PSD2 - Second Payment Services Directive

Information Set

Association
of Latvian
Commercial Banks

PSD2: at the starting line

> February 2017 – EBA published the final draft RTS on SCA

> November 2017 – EC published the final RTS on SCA

> January 13 2018 – Deadline to transpose PSD2 in Member States

> June 2018 - eIDAS standard for PSD2 will be published by ETSI.

> September 2019 – RTS on SCA enter into force

>
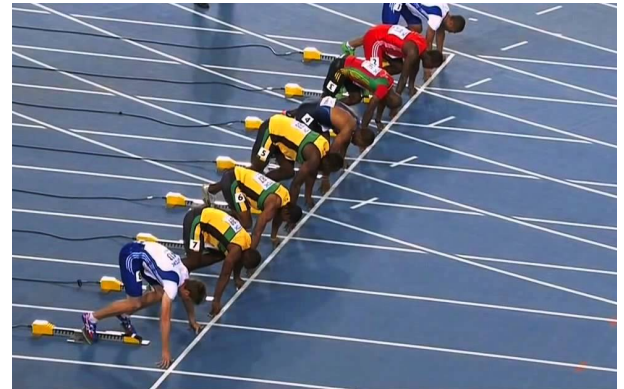
4 types of stakeholders in the bank

Business

Technology

Legal

Strategy

What is PSD2?

PSD adopted in 2007

Single market for payments in EU

Digitalisation progressed, new players for online payments have appeared

What is PSD2?

Problem: new players are outside of PSD, not regulated

PSD2 introduces new roles, like TPP (Third Party Payment Services Providers)

PSD2 extends the scope of PSD

New role definitions (AISP, PISP, ASPSP)

Improved consumer protection, SCA (Strong Customer Authentication)

Ban on surcharging

Applicable to all payments and accounts within the EU and the EEA, regardless of the currency

Third-party providers will get the right to access the payment service user's account

Aim of PSD2

> **Make payments safer**

> **Increase consumers' protection**

> **Foster innovation and competition**

> **Ensure a level playing field for all players (including the new ones)**

Business drivers

Customer expectations

Customers, especially millenials, expect full digital service and are not loyal to established banks.

Technology

New technologies continue to grow: AI, bots, blockchain, biometrics, big data, IoT,... Flexibility and rapid experimentation is needed.
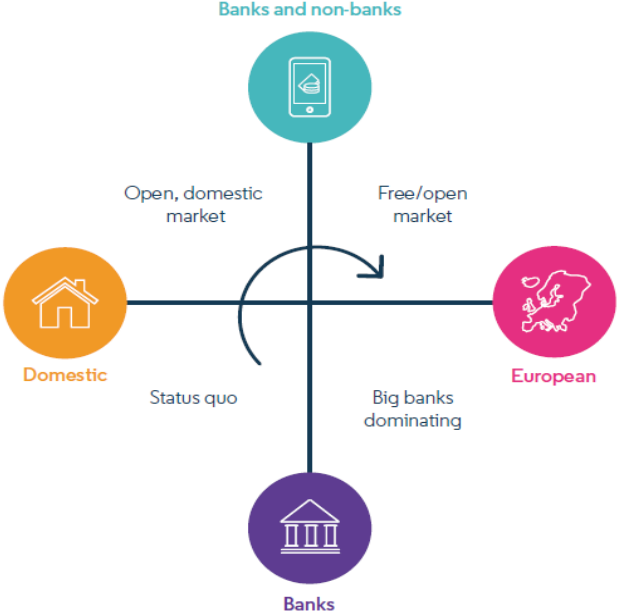
Competition

Today banks have processes and technology to maintain stability and minimise risk. Not the case for fintechs. Agility and customer focus are future competitive factors.

Regulation

Old regulations do not work. New bank competitors have emerged who simply do not care about regulation.

Scenarios

Source: Evry

New potential areas of growth for the TPP

Become aggregator for customers with multiple bank relationships

Approach new customer segments by creating unique products

Create new products together with banks' accelerator programs

New potential areas of growth for the TPP

Launch new products to banks' customers

Provide new customer insight by accessing their external data

And many more!

Participants NextGenPSD2 Taskforce

Main PSD2 initiatives

Initiative	Focus	Description
ERPB (Euro Retail Payments Board)	Overall facilitation of PSD2	Align all relevant standardization initiatives, consider implications and synergies. DO NOT develop technical specs
The Berlin Group	Development of XS2A	Specification (application, security and transport levels) and organizational framework
CAPS (Convenient access to PSD2 services)	Common framework for ecosystem	Intermediary «Hub» between ASPSPs and PISPs/AISPs to concentrate the connections
PRETA (Subsidiary of EBA Clearing)	Directory of licensed participants	Establish real-time directory of authorized third parties and banks

XS2A main actors
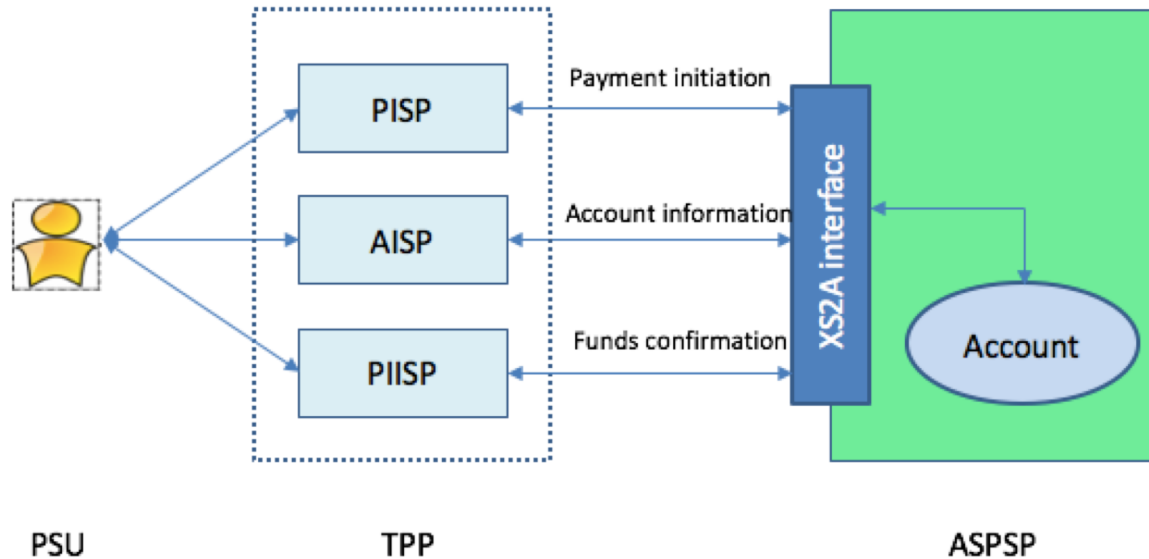
PSD2 does not regulate APIs in detail

> In theory, each European bank could develop (and test, and maintain) its own proprietary XS2A communication standard……… to which each TPP can connect
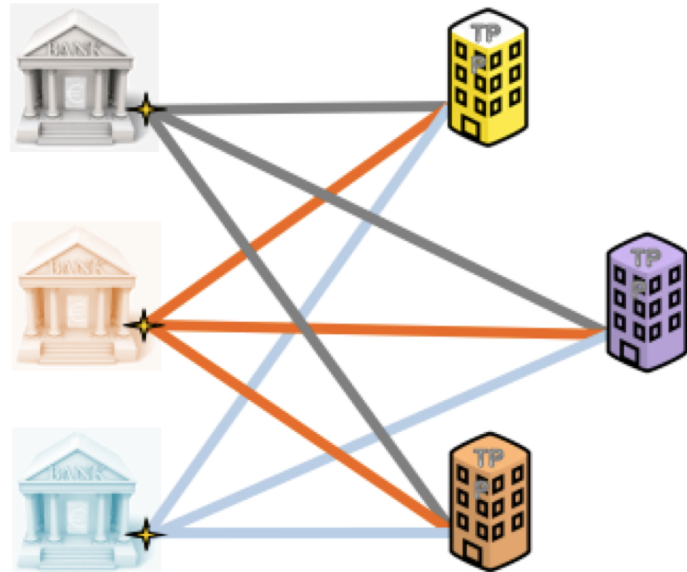
There are >4000 banks and 1000s of TPPs

Development, testing and maintenance of proprietary, bank-specific XS2A communication standards would create a pan-European IT nightmare and ultrahigh costs for banks and TPPs
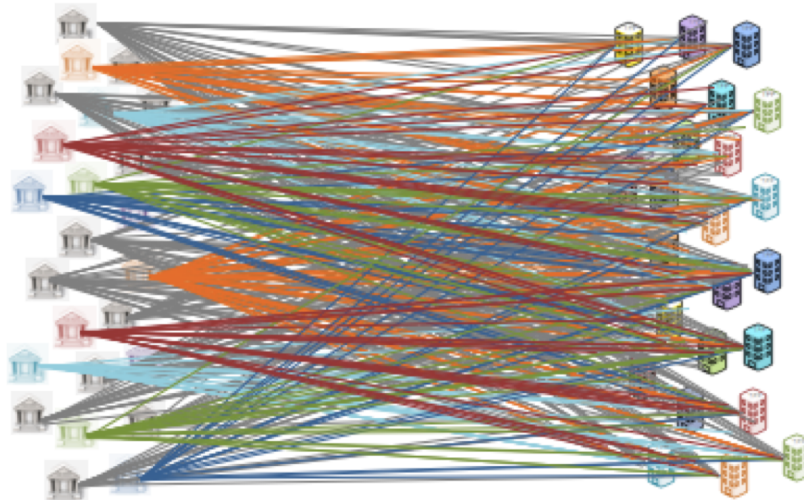
Uniform standard will help

Banks

Uniform and interoperable communications between banks and TPPs

THE *Berlin* GROUP
A EUROPEAN STANDARDS INITIATIVE

API*

TPPs

Rationale - Benefits

- Provides for detailed technical implementation standards that the market requires
- Fits with approach of the Euro Retail Payments Board

EUROPEAN CENTRAL BANK
EUROSYSTEM

ERPB Secretariat   ECB-UNRESTRICTED

11 November 2016
ERPB/2016/018

Provision of payment initiation services at pan-European level

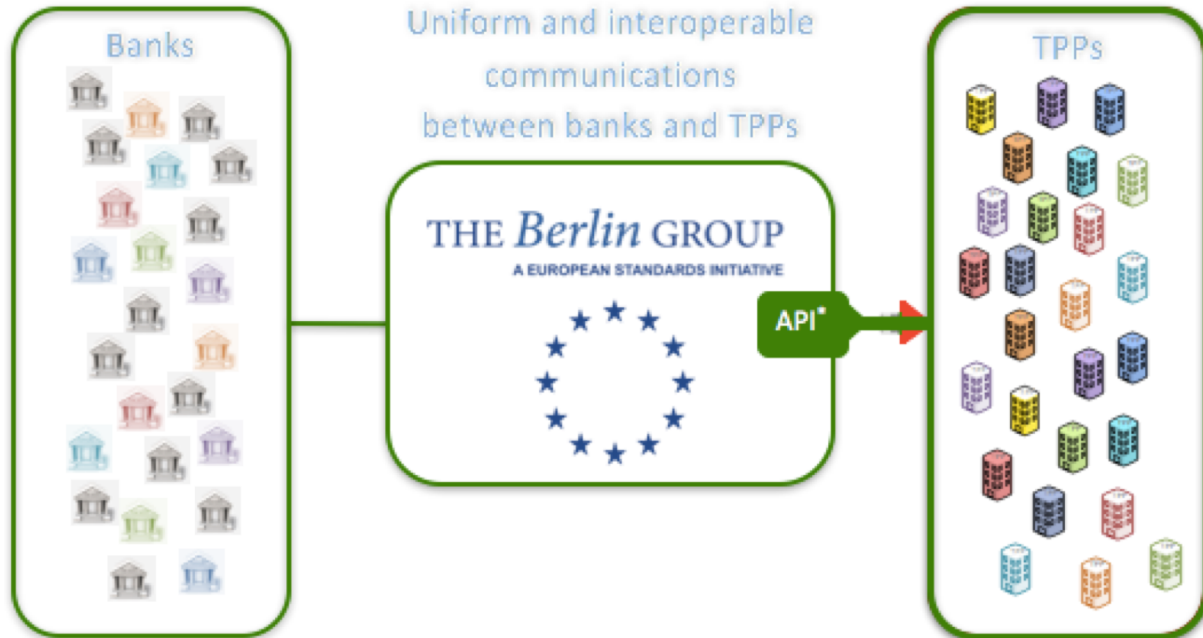"Following the draft EBA RTS, there is a need to develop a *standardised interface*[2] that account-servicing payment service providers (ASPSPs) will offer to PIS-providers (PISPs) for identification, authentication of the user, and secure communication."

[1] There are close links between PIS and account information services (AIS) and the confirmation on the availability of funds for issuers of card-based payment instruments. Any further work on PIS will need to consider the benefits it may have also on the provision of these other services.

Approach

> Open access for banks (ASPSPs), banking associations, payment associations and interbank processors/ACHs

> Deliver open, common, royalty-free standards for processes, data, interfaces and infrastructures

> Governance of interoperability standards separated from market implementation

> Where possible, leverage existing interoperability standards and achieved SEPA harmonisation

Approach

> Pragmatic approach with focus on Must Have and Should Have business and functional requirements

> Fostering dialogue amongst financial industry players at a pan-European level

> Open for cooperation or liaison with other relevant Open Banking initiatives

> Structured early consultation anticipated with demand-side

Approach

For building a standardised connectivity between banks and TPPs:

- **3 levels for the communication are being standardised**
- **An organisational framework is being defined**

Approach

organisational framework

- application level (banking)
- security level
- transport level

- Account service definitions
- Data Modelling

- Strong customer authentication of the bank customer
- Identification of TPP according to article 20 of EBA RTS

- Message exchange
- General composition of messages
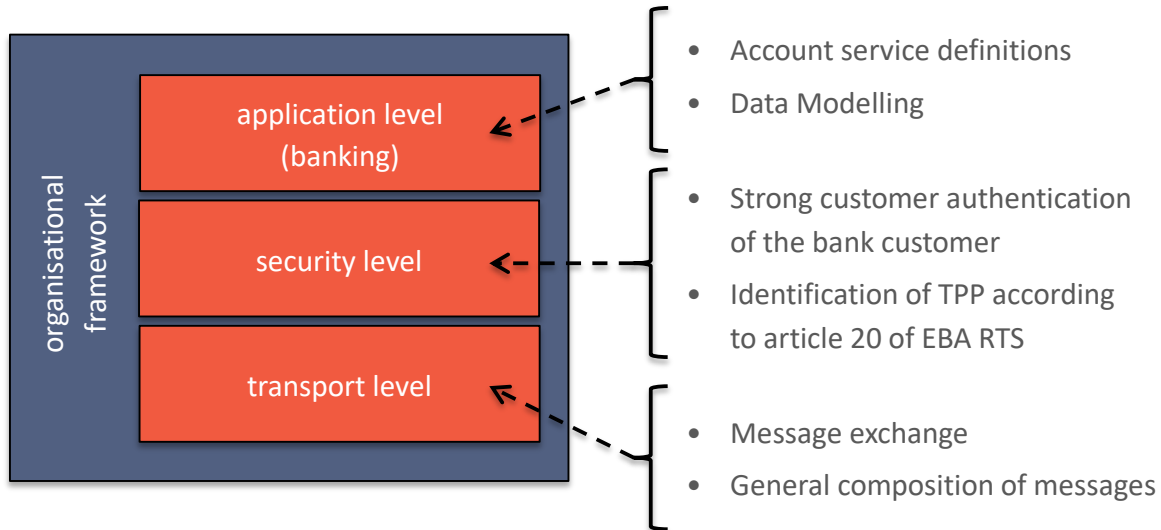
Why Berlin Group standards?

> **Comprehensive**
> covering the roles of Payment Initiation, Account Information and Confirmation Funds

> **Flexible**
> covering a diverse range of strong customer authentication means

> **Efficient**
> re-using existing banking standards as e.g. ISO 20022

> **Modern**
> based on newest technologies as RESTFul, JSON etc.

Why Berlin Group standards?

> **Secure**
> using identification standards as eIDAS

> **Simple**
> clear layered model where each actor can choose the parts relevant to them

> **Pan-European**
> actors from all over Europe and have contributed to the framework

> **Open**
> it's publicly available for everyone

Core services

AISP

- Establish account information consent

- Get list of reachable accounts

- Get balances for a given list of accounts

- Get transaction information for a given account

PIISP

Get confirmation on the availability of funds

PISP

- Initiation of a single payment

- Status query

Technical characteristics

Transport Protocol

- HTTP version 1.1
- TLS version 1.2 for communication between TPP and ASPSP

Application Protocol

REST

Authorization Protocol

OAUTH2 (optional)

Character set

UTF-8

Data structure

JSON & XML

Data model origin

ISO20022

Identifier naming convention

ISO20022 extended names

Security features

TPP authentication by the ASPSP

- Based on TLS

- Electronic signature at application level (at ASPSP discretion)

ASPSP authentication by the TPP

Based on TLS

PSU

Delegated by the TPP to the ASPSP

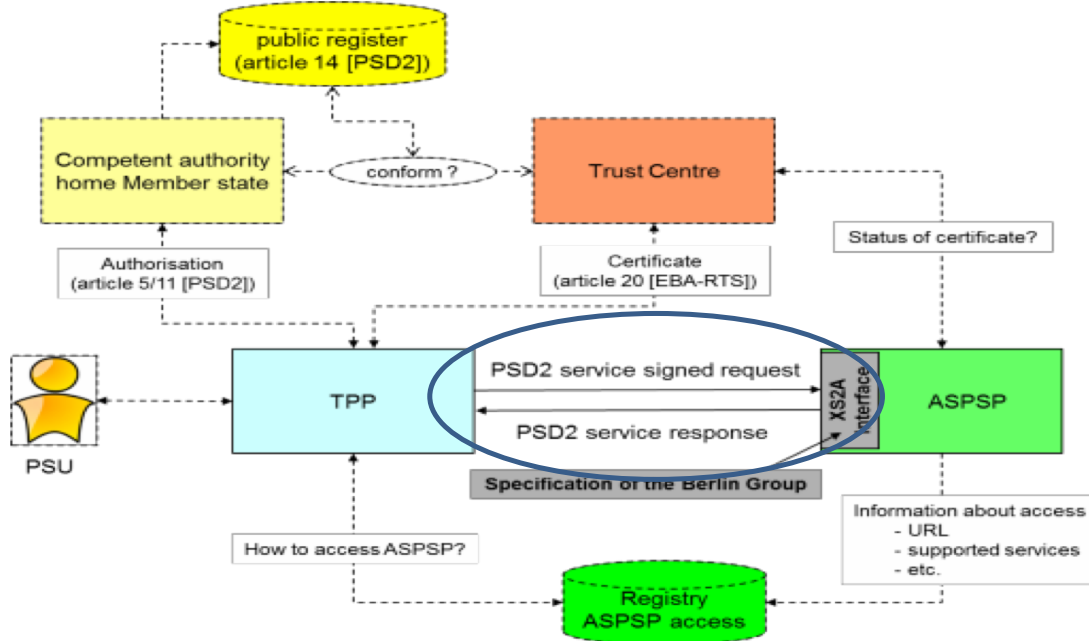**Data encryption**

Based on TLS

Proof management

Optional

Fraud detection support

Based on PSU related Data

Scope of XS2A framework

XS2A interoperability framework documents

> Operational rules

> Implementation guide

> Market consultations ongoing until November 17
https://www.berlin-group.org/market-consultations

Operational Rules

> An overview of the PSD2 compliant XS2A interface

> Rules to be observed by a TPP when using an interface

> Rules to be observed by an ASPSP when providing an interface

API technical specifications
are detailed in
Implementation Guidelines

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

Messages-transactions-sessions

Message

- A basic building block at the XS2A interface

- Request and response messages

Transaction

- A set of all messages to execute one of the business transactions (see use cases)

- It is not possible to mix different services in one transaction

Session

- A set of transactions executed consecutively at the XS2A interface

- Sessions can be used by an ASPSP for example to decide if strong customer authentication of the PSU is necessary as part of a transaction within the session.

- Transactions belonging to different services may be mixed within a single session

- The support of sessions at the XS2A interface is optional for an ASPSP

Messages-transactions-sessions: example
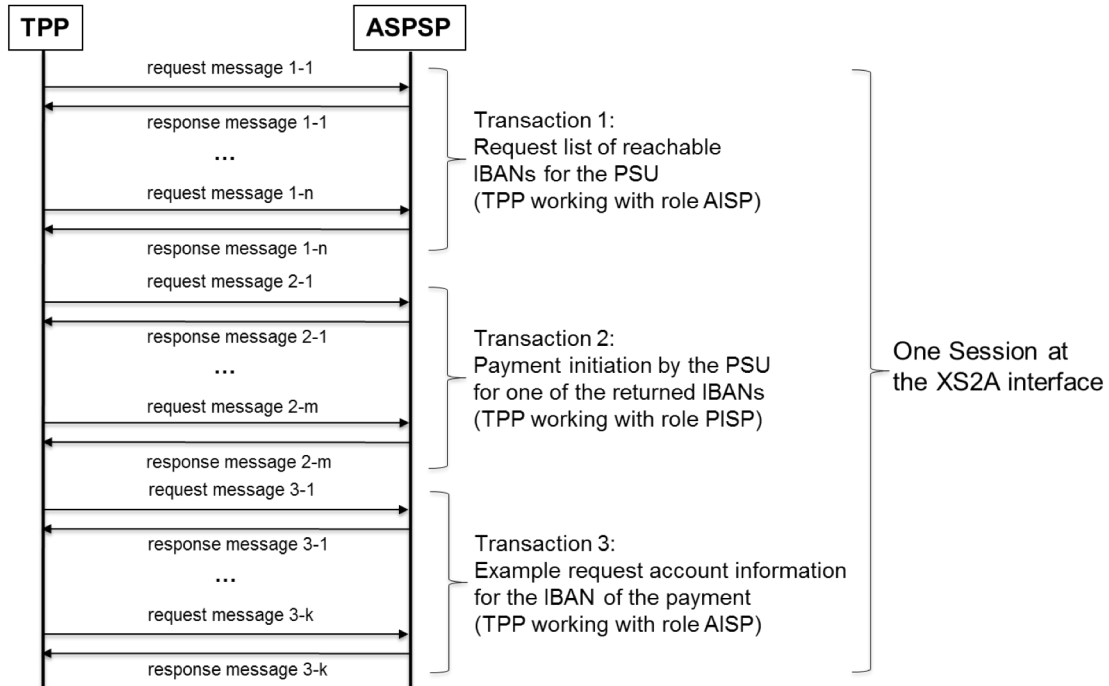
Payment initiation and Account information consent transactions require SCA. 3 SCA approaches are supported by standard

> **3 SCA approaches are supported by standard**

- Embedded: SCA is completely executed as part of PIS/AIS transaction in the XS2A

- Redirect: PSU is redirected to web interface of ASPSP. SCA is executed using this web interface or authentication app of ASPSP without involvement of XS2A i/f.

- Decoupled: SCA is executed completely decoupled from PIS/AIS transaction

> **Decided by ASPSP, which approaches are supported by its API**
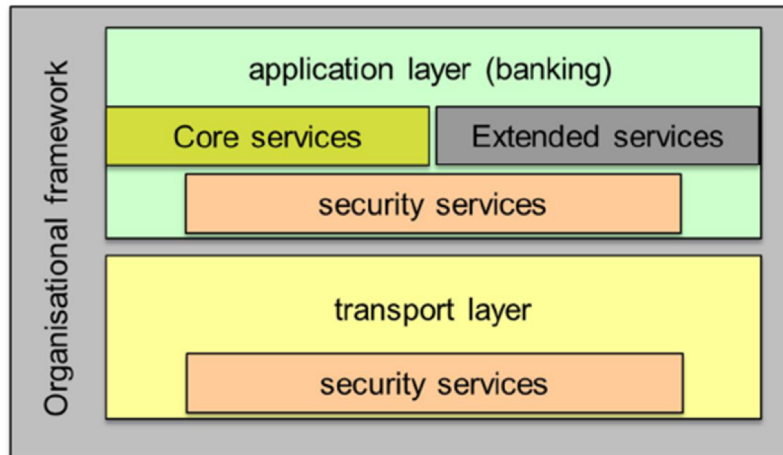
Implementation guidelines

Details the standard in defining messages and detailed data structures for the XS2A Interface
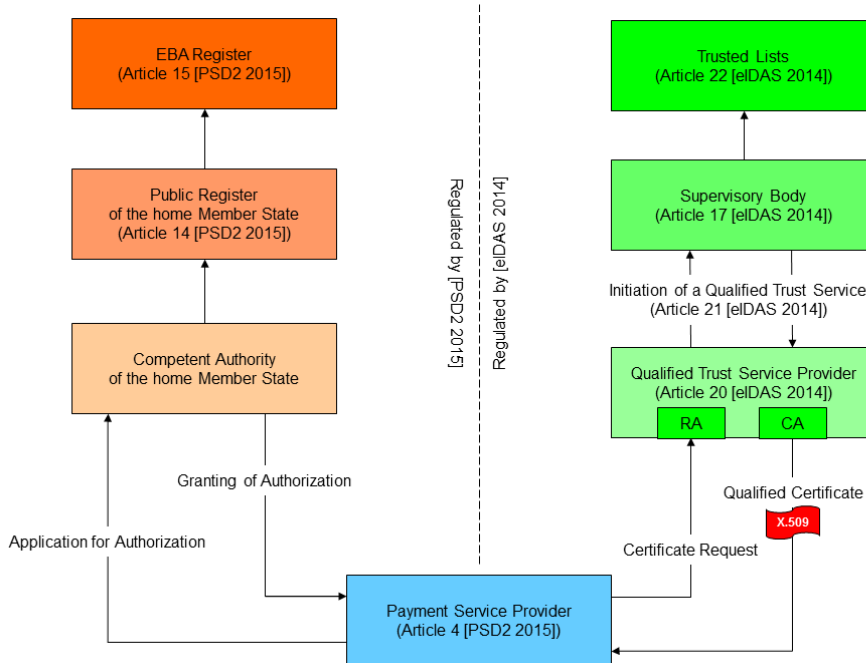
> Two layers are distinguished: application and transport

> At the application layer only the core services will be specified in the first version

Identification of TPP
(not part of Berlin Group)

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

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

Excursion: eIDAS compliant qualified certificates

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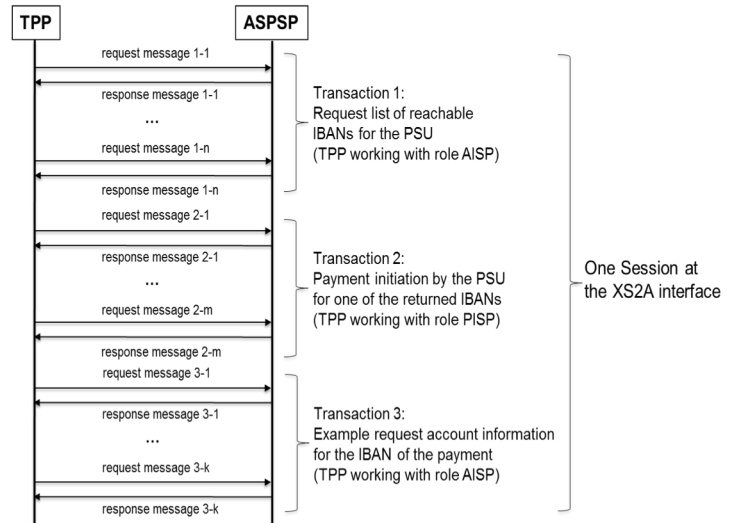
Session at the XS2A interface
- Set of transactions executed consecutively at the XS2A API

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

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
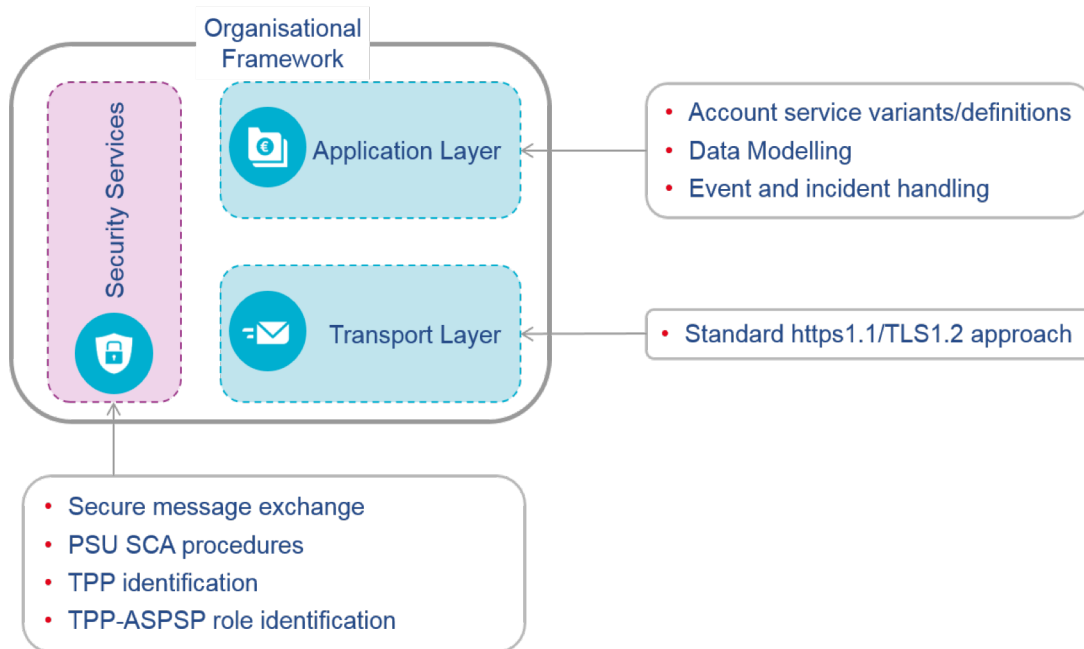
Key concepts: Identification of a TPP at the XS2A interface

> 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
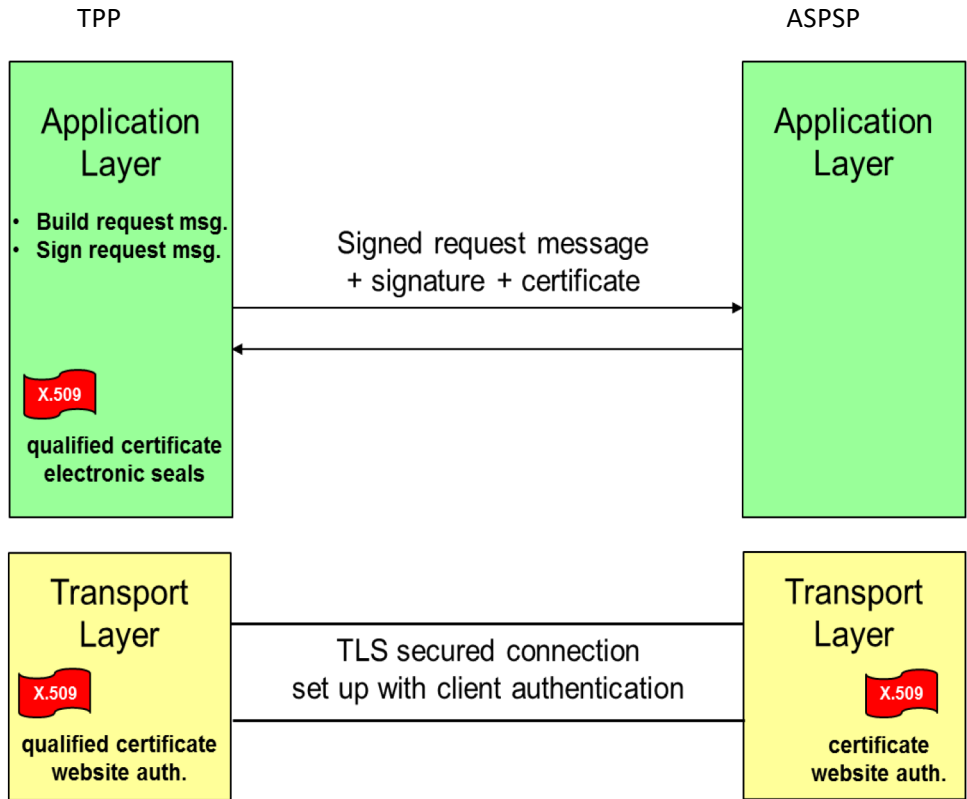
Key concepts: Strong customer authentication (SCA)

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

Key concepts: Strong customer authentication (SCA)

Different approaches for implementing SCA

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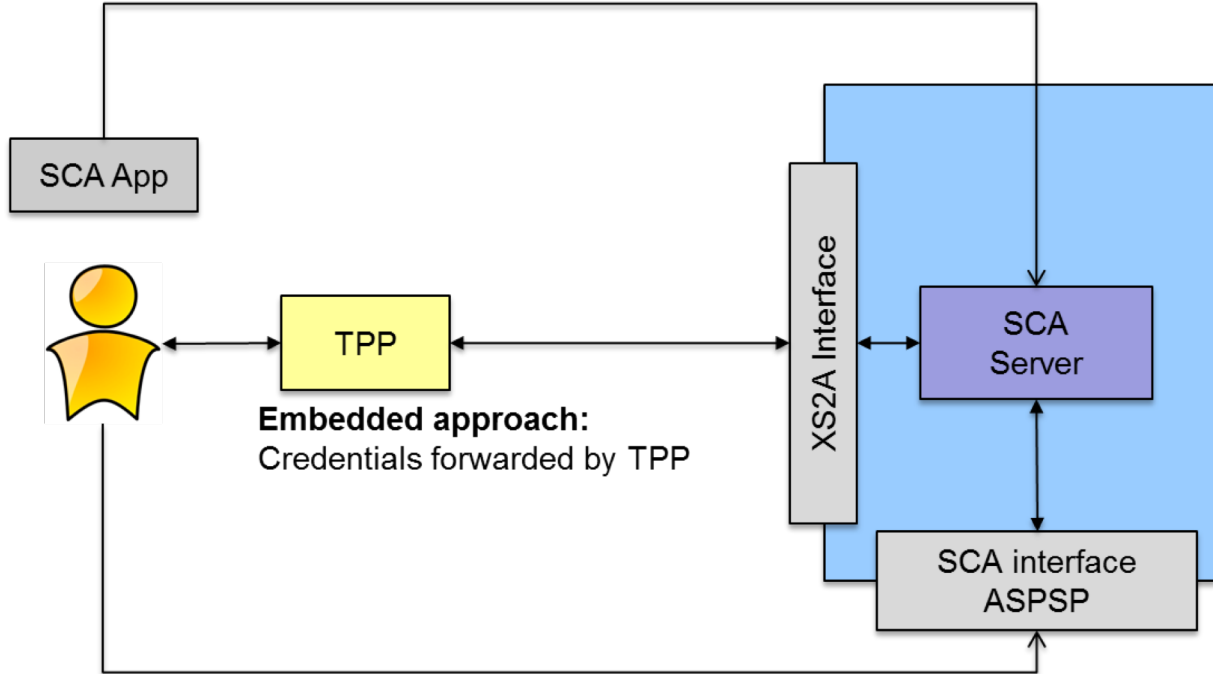> - PSU is redirected to web interface provided by the ASPSP

> **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

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
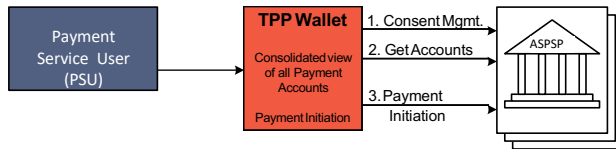
Use Case

- 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

Use cases – Wallet vs. Payment Initiation only

## Payment Initiation Service (Online Shop)
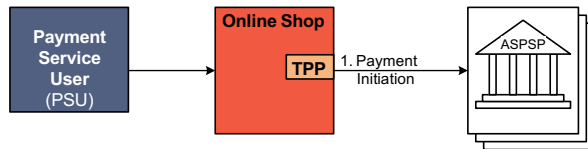
Use Case

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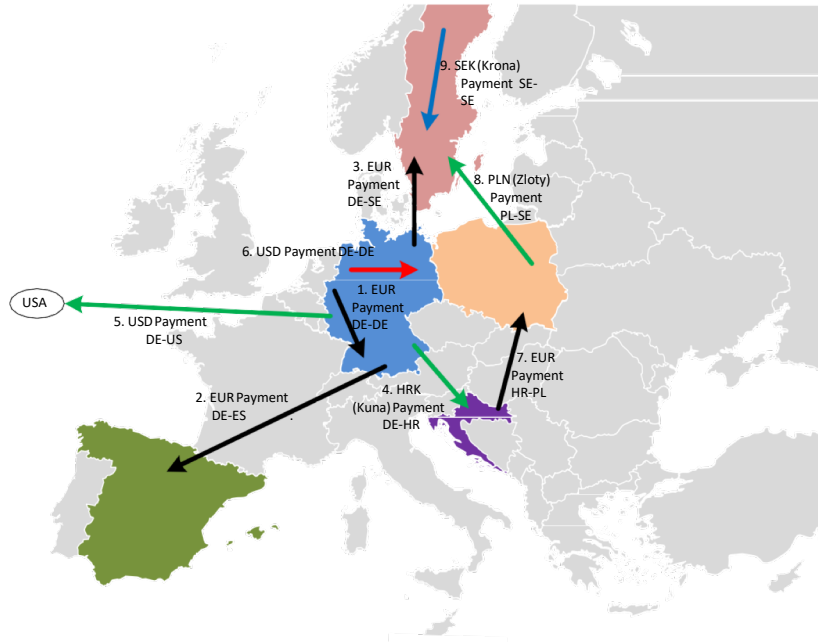
EUR Payments (SCT & SCT^inst)
- The SEPA Credit transfer is availbale in all european countries (incl. Instant payments)
- Format: pain.001.001.03 (Germany)
- Examples: 1. 2. 3. 7.

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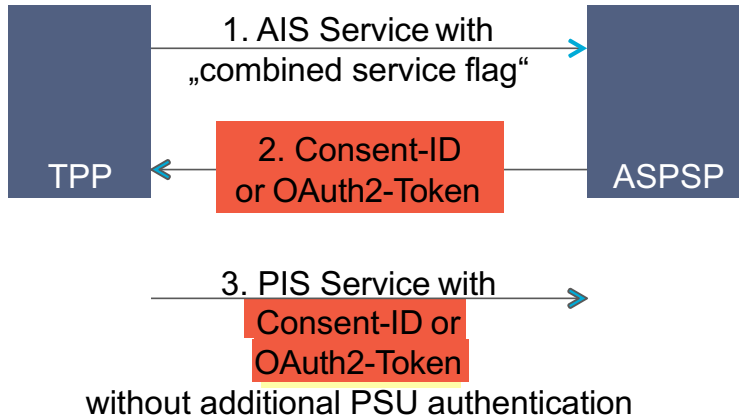- Format: tbc. (pain.001 based or legacy format)
- Example: 9.

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.

Map labels:
- 9. SEK (Krona) Payment SE-SE
- 3. EUR Payment DE-SE
- 8. PLN (Zloty) Payment PL-SE
- 6. USD Payment DE-DE
- USA
- 1. EUR Payment DE-DE
- 5. USD Payment DE-US
- 7. EUR Payment HR-PL
- 2. EUR Payment DE-ES
- 4. HRK (Kuna) Payment DE-HR

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

TPP — 1. AIS Service with „combined service flag" → ASPSP

TPP ← 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.

- 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.

High Level Overview: Bank Systems for Online Banking and API

Account Information Service

Association
of Latvian
Commercial Banks
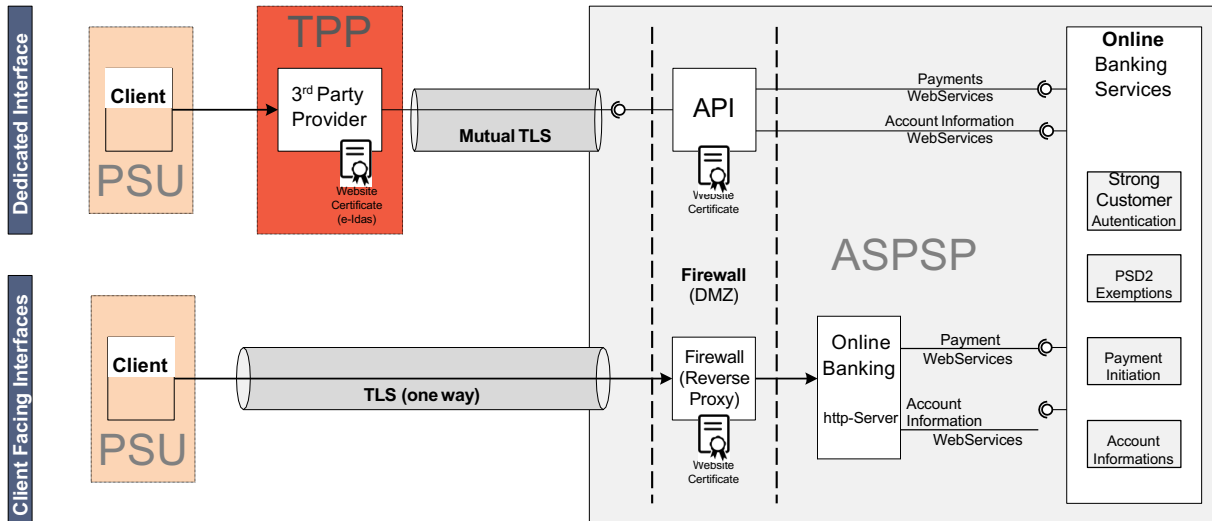
Establishing account information consent and presenting account information data to the PSU consist of five steps

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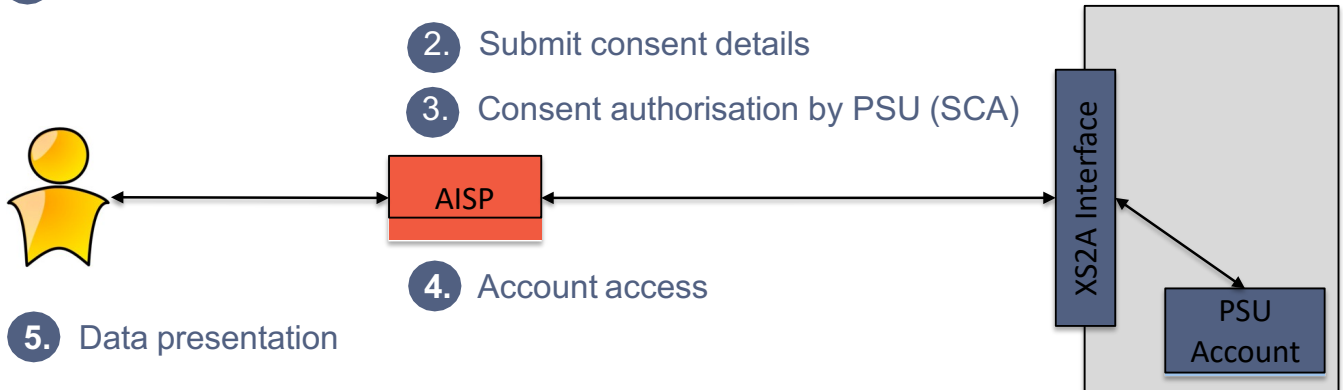2. Submit consent details
3. Consent authorisation by PSU (SCA)

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

Next Steps Berlin Group NextGenPSD2

Public Market Consultation and Finalisation Version 1.00

- Aim: Publish NextGenPSD2 Framework standards before end of January 2018

Organise Implementation & Market Involvement

- A set of all messages to execute one of the business transactions (see use cases)

- It is not possible to mix different services in one transaction

Next Steps Berlin Group NextGenPSD2

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

Thank you!

Association of Latvian Commercial Banks

Doma sq 8A, Riga, LV-1050, Latvia

Phone: +371 67284528

www.lka.org.lv

Sanda Liepiņa

Chairman of the Executive Board

sanda.liepina@lka.org.lv