 1344 6170
  E-mail: ecb.secretariat@ecb.europa.eu

Contact details

Stephanie Czák

stephanie.czak@ecb.europa.eu

+49 69 1344 5091

Disclaimer

The views expressed in this presentation are those of the speaker and do not necessarily reflect those of the European Central Bank.