PRETA and PSD2

Access to Accounts (XS2A)
(4) The review of the Union legal framework on payment services and, in particular, the analysis of the impact of Directive 2007/64/EC and the consultation on the Commission Green Paper of 11 January 2012, entitled, ‘Towards an integrated European market for card, internet and mobile payments’, have shown that developments have given rise to significant challenges from a regulatory perspective. Significant areas of the payments market, in particular card, internet and mobile payments, remain fragmented along national borders. Many innovative payment products or services do not fall, entirely or in large part, within the scope of Directive 2007/64/EC. Furthermore, the scope of Directive 2007/64/EC and, in particular, the elements excluded from its scope, such as certain payment-related activities, has proved in some cases to be too ambiguous, too general or simply outdated, taking into account market developments. This has resulted in legal uncertainty, potential security risks in the payment chain and a lack of consumer protection in certain areas. It has proven difficult for payment service providers to launch innovative, safe and easy-to-use digital payment services and to provide consumers and retailers with effective, convenient and secure payment methods in the Union. In that context, there is a large positive potential which needs to be more consistently explored.
PSD2 State of play

- PSD2 was published in EU's OJ on 23 December 2015;
- PSD2 comes into force 2 years later, i.e. 13 January 2018
- Subject to:
  - Transposition (i.e. implementation by individual Member States)
  - Member State derogations
  - Transitional provisions
  - EBA mandates –
    Guidelines,
    RTS (regulatory technical standards) and
    ITS (implementing technical standards)
# AS PSPs and TPPs

<table>
<thead>
<tr>
<th>Account Servicing PSPs</th>
<th>AS-PSPs</th>
</tr>
</thead>
<tbody>
<tr>
<td>AS-PSPs are Credit Institutions and Payment Institutions with Payment Accounts.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Payment Initiation Service Providers</th>
<th>PI-SPs</th>
<th>Account Information Service Providers</th>
<th>AI-SPs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collectively known as “Third Party Providers” or TPPs</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TPPs must be a Credit institutions or Payment Institutions with the appropriate license.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Institutions can play both roles, i.e. a bank, payment institution or other FinTech can be both an AS-PSP and a TPP.
## Actors and responsibilities

<table>
<thead>
<tr>
<th>Payment Initiation Services</th>
<th>Account Information Services</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Payers</strong></td>
<td><strong>Payment Service Users</strong></td>
</tr>
<tr>
<td>Consumers, Businesses or other Account Holders who want to pay using PIS, a right given under PSD2.</td>
<td>Consumers, Businesses or other Account Holders who want to use AIS, a right given under PSD2.</td>
</tr>
<tr>
<td><strong>AS PSPs</strong></td>
<td><strong>AS PSPs</strong></td>
</tr>
<tr>
<td>Must allow PIS.</td>
<td>Must allow AIS.</td>
</tr>
<tr>
<td><strong>Payment Initiation SPs</strong></td>
<td><strong>Account Information SPs</strong></td>
</tr>
<tr>
<td>Must act only with the consent of the Payer.</td>
<td>Must act only with the consent of the Account holder.</td>
</tr>
<tr>
<td><strong>Payees</strong></td>
<td></td>
</tr>
<tr>
<td>Merchants, Public Authorities, small Businesses, Consumers who want to be paid.</td>
<td></td>
</tr>
</tbody>
</table>
Article 66: The Payment Initiation flow

The PI-SP Shall: “every time a payment is initiated, identify itself towards the AS-PSP of the payer and communicate with the AS-PSP, the payer and the payee in a secure way, in accordance with point (d) of Article 98(1).”

The AS-PSP Shall: (a) communicate securely with payment initiation service providers in accordance with point (d) of Article 98(1) & (b) immediately after receipt of the payment order from a PI-SP, provide all information on the initiation of the payment transaction and all information accessible to the account servicing payment service provider regarding the execution of the payment transaction to the PI-SP; (2) When the payer gives its explicit consent for a payment to be executed in accordance with Article 64.

Described by many as an API.

The Customer Authentication model hotly debated.
Article 67: The Account Information Service flow

The AI SP shall (2a) where based on the payment service user’s explicit consent, (2c) for each communication session, identify itself towards the account servicing payment service provider(s) of the payment service user and securely communicate with the account servicing payment service provider(s) and the payment service user, in accordance with point (d) of Article 98(1);

In relation to payment accounts, the AS PSP shall: (3a) communicate securely with the account information service providers in accordance with point (d) of Article 98(1); and (3b) treat data requests transmitted through the services of an account information service provider without any discrimination for other than objective reasons.

Described by many as an API.

The Customer Authentication model hotly debated.
Open Issues include (but are not limited to)

Definitions of Payment Account
How the Customer authentication security model works
Definitions of Sensitive Data
Issues over liability for unauthorised transactions.
The responsibility of the AS-PSP to protect their customer, but at the same time to grant them a simple, non discriminatory access.
How it all works in practice.

*While these areas of uncertainty exist, this does not stop the implementation work progressing.*
Access to the Account (XS2A) compliance

A bad outcome?

A good outcome?

Possible areas of collaboration

<table>
<thead>
<tr>
<th>A Directory</th>
<th>Data Set</th>
</tr>
</thead>
<tbody>
<tr>
<td>Governance</td>
<td>Messaging layer</td>
</tr>
<tr>
<td>Central Information</td>
<td>Administrative framework</td>
</tr>
</tbody>
</table>

Stakeholders

PSPs
- AS PSPs
- AI SPs / PI SP
- Associations

Service Providers
- API Developers
- Integrators
- OBEP Schemes

End Users
- Consumer
- Merchants
- Public Authorities

Regulators
- ECB / EC / EBA
- ERPB / EPC

Questions

- Do you recognise a problem that PSD2 XS2A presents around security and possible fragmentation?
- Do you see that a collaborative approach could be useful, in this case?
- If what we believe about the RTS are true, and if EBA CLEARING/ PRETA investigate a solution that will provide security and compliance, would you be interested in this?

Roadmap

2016
Build consensus

2017
Develop

2018
Go live

© PRETA All rights reserved.

Preta S.A.S is a wholly owned subsidiary of EBA CLEARING
Context of regulated and non-regulated Access Services

There is much discussion about Open Banking, Open Data, and APIs.

Some of this is being pushed by regulators, e.g. PSD2 and so creating compliance requirements.

Some is being done voluntarily – often through an API program – in order for Account Servicing PSPs to find new ways to offer services to their customers.

PSPs must comply with new legislation, while keeping an eye to new developments.
PRETA will continue to offer solutions such as **MyBank** - based on strong market needs - that deliver value to all parties in the ecosystem.

PRETA will examine how to offer tools to help all banks to meet their compliance obligations. This may include:

2. Interfaces, participant registries, helpdesk facilities, dispute resolution tools.

3. Links to existing interfaces to avoid fragmentation.

“PSD2 X2SA API Service” (XS2API)

Unbranded
How PRETA might fit into the industry landscape

Who they are

- Regulators
- EPC / ERPB
- ISO / W3C
- National and EU Organisers
- Processors & Gateways
- PSPs (AS-PSP, PI-SPs, AI-SPs) & PSUs

What they provide

- PSD2 and RTS
- Schemes & Standards
- Deployment tools, management tools and operational administration
- Hardware / Software / Physical Infrastructure
- PSD2 Compliance
Operational Threat from PSD2

Access to the account puts technical obligations on banks

The “Regulatory Technical Standards” may be principles than specifications.

There is a fear that fragmentation will lead to money being wasted PSD2 fails to achieve the aims of harmonising services. There are fears over Security.
APIs may be Part of the Solution, but they are not THE Answer.
Possible Deliverables: Some or all might be applicable

<table>
<thead>
<tr>
<th>A Directory</th>
<th>Specifications for a data layer</th>
</tr>
</thead>
<tbody>
<tr>
<td>• A secure operational directory containing</td>
<td></td>
</tr>
<tr>
<td>• Details of AS-PSPs</td>
<td></td>
</tr>
<tr>
<td>• Details of PI and AI-SPs</td>
<td></td>
</tr>
<tr>
<td>• An onboarding process to ensure that the</td>
<td></td>
</tr>
<tr>
<td>Directory is populated properly.</td>
<td></td>
</tr>
<tr>
<td>• A helpdesk and support service</td>
<td></td>
</tr>
<tr>
<td>• To be seen to what extent RTS covers this.</td>
<td></td>
</tr>
<tr>
<td>• Operational XML schema’s that can be used by all parties.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Central Governance Functions</th>
<th>Specifications for a secure messaging layer</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Improvements / Evolution</td>
<td></td>
</tr>
<tr>
<td>• Release of security patches</td>
<td></td>
</tr>
<tr>
<td>• Dispute resolution and problem solving</td>
<td></td>
</tr>
<tr>
<td>• To be seen to what extent RTS covers this.</td>
<td></td>
</tr>
<tr>
<td>• A secure access method that delivers authentication, integrity, non-repudiation and confidentiality</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Central information functions</th>
<th>A contractual / administrative framework</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Statistics</td>
<td></td>
</tr>
<tr>
<td>• Incidents</td>
<td></td>
</tr>
<tr>
<td>• Helpdesk</td>
<td></td>
</tr>
<tr>
<td>If needed.</td>
<td></td>
</tr>
</tbody>
</table>
The value Proposition for PSPs

For AS-PSPs

An AS-PSP does not have to design its own Access method (API) but can take an RTS compliant solution developed by the industry.

The AS-PSP does not have to verify the credentials of X,000 TPPs. This is done once, centrally.

This solution will bring security and order.

The AS-PSP can (optionally) use the same technology to deliver additional value added services to its customers.

For PI-SPs and AI-SPs

A PI-SP does not have to try to interface to X,000 different AS-PSPs but can take an RTS compliant solution developed by the industry.

The PI-SP does not have to convince 4,000 AS-PSPs that it has a right to do business.

This solution will bring security and order.

The PI-SP can (optionally and with appropriate permission) use the same technology to deliver value added services to its customers.
EBA CLEARING, through PRETA, must create harmonisation:

1. Where no solution exists, directly offer XS2API.
2. Where existing individual solutions (e.g. API’s) exist, link them to a common solution.
3. Where existing Community Solutions exist, link them to a common solution.

Each FI has a single channel to be accessed from all of Europe.

Note: PRETA will probably not provide processing services. Left to service providers.
Timing and Actions

2016
XS2API: Build consensus

2017
XS2API: Develop.

2018
XS2API: Go live.

Building commitment
? 07/2016 Would you be interested?
? 10/2016 What do we need?
? 02/2017 Are you onboard?
X2API is a Solution to PSD2 Access to the Account (XS2A)

- A market driven solution providing direct but controlled access to account services:
- Country neutral: provides European reach
- Open: All regulated players can use the solution
- Low cost: reuses existing infrastructure and ISO20022 standards in API.
- Safe security model.
- Provides clarity via common rules without the need for individual contracts between all players.
- Compliance orientated.
- Overcoming fragmentation. Promoting efficiency.
Engagement Questions

While we recognise that we are missing many elements of the picture, for the time being:

• Do you recognise a problem that PSD2 XS2A presents around security and possible fragmentation?

• Do you see that a collaborative approach could be useful, in this case?

• If what we believe about the RTS are true, and if EBA CLEARING/PRETA investigate a solution that will provide security and compliance, would you be interested in this?
Thank you

www.pretaw.eu