## Key Standards

<table>
<thead>
<tr>
<th>THEME</th>
<th>STANDARD</th>
<th>COMMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Access Network</strong></td>
<td>Internet</td>
<td></td>
</tr>
<tr>
<td><strong>Transport Protocol</strong></td>
<td>HTTP 1.1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TLS 1.2</td>
<td>Provides data encryption during transportation</td>
</tr>
<tr>
<td></td>
<td>TLS 1.2</td>
<td>Provides cross-authentication of the actors</td>
</tr>
<tr>
<td></td>
<td>TLS 1.2</td>
<td>May be enforced by STS and/or TFS</td>
</tr>
<tr>
<td><strong>Authorisation Protocol</strong></td>
<td>OAUTH2</td>
<td>Authorisation Code Grant (AISP + PIISP)</td>
</tr>
<tr>
<td></td>
<td>MTLS</td>
<td>Client Credentials (PISP)</td>
</tr>
<tr>
<td><strong>Applicative Protocol</strong></td>
<td>REST</td>
<td>Richardson Maturity Model on level three</td>
</tr>
<tr>
<td><strong>Data Format</strong></td>
<td>JSON/UTF8</td>
<td>Transposition of ISO20022 structures</td>
</tr>
<tr>
<td><strong>Technical Documentation</strong></td>
<td>SWAGGER 2.0 (AOS2)</td>
<td>AOS3 format also available</td>
</tr>
</tbody>
</table>
PSD2 Actors

Account Information Services Provider
Payment Initiation Services Provider
Payment Instrument Issuer Service Provider

Payment Requester
Payment Service User
Payment Account Owner

Third Party Provider

Account Servicing Payment Service Provider

API actor

Registration Authority

©STET – Any use or copy without STET authorisation are prohibited
PSD2 Actors: The Payment Service User

The Payment Service User: A natural or legal person making use of a payment service in the capacity of payer, payee, or both.
PSD2 Actors: The PSD2 API actors

The Payment Service Provider:
- Credit Institutions
- Electronic Money Institutions
- Post Office Giro Institutions
- Payment Institutions
- ECB and National Central Banks
- Member States or Regional/Local Authorities
PSD2 Actors: Account Servicing Payment Service Providers

Payment Service Providers:
- Credit Institutions
- Post Office Giro Institutions

PSD2 API services providers
Account Information Services Providers (AISP) allow the Payment Account Owner to get information about all of his/her payment accounts:
- through a single interface,
- whatever the bank holding those accounts.

PSD2 API services clients
PSD2 Actors: Payment Instrument Issuer Service Providers

Payment Instrument Issuer Service Providers (PIISP) check the coverage of a given payment amount by the available funds on a given PSU’s account.

PSD2 API services clients
PSD2 Actors: Payment Initiation Service Providers

Payment Initiation Service Providers (PISP) request a Payment Request execution through a Credit Transfer (PISP role).

PSD2 API services clients
PSD2 Actors vs W3C Model

- Payment Service User
- Payment Requester
- Payment Account Owner
- Payment Account Service Provider
- Payment Service Provider
- Payment Instrument Issuer Service Provider
- Account Servicing Payment Service Provider
- Payment Handler Providers
- Browser (Desktop/Mobile)
- Payment Handler
- User
- Payment Requester
- Third Party Provider
- Payment Account Owner
- API actor
- Registration Authority
- Merchant
- User
AISP Use Cases

AISP

Gets the PSU context

<<includes>>

Gets account data

Gets account balances

Gets account transactions

Gets account transaction history

Gets account transaction forecast

Gets trusted beneficiaries

Send PSU consent

©STET – Any use or copy without STET authorisation are prohibited
PIISP Use Case

PIISP

Checks funds coverage
PISP Purchase Use Cases

Merchant (Payment Requester)

Asks for a transfer

Sends a payment request

PISP

Confirms the request

Orders Party (Payment Account Owner)

Asks for a cancellation

Sends a cancellation request

Sends a payment request

Initiates the Credit Transfer

PSU’s Bank (ASPSP)

Asks for PSU authentication

Forwards the payment request status

Get the payment request status

Cancels a scheduled transfer

©STET – Any use or copy without STET authorisation are prohibited
PISP Transfer Use Cases

Ordering Party (PSU) ➔ PISP ➔ PSU’s Bank (ASPSP)

- Asks for a transfer
- Sends a transfer request
- Initiates the Credit Transfer
- Get the transfer status
- Confirms the transfer request
- Asks for SCA

<<Extends>>
<<Extends>>
<<Extends>>
<<Extends>>
PISP Purchase Use Case

1) Purchase

2) Payment Initiation Request

3) Customer’s Authentication

4) Payment Initiation Report

5) Credit Transfer

E-commerce marketplace

Payment Initiation Service Provider

Customer’s Bank

Merchant’s Bank

Online Customer
PISP Purchase Use Case in a W3C approach (initial setup)

- Payee's Bank (ASPSP)
- Payee (Payment Requester)
- Payment Handler Provider (PISP or other actor)
- Payment Handler
- User Agent
- Consumer/Payer (PSU)
- Payer's Bank (ASPSP)

1. Suggest Payment Handler Installation
2. Accept
3. Download Payment Handler
4. Initiate Payment Handler Installation
5. Payment Handler Installs
6. Suggest Payment Handler Setup
PSD2 decoupled from Payment Request API

Payee's Bank (ASPSP) → Payee (Payment Requester) → Payment Initiation Service Provider (PISP) → Payment Handler → User Agent → Consumer/Payer (PSU) → Payer's Bank (ASPSP)

- **Provide Checkout Page**
- **Click Buy Button**
- **Call Payment Request API (List of acceptable payment handlers)**
- **Compute the list of usable payment handlers**
- **Ask for payment handler choice**
- **Select payment handler**
- **Call payment handler API**
- **Present user experience**
- **Choose payment method**
- **Send payment data**
- **Returns to the payment handler**
- **Payment handler API returns**
- **Payment Request Request returns**
- **Send the payment request to the Bank (PSD2 API)**
- **Process initial checks**
- **Ask for consumer authentication**
- **Authenticate**
- **Forward the payment report (PSD2 API)**
- **Notify**
- **Send the Credit Transfer**
- **Notify the Credit**

©STET – Any use or copy without STET authorisation are prohibited
**PSD2 During Payment Request API**

1. **Payee's Bank (ASPSP)**
2. **Payee (Payment Requester)**
3. **Payment Initiation Service Provider (PISP)**
4. **Payment Handler**
5. **User Agent**
6. **Consumer/Payer (PSU)**
7. **Payer's Bank (ASPSP)**

- **Provide Checkout Page**
- **Click Buy Button**
- **Call Payment Request API (List of acceptable payment handlers)**
- **Compute the list of usable payment handlers**
- **Ask for payment handler choice**
- **Select payment handler**
- **Call payment handler API**
- **Present user experience**
- **Choose payment method**
- **Send payment data**
- **Send the payment request to the Bank (PSD2 API)**
- **Process initial checks**
- **Ask for consumer authentication**
- **Display authentication request to the User**
- **Authenticate**
- **Forward the payment report (PSD2 API)**
- **Notify**
- **Returns to the payment handler**
- **Payment handler API returns**
- **Payment Request API returns**
- **Send the Credit Transfer**
- **Notify the Credit**
PSD2 API and ISO20022

- STET already experienced ISO20022 through
  - SEPA payments implementation (from 2008)
  - Account Management messages (2009)
  - SEPAmail messages (2011)
- So using ISO20022 was a strategic choice. It was also a recommendation from the RTS on SCA.
  - V1.0, V1.1 and V1.2 used
    - ISO20022 data structures for AIS and PIISP
    - a whole copy/paste of some messages for PIS
- ISO20022 Modelling of STET API work started in Fall 2017
  - Reflexions about API resources and automatic documentation
  - V1.3 and V1.4 provide a smarter use of ISO20022 building blocks
  - Berlin Group joined in June 2018
- ISO TC68/SC9/WG2 started to work on general usage of ISO20022 in Spring 2018
Identification and Authentication (1/4)

- Using a National Id (e.g. Social Security Number)
  - National Directory
  - Government
  - National Authentication Server

- Using a National Scheme
  - Trust Domain
    - Access Right Management
    - Consent Management
    - Data access authorisation
  - May Rely on
  - May Rely on

- Using the Organisation Scheme
  - Organisation Authentication Server
  - Organisation
  - Organisation Directory

- Using an Organisation Specific Id (e.g. client Id, account Id...)
  - May Rely on
  - May Rely on

Person

Identification

Authentication (Simple or Strong)
Identification and Authentication (2/4)

ASPSP DOMAIN

- Using a National Id (e.g. Social Security Number)
- Using a National Scheme
- Using the Organisation Scheme
  - Using a Organisation Specific Id (e.g. client Id, account Id...)
  - Trust Domain
    - Access Right Management
    - Consent Management
    - Data access authorisation

Person

REDIRECT APPROACH

Government

National Directory

National Authentication Server

Organisation Authentication Server

Organisation

Organisation Directory
Identification and Authentication (3/4)

**TPP DOMAIN**
- Using a National Id (e.g. Social Security Number)
- Identification
- Authentication (Simple or Strong)
- Using the Organisation Scheme
- Using a Organisation Specific Id (e.g. client Id, account Id...)

**ASPSP DOMAIN**
- National Directory
- Government
- National Authentication Server
- Organisation Authentication Server
- Organisation
- May Rely on

**DECOUPLED APPROACH**
Identification and Authentication (4/4)

**TPP DOMAIN**
- Using a National Id (e.g. Social Security Number)
- Using a Organisation Specific Id (e.g. client Id, account Id...)

**ASPSP DOMAIN**
- Using a National Scheme
- Trust Domain - Access Right Management
- Consent Management
- Data access authorisation

**EMBEDDED APPROACH**

Person

©STET – Any use or copy without STET authorisation are prohibited
THANK YOU!