Aktualitātes no Berlin Group NextGen PSD2 konferences.

Māris Ozoliņš

Latvijas
Komercbanku
Asociācija

Rīga, 2017. gada 15. novembris

THE *Berlin* GROUP
A EUROPEAN STANDARDS INITIATIVE

NextGenPSD2 Conference 2017

October 25, 2017

BUILDING BRIDGES

Participants NextGenPSD2 Taskforce

THE *Berlin* GROUP
A EUROPEAN STANDARDS INITIATIVE

First Data.

nets

Swedbank

BITS

Banking & Payments Federation Ireland

Danske Bank

SDC

Association of Latvian Commercial Banks

VISA

Payments UK
Leading the way we pay

PAN-NORDIC CARD ASSOCIATION

SEB

equensWorldline

Dutch Payments Association

SIA

N26

Deutsche Bank

trionis

SOCIETE GENERALE

Bancontact

Payment Services Austria

SIX Payment Services

stet

ZWIĄZEK BANKÓW POLSKICH

Die Deutsche Kreditwirtschaft

Finanzgruppe Deutscher Sparkassen und Giroverband

SIBS FORWARD PAYMENT SOLUTIONS

Redsýs

bankenverband

DZ BANK

HypoVereinsbank

Bundesverband Öffentlicher Banken Deutschlands

Postbank
Eine Bank fürs Leben.

PRETA

Bundesverband der Deutschen Volksbanken und Raiffeisenbanken

EURO Kartensysteme

HRVATSKA UDRUGA BANAKA
CROATIAN BANKING ASSOCIATION

ICBPI

Scope of Berlin Group NextGenPSD2

- QTSPs issuing certificates for identification of the PSP
- Contents eIDAS certificates for PSD2

- SCA & XS2A Interface Design
- Core PSD2 services & extended services
- TPP Identification
- PSU consent

LICENSING - REGISTRATION

1

SETUP

3

DISPUTE HANDLING

5

- Public registers operated by the national authorities with information about authorised PSPs

CERTIFICATE HANDLING

2

- Registry/Routing service containing information helping the TPPs to find ASPSP API locations, contacts and documentation

TPP – ASPSP INTERFACE

4

- Incident reporting
- Dispute resolution

THE *Berlin* GROUP
A EUROPEAN STANDARDS INITIATIVE

* Courtesy of PRETA SAS

XS2A main actors
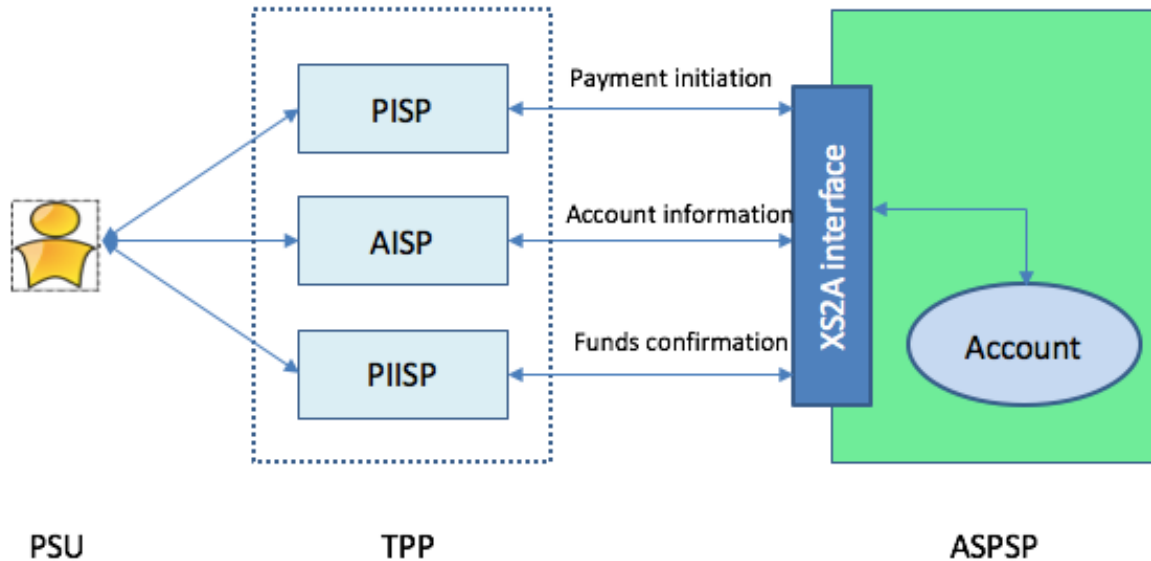
Services supported by the XS2A interface

Core Services are supported by each implementation of the XS2A interface

- Payment initiation service
  - As defined by PSD2 article 66
- Account information service
  - As defined by PSD2 article 67
- Confirmation of funds service
  - As defined by PSD2 article 65

- No contract between ASPSP and TPP

Extended Services may be supported by an implementation of the XS2A interface

- To be decided by the ASPSP
- May be specified in future
  - By the Berlin Group as part of a new release of the specifications
  - By a group of interested ASPSP
  - By a single ASPSP

- A contract between ASPSP and TPP might be necessary

Excursion: eIDAS compliant qualified certificates

> Trust Centre QTSP
> (eIDAS compliant)

- ■ eIDAS regulation
    - Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market
- ■ Qualified certificates have to be issued by a qualified trust service provider (QTSP)
    - QTSP do exist in different countries of the EU
    - After registration by the national authority a TPP has to apply for a qualified certificate by one of the existing QTSP
- ■ Qualified certificates compliant with EBA RTS are not available today
    - But standardisation has started by corresponding ETSI working group
- ■ It is expected that compliant certificates will be provided in time by some QTSP

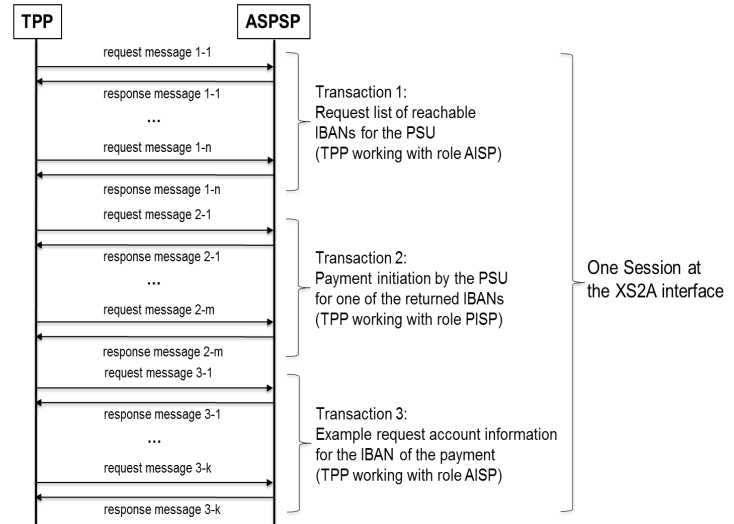# Key concepts: Message – Transaction – Session at XS2A interface

- **Session at the XS2A interface**
  - Set of transactions executed consecutively at the XS2A API

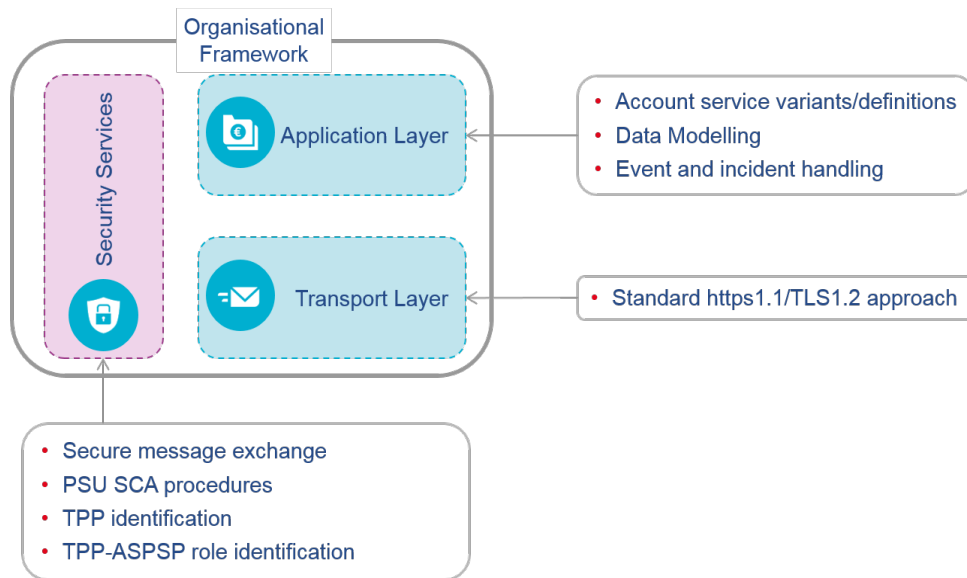- **Support of sessions at the XS2A interface is optional for the ASPSP**

- **Important:**
  - For a single transaction a TPP has to use only one of its roles
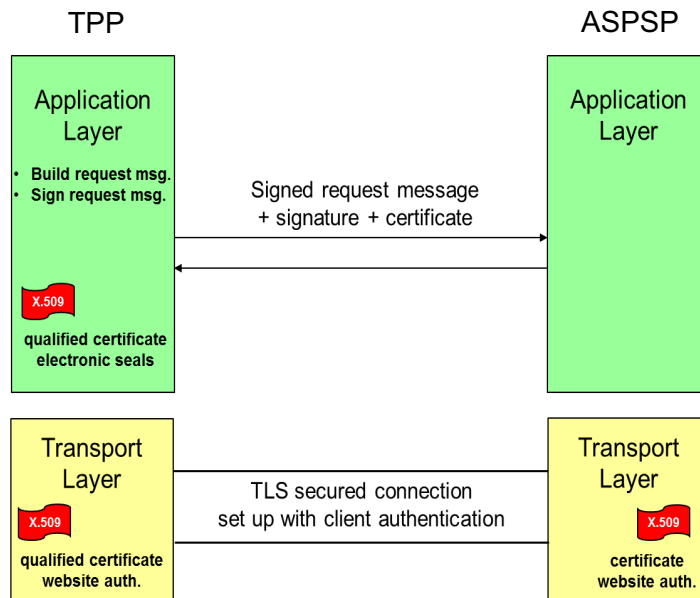 - Within a session a TPP can use different of its roles

Diagram content:

TPP		ASPSP
request message 1-1	→	
response message 1-1	←	
...		
request message 1-n	→	
response message 1-n	←	

Transaction 1:
Request list of reachable IBANs for the PSU
(TPP working with role AISP)

request message 2-1	→	
response message 2-1	←	
...		
request message 2-m	→	
response message 2-m	←	

Transaction 2:
Payment initiation by the PSU for one of the returned IBANs
(TPP working with role PISP)

request message 3-1	→	
response message 3-1	←	
...		
request message 3-k	→	
response message 3-k	←	

Transaction 3:
Example request account information for the IBAN of the payment
(TPP working with role AISP)

One Session at the XS2A interface

3 levels of communication are standardized

Organisational Framework

Security Services

Application Layer
- Account service variants/definitions
- Data Modelling
- Event and incident handling

Transport Layer
- Standard https1.1/TLS1.2 approach

- Secure message exchange
- PSU SCA procedures
- TPP identification
- TPP-ASPSP role identification

Key concepts: Identification of a TPP at the XS2A interface

- ■ Certificate shall contain the role of the TPP which is necessary for the corresponding transaction
- ■ Always identification at transport layer
- ■ Identification at the application layer only if requested by the ASPSP

- ■ ASPSP will reject any request
  - If the identification of the TPP cannot be verified correctly
  - If the certificate does not contain the correct role

TPP

ASPSP

Application Layer
- Build request msg.
- Sign request msg.

X.509

qualified certificate
electronic seals

Signed request message
+ signature + certificate

Application Layer

Transport Layer

X.509

qualified certificate
website auth.

TLS secured connection
set up with client authentication

Transport Layer

X.509

certificate
website auth.

Key concepts: Strong customer authentication (SCA)

Strong customer authentication

■ Requirement of PSD2 and EBA RTS

- For access to account information
- For payment initiation

■ Exemptions compliant with EBA RTS are possible

- Exemptions are optional
- Decision about an exemption is always in the responsibility of the ASPSP

Key concepts: Strong customer authentication (SCA)

Strong customer authentication

■ Different methods and procedures exist for executing a strong customer authentication of the PSU as part of a transaction

- ASPSP decides (together with PSU) which methods/procedures have to be used for SCA

- Specification of the Berlin Group does support all methods/procedures in a generic way

- ASPSP informs as part of its documentation about methods/procedures to be used and (if necessary) how to implement these as part of the TPP interface

THE *Berlin* GROUP

A EUROPEAN STANDARDS INITIATIVE

Copyright Berlin Group

Key concepts: Strong customer authentication (SCA)

Different approaches for implementing SCA

- Redirect approach
  - PSU is redirected to web interface provided by the ASPSP

- Decoupled approach
  - SCA out-of-band using a special APP
  - Same behaviour as for Online Banking

- Embedded approach
  - PSU enters credentials on the interface of the TPP

Decoupled approach:
SCA using specialised App

SCA App

TPP

Embedded approach:
Credentials forwarded by TPP

XS2A Interface

SCA Server

SCA interface ASPSP

Redirect approach:
Credentials inserted using interface provided by ASPSP

THE *Berlin* GROUP
A EUROPEAN STANDARDS INITIATIVE
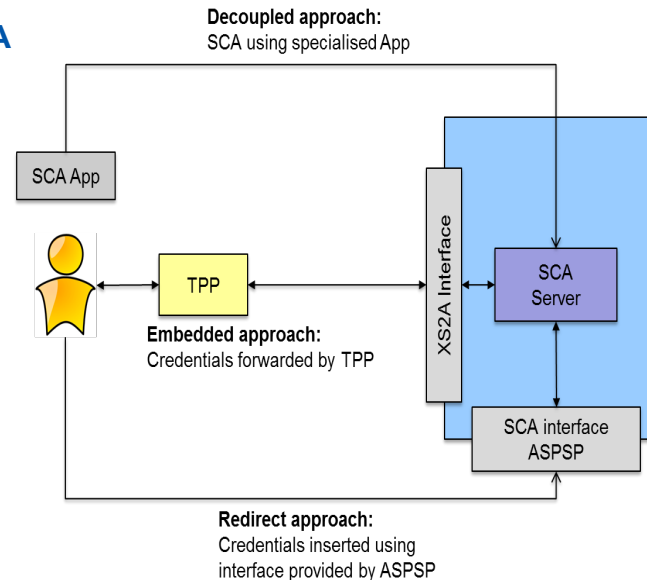
Key concepts: Authorisation of the PSU consent

Each transaction at the XS2A interface is subject to the consent of the PSU

- How to proof that a PSU has given its consent to a transaction?

- Easy if SCA has to be used for this transaction
  - By executing SCA as part of a transaction the PSU gives its commitment to this transaction

- But how to do this
  - if no SCA has to be used for the transaction ?
  - if the PSU is not directly involved in the transaction?
    - reading account information by an AISP according to article 31 EBA RTS

Key concepts: Authorisation of the PSU consent

Using the special "Establish account information consent" transaction at the XS2A interface

- Includes SCA of the PSU

- Result is an access token given to the TPP

- TPP can use this for following accesses of account information of that PSU

Using OAuth2 protocol for asking the PSU for a confirmation

- Result is an access token given to the TPP

- TPP can use this for following accesses of account information of that PSU

Use cases

> Use case	> Service	> Role of the TPP	> Support optional	> PSU directly involved
Initiation of a single payment	Payment initiation service	PISP	no	yes
Establish account information consent	Account information service	AISP	yes[2]	yes
Get list of reachable accounts	Account information service	AISP	yes	no
Get balances for a given list of accounts	Account information service	AISP	no	no
Get transaction information for a given account once	Account information service	AISP	no	no
Get a confirmation on the availability of funds	Funds confirmation service	PISP	no	no

[2] Establishing the consent on account information access can alternatively be managed by the OAuth2 protocol

Payment Initiation Service.

Use cases – Wallet vs. Payment Initiation only

TPP - Wallet
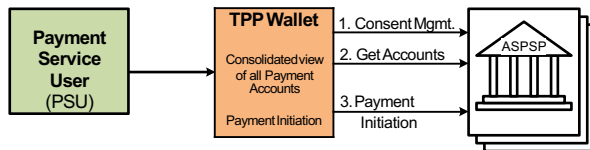
Use Case:

- This TPP provides the PSU a consolidated view of his payment accounts across all banks and allows the initiation of payments from these accounts.

- Regular usage of this service by the PSU, based on a contract between PSU and TPP.

Payment Initiation

- In case of a TPP-Wallet, all PSU data needed for the payment Initiation are available on TPP side.

Payment Initiation Service (Online Shop)
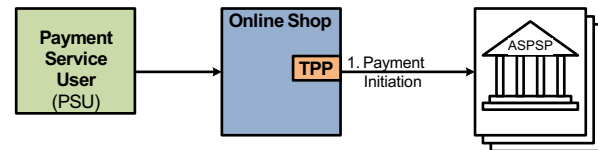
Use Case:

- The main purpose of this service is a payment initiation for an online Shop.

- The PSU uses this Service only on demand, no permanent relationship between PSU and TPP

Payment Initiation

- The TPP needs for the Payment Initiation additional information from the PSU or the ASPSP (e.g.: IBAN). To be captured by the PSU or via an additional AIS request provided by the ASPSP.

Payment Flows

9. SEK (Krona) Payment SE-SE

3. EUR Payment DE-SE

8. PLN (Zloty) Payment PL-SE

6. USD Payment DE-DE

1. EUR Payment DE-DE

USA

5. USD Payment DE-US

7. EUR Payment HR-PL

2. EUR Payment DE-ES

4. HRK (Kuna) Payment DE-HR
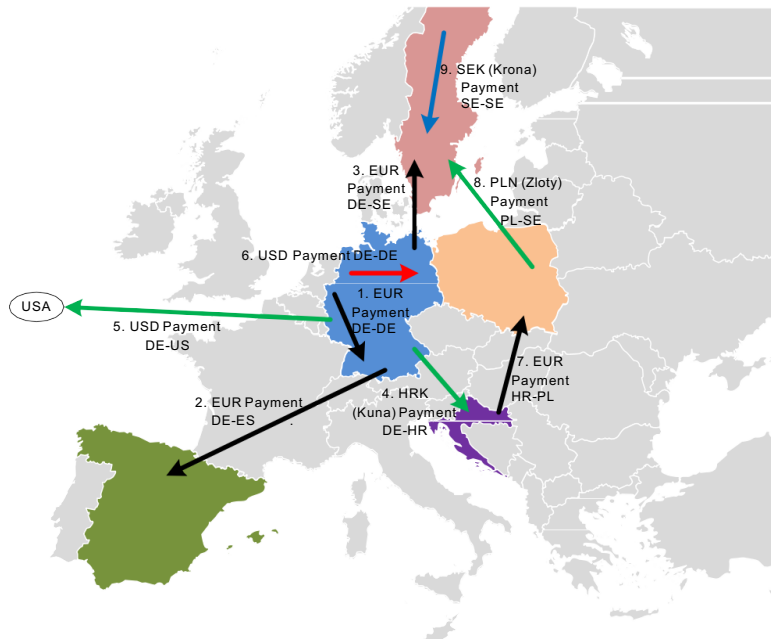
EUR Payments (SCT & SCT^{inst})
- The SEPA Credit transfer is availbale in all european countries (incl. Instant payments)
- Format: pain.001.001.03 (Germany)
- Examples: 1. 2. 3. 7.

Domestic Payments in local currency (nonEUR)
- Propriotary formats for domestic payments in non EUR countries available.
- Format: tbc. (pain.001 based or legacy format)
- Example: 9.

Domestic Payments in foreign currency
- Propriotary formats for domestic payments in foreign currency available
- Format: european standard format is not available (in Germany DTAZV)
- Example: 6.

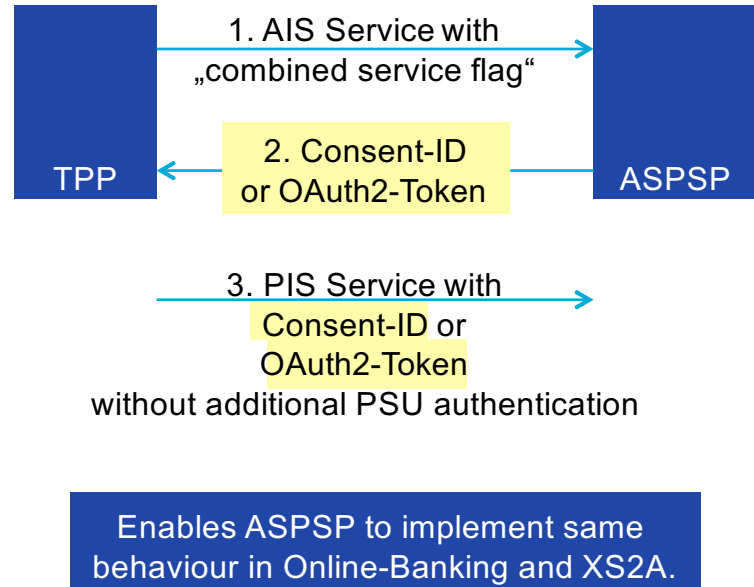**Cross-Border Payments (non EUR)**
- Propriotary formats for cross-border payments available
- Format: european standard format is not available (in Germany DTAZV)
- Examples: 4. 5. 8.

Copyright Berlin Group
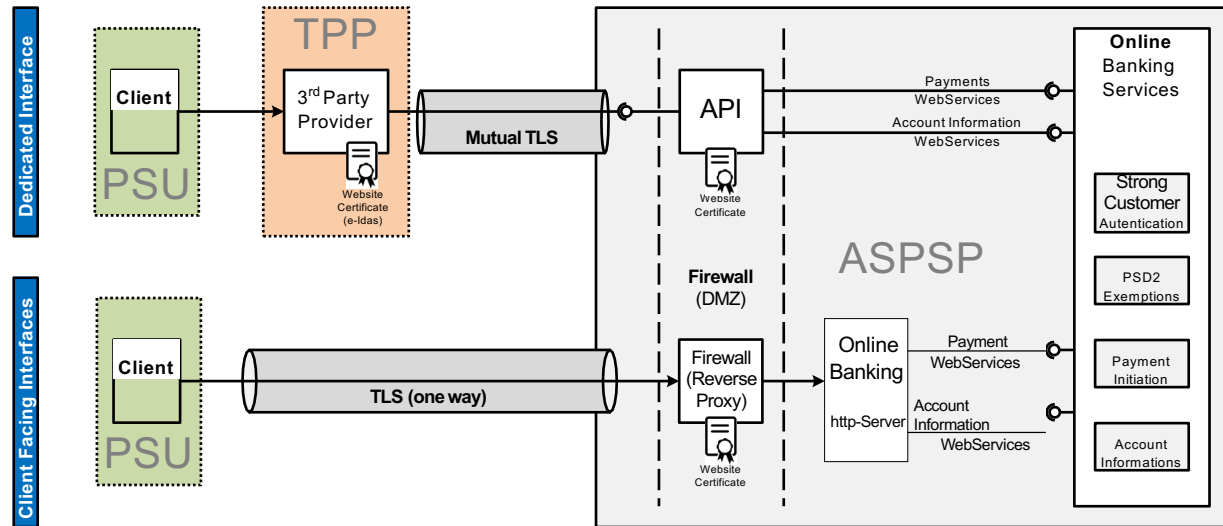
THE *Berlin* GROUP
A EUROPEAN STANDARDS INITIATIVE

Combination of AIS and PIS (Consent ID or optional OAuth2)

- TPP can always combine AIS and PIS results in the TPP/PSU interface, e.g. in a wallet like TPP solution, where recurring account access is supported.

- In addition, a combination of AIS and PIS is supported in the standard e.g. for batch booking banks to also support easy access and risk management solutions of TPPs.

- This is an optional function for the ASPSP in the standard.

TPP

1. AIS Service with „combined service flag"

2. Consent-ID or OAuth2-Token

ASPSP

3. PIS Service with Consent-ID or OAuth2-Token

without additional PSU authentication

Enables ASPSP to implement same behaviour in Online-Banking and XS2A.

THE *Berlin* GROUP

A EUROPEAN STANDARDS INITIATIVE

High Level Overview: Bank Systems for Online Banking and API

THE *Berlin* GROUP
A EUROPEAN STANDARDS INITIATIVE

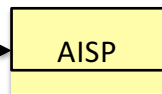# Account Information Service.

Latvijas Komercbanku Asociācija

Establishing account information consent and presenting account information data to the PSU consist of five steps

1. Get PSU account access consent
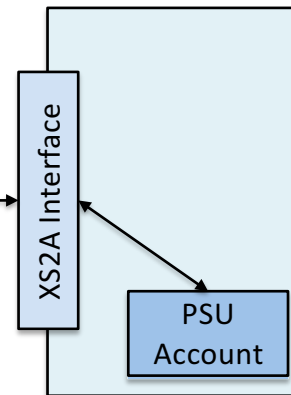2. Submit consent details
3. Consent authorisation by PSU (SCA)

AISP

XS2A Interface

PSU Account

4. Account access
5. Data presentation

Step 2 & 3 can alternatively be handled via OAuth2 protocol

Some things worth noting for the consents (step 2)

- Consent can be given for balances only or for transactions
- Credit card transactions if available. PAN tokenized or masked.
- Possibility to set validity for recurring access

Next steps.

Latvijas Komercbanku Asociācija

Next Steps Berlin Group NextGenPSD2

- **Public Market Consultation and Finalisation Version 1.00**
    - Market Consultation ends on 17 November 2017 (COB)
    - EC endorsement of EBA RTS and official publication now expected in November 2017
    - Aim: Publish NextGenPSD2 Framework standards before end of 2017
- **Organise Implementation & Market Involvement**
    - After publication of V1.00 increased focus on Implementation Support
    - Provide guidance on implementation and interoperability issues
    - Offer support with e.g. best practices guidelines where needed
    - Contribute to future evolution of the standards
- **Organise Testing Approach**
    - Art. 27(6) Final draft EBA RTS: "ASPSPs shall make available a testing facility, including support, for connection and functional testing by TPPs"
    - Harmonised interoperability standards provide a basis for harmonised testing requirements, common test policy, testcase catalogue and testtools
    - Harmonised testing simplifies interoperability testing and renders cost and maintenance efficiencies

Aktuāli

> Tehniskā standarta par klientu autentifikāciju un komunikācijām gala versijas publicēšana EK plānota 25.novembrī. Pēc tam 3 mēnešu laikā Eiroparlaments to oficiāli apstiprinās. Līdz ar to, PSD2 ieviešanas termiņš paredzēts 2019.gada vasaras beigās.

> Standartā būs paredzēts, ka bankām jāpiedāvā rezerves opcija ar «screen scraping», ja API nenodrošina atbilstošu veiktspēju. Tomēr, tiks paredzēts testēšanas periods, kura laikā bankām jāpierāda, ka API darbojas veiksmīgi. Tādā gadījumā bankas varēs nepiedāvāt «screen scraping» rezerves opciju. *(2019.g.sept – 6 mēneši = deadline for internal readiness.)*

> Tikai šobrīd ETSI uzsāk darbu pie eIDAS standarta izstrādes, lai nodrošinātu TPP identifikāciju atbilstoši PSD2. Plānots, ka standarts tiks publicēts 2018.gada vasarā.

Jautājumi?

Māris Ozoliņš

Maris.Ozolins@instavision.eu

Žanete Glaudiņa

Zanete.Glaudina@lka.org.lv

Latvijas
Komercbanku
Asociācija