Strong Customer Authentication and common and secure communication under PSD2

PSD2 in a nutshell

4

pwc

Summary

On August 12, the EBA has issued the long-awaited draft of the Regulatory Technical Standards (RTS) in the field Strong Customer Authentication (SCA) and open and secure communication standards, which continues addressing the technical issues underlying the PSD2 Directive, implementing the comments and feedbacks received so far from stakeholders in the context of the discussion paper published previously, but also proposing new questions on still open issues.

The most striking innovation introduced by the RTS draft, also in relation to market expectations that the Directive and the consultation paper created, is that in order not to constrain the future technological progress a centrally and shared single standard for the dialogue between the ASPSP, PISP and AISP will not be defined.

Issues to be addressed

Each ASPSP will make appropriate communication interfaces available that adopt the ISO 20022 standard (implicitly allowing the use of API!) and are exhaustively documented on its website, consequently PISP and AISP will have to customize their own applications for the interview with the specific ASPSP.

Additional clarifications are undertaken in relation to:

- the necessary requirements for the identification and security of the communication session between ASPSP, PISP and AISP, based on authentication certificates and encrypted messages;
- the safety requirements to be adopted (dynamic link, real-time fraud detection and prevention, etc.), with special focus for card-based payments and used to protect the confidentiality and integrity of customized security credentials;
- the identified exemptions for the adoption of the SCA;
- the need to align the service levels and the completeness of the information available for AIS services to those paid directly by ASPSP to its customers;
- the processing of sensitive customer data.

EU Member States will have to transpose the Directive by January 13th, 2018 and the full implementation of the components related RTS in analysis is not expected before the second half of 2018.

Focus on open standards and secure communication

The main innovations introduced in the draft, related to the discussion and definition of interfaces between ASPSP, PISP and AISP, can be summarized in the following points:

Talking Interfaces

In the management and definition of interfaces, for which EBA advocates the adoption of the ISO 20022 standard *(see BOX Data Model for the interoperability of systems),* the ASPSP must:

i. make available interfaces that enable the operations of identification, authentication and implementation of the activities for AISP, PISP and for card-based payment services;

ii. make available free comprehensive technical documentation on their websites, in order to allow the integration with TPP systems;

iii. make available infrastructures and support to allow the test end to end of the TPP applications;

iv. advertise any technical modification at least 3 months in advance to the production start.

In this regard, ASPSPs, through the responses to the discussion paper, seem to require a "governing entity" responsible for supervising the design, development and maintenance of an interface standard of communication

Service levels

Service levels and related support shall be warranted as the services directly provided by ASPSP to its customers.

Information Set

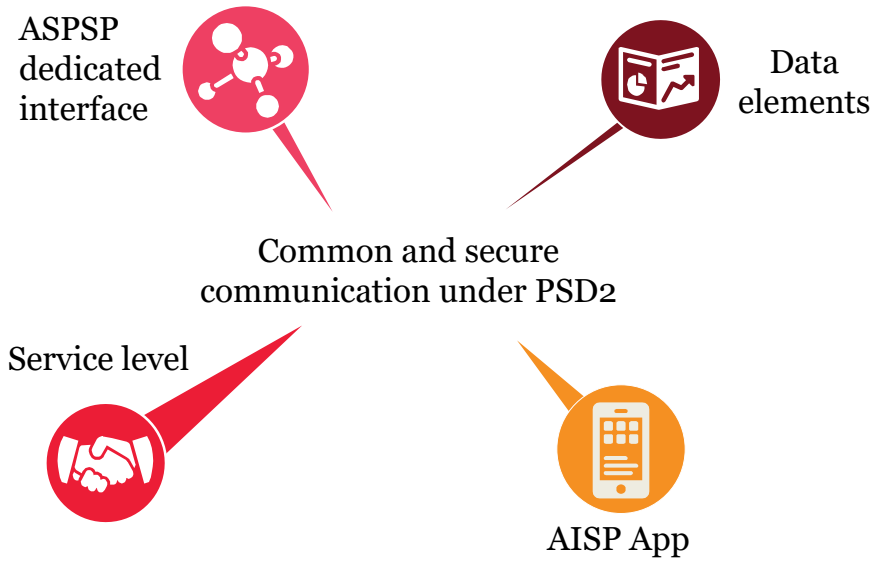
The interfaces for PISP and AISP should ensure the same information available to the services directly provided to the ASPSP customers, with the exception of sensitive payment data to be properly categorized and excluded from the disclosure requirement traded to the TPP.

AISP Applications

Applications must:

i. allow users to limit their queries according to the explicitly provided consensus;

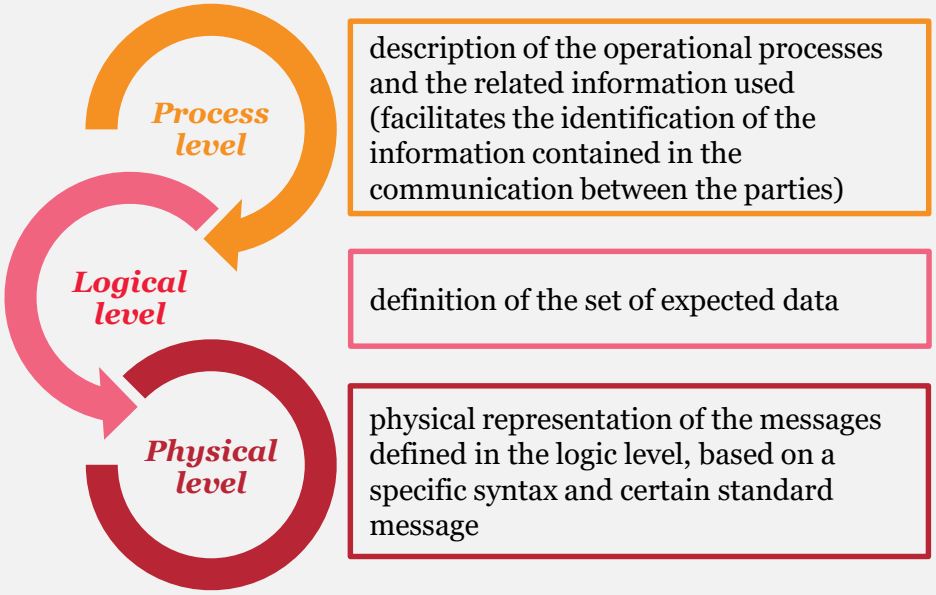
ii. limit information requests not directly placed by the users to a maximum of two per day *(see BOX repetitive authorization to data access).*



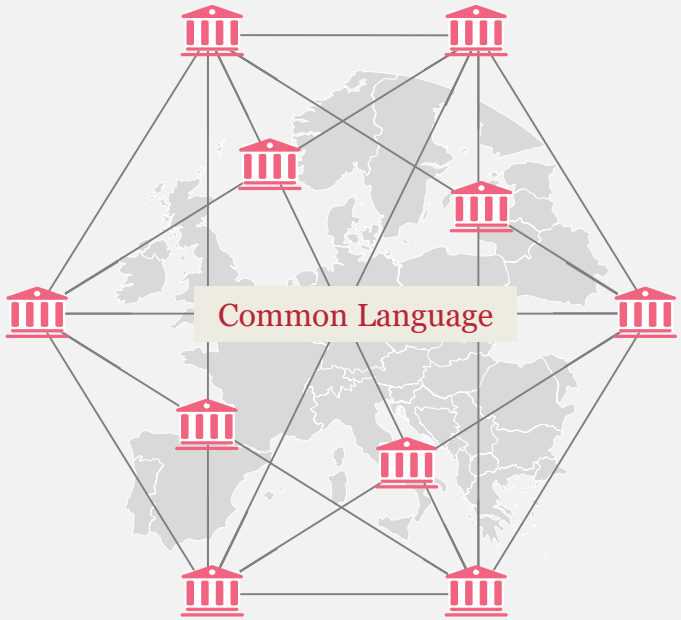
Model data for interoperability of the systems

EBA encourages, thought not indicating a precise standard to be used, the adoption of communication standards developed by European or International bodies and of ISO 20022 in particular, which contemplate the use of both XML (eXtensible Markup Language) and ASN.1 (Abstract Syntax Notation One) for the definition of data structures at a high level.

This scenario, similar to what was achieved for SEPA systems, leads to the adoption of structured data models for XS2A systems (Access To account) in the PSD2 perimeter structured in three different levels:



- description of the operational processes and the related information used (facilitates the identification of the information contained in the communication between the parties)
- definition of the set of expected data
- physical representation of the messages defined in the logic level, based on a specific syntax and certain standard message



ISO 20022 also contemplate the presence of a "dictionary" containing the semantic description of the objects provided by the data model. Currently, about 700 are defined as business components and more than 300 "message definitions", managed by “ISO 20022 Registration Authority (RA)”.

This type of patterns (as for example: MT103 and ISO15022 used in swift, ISO 8583 used for transactions with credit and debit cards, etc.), introducing the possibility to carry out comparisons and find similarities on business concepts described in defined data patterns (although differently structured), it allows mutual mapping with other standards used in the financial world.

Focus on safety requirements and exemptions

Below are the main points of attention highlighted in the draft, in relation to security issues:

The identification of TPP

EBA aims to strengthen security and confidence of consumers in relation to transactions using the Internet. Thus, it becomes necessary to promote the implementation of measures to identify the players involved (ASPSP, AISP and PISP) which must take place through the use of certificates and-IDAS. This would allow to generate a list of selected payment service providers. Underlying this idea is the creation of a Public Key Infrastructure (PKI) to allow the actors to interact with an adequate level of safety. Prerequisite for the provision to be applied would be the establishment of a certification authority and-IDAS. Given the stringent timing requires the consultation paper to stakeholders to propose alternative solutions.

Authorization of transactions and dynamic link

The protection of sensitive payment data and personal information of the users becomes paramount. The player will have to adopt technological solutions that guarantee confidentiality, authenticity and integrity of the data and are consistent with ISO 27001. However, in the face of this need, the data classified as sensitive has not been defined to date. It is anyway mandatory for the communicating parties to adopt cryptographic techniques widely recognized for data protection and solutions enabling the "dynamic link" of the transaction to a specific amount and beneficiary. It is also expected that ASPSPs implement mechanisms to prevent, detect and block fraudulent transactions before the payment authorization by the PISP. The practice is today widespread for card payments and the goal is to extend the application even to without-card payments.

Use of certificates

- *Electronic ID & Trust Services (eIDAS)*
- *Public Key Infrastructure (PKI)*

Data exchange

- *ISO27001*
- *Sensitive payment data protection*

Security measures

- *Dynamic link*
- *Fraud detection and prevention mechanisms*
- *SCA*

User authentication

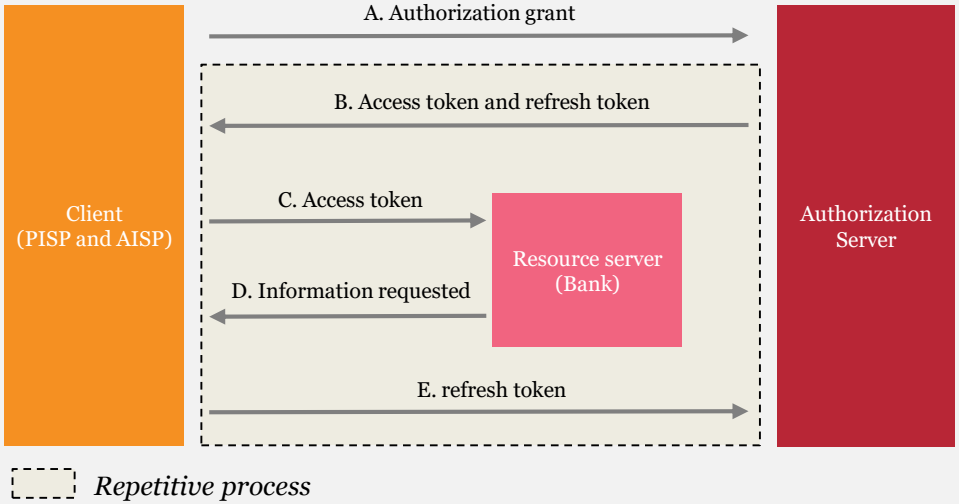
RTS clarifies the obligations and exemptions of the players involved, and, in relation to the theme of strong customer authentication, the Banks will have the burden to define the authentication procedures to be applied when a transaction is initiated through third-party services. In addition to what previously defined, it opens the possibility for the TPP to take charge of the authentication process but only in case of a particular preventive contractual agreement with the Bank. The process must also contemplate the generation of an authentication code which would allow to limit the claims of non-arranged information from users directly to a maximum of two accesses per day *(cf. repetitive Authorization to access to data BOX)*.

Repetitive authorization to access to data

One of the main changes introduced by RTS regards the possibility for the user to authorize the AISP to automatically question its own checking account. An AISP can access automatically maximum twice a day and not later than one month after the last day in which strong customer authentication was applied.

This requirement suggests the generation of an authentication Token with temporary validity which, once verified from ASPSP, enables the AISP to access services without further interaction of the user.

A possible way to implement the service, widely used to authorize access to external applications to "protected" contents, might contemplate the use of OAuth 2.0 framework, which involves the use of a token exchanged through TLS channel (RFC 6749) to be associated the correct security principals, providing the encryption of tokens and / or the achievement of the appropriate security certifications (eg PCI-DSS and / or ISO 27001) with regard to the systems in scope.



A. The client initiates the authorization process using the credentials previously acquired by the user through the services made available from the ASPSP

B. If credentials are valid, the token and (if any) the refresh token are returned

C. The client requests access to the service

D. If the token is valid, the Bank returns what requested

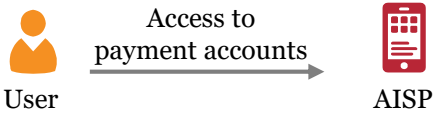
Points C and D can be repeated until the token is valid

E. The client uses the refresh token obtained in step B to restart the authorization process. The process starts again from step B

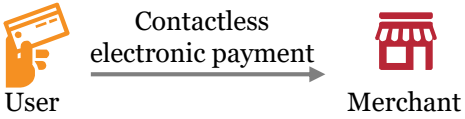
Exemptions from SCA

RTS details the case studies for which the adoption of measures of strong customer authentication is not required[1]. In particular, the adoption of such measures is at the discretion of the institution in the event of:

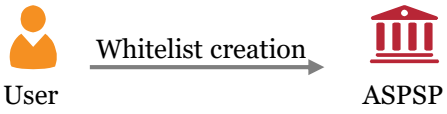
i. Access to the information of the user account for consultation. First access authentication is still contemplated and will have maximum validity of one month. For longer timing re-authenticate the client will be needed;



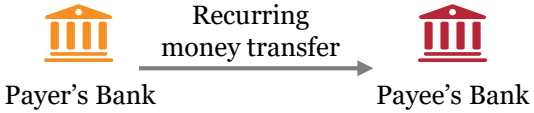
ii. Payments with contactless cards at retail stores with amounts for individual purchase not exceeding 50 € and a maximum cumulative value of 150 €;



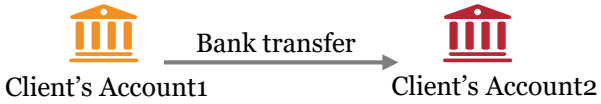
iii. Transactions to beneficiaries included in a whitelist created with the Bank in which the bank account is rooted. The application of strong authentication measures is required in the process of creation of the beneficiaries list and for any subsequent modification by the user;



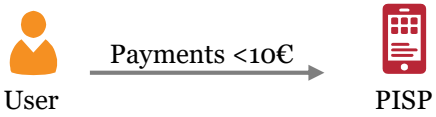
iv. Continuous transfers of same amount and to the same beneficiary, excluding the first launch of the series of wire transfers and in case of change of amount and / or beneficiary;



v. Transfers made on current accounts of the same bank made payable to the same person or entity;



vi. Payment via remote channel with maximum amount of 10 € , and the cumulative value of 100 €.



The implementing provisions, once in force, will replace the "Guidelines for the security of payments via Internet" issued by the EBA December 19, 2014 and adopted the 16th update of Circular no. 285 of 17 May 2016, strengthening their effectiveness.

[1] It is being studied the possibility that the above-mentioned exemptions are mandatory for the ASPSP and not only applicable, in order to promote a more homogeneous application of them in the market.

Robert Bo Jensen

Partner | Financial Services

M: +45 5353 8263
ROJ@pwc.dk

Sune B. Krings

Senior Manager | Financial Services

+45 3068 7728
SBK@pwc.dk