

API Evaluation Group

Authentication (Strong Customer Authentication)

Key topic clarification for API standards initiatives

Summary

- The API interface must allow PSPs to rely on all authentication methods and processes issued by the ASPSP to PSUs and AISPs/PISPs cannot be prevented from using the ASPSP-issued PSU credentials
- An ASPSP will need to be able to demonstrate, amongst other criteria, that their API interface has been widely used for at least 3 months by PSPs to benefit from a fallback-exemption under the RTS
- The identification and authentication journey, facilitated by the API interface, is a critical component as it has a key impact on the experience of the PSU
- The range of authentication methods and processes (e.g. redirection, embedded, decoupled/redirect and decoupled/embedded - see slide 6&7 for overview) and the design of those to enable SCA should be supported by the API initiatives
- The API initiatives should define specifications that support all SCA methods and processes and should not only support the redirection method – thus a spectrum of options would be supported. This will enable an ASPSP to implement one, or more, authentication method and process in a standardised uniform way within the framework of the API initiative and to facilitate market choice
- The spectrum of options and the decision of the ASPSP to implement one or more authentication method(s) inherently involves trade offs between risk, liability, space to innovate, business models etc. For example an API interface that allows the PSP to be able to securely transmit the ASPSP-issued PSU credentials (e.g. decoupled/embedded) is more likely to be widely used by PSPs. It however trades off the fact that the PSU will be required to communicate their ASPSP-issued credentials to the PSP

Problem Statement

PSU should be able to grant PSP secure and convenient access to their payment account. The API interface must not introduce obstacles and be widely used by PSPs

- The PSU has to be able to undergo Strong Customer Authentication (SCA) using their ASPSP credentials in order to allow a PSP access to account information and payment initiation
- The PSU must be able to utilise payment initiation and data services that are safe and secure
- The PSU should not be limited to only have to give secure access via a web browser but should be able to do so also on other devices, using other technologies and channels
- The API initiatives should define specifications for all authentication methods and processes and support the full range of personalised security credentials (such as, but not limited to, biometrics) which are used by the ASPSPs that will implement the standard
- The SCA methods and process should be convenient for the PSU. Requiring the PSU to have to pass through numerous screens and/or multiple steps will impact the PSU experience and will have a bearing upon how widely used an interface will be

Key principles

In addition to meeting relevant regulatory requirements (including PSD2/RTS and GDPR), the following core principles should apply:

PSU considerations

- The PSU should be able to give a PSP access to their payment account via SCA without any unnecessary friction
- The PSU should be able to use the services of a PSP without being unnecessarily constrained to have to use a specific device or communication channels as part of the authentication methods and processes
- The PSU should be able to trust the SCA process, that it is secure and reliable

Market point of view

- The PSP should have the maximum freedom to innovate the PSU experience and be able to define and control the front end 'visible' PSU experience
- The ASPSP is responsible for the PSU authentication and granting access. The ASPSP has legal responsibilities to mitigate security and fraud risk when granting access
- PSU consent is provided to the TPP
- PSU authentication is achieved using the ASPSP-issued personalised security credentials

Guidance to the API initiative

- All authentication methods and processes should be supported by the API initiative in their specification, including those where the PISP and AISP can transmit the PSU credentials, when they are classed as transmittable, to authenticate
- Authentication methods and processes should be able to be completed on one single device, while the rest of the user experience takes place on another
- PSU consent is provided to the PSP. The API will allow the ASPSP to use SCA to authenticate
- Biometric-based authentication should be supported as it can help to facilitate a positive PSU journey (support for biometric-based SCA is a market choice of the ASPSP)

API considerations depending on whether or not personalised security credentials are transmittable

A variety of different personalised security credentials exist and not all ASPSPs support all the same types of credentials. These vary per institution and per customer. What is implemented is a market facing choice of the ASPSP. The API initiatives need to support all authentication methods and processes used by ASPSPs.

PSU transmittable credentials

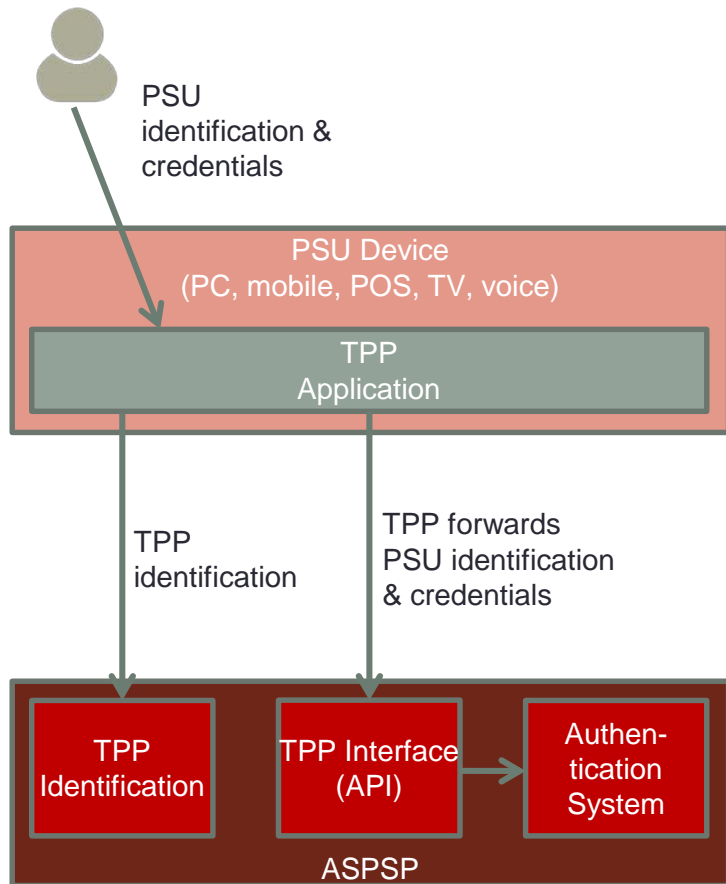
- For credentials that are transmittable by the PSU, ASPSPs shall provide interface(s) through which PSPs can transmit the credentials issued by ASPSP to their customer. For example these may include; a static password and OTP/TAN
- The API should include the option to allow the PSP to transmit PSU credentials (along with user name/identifier) to the ASPSP. Additional authentication steps between the PSU and the ASPSP in this scenario are not necessary
- The process journey for authentication (web/app/mobile etc.) of the PSU should not be more complex or involve unnecessary steps

PSU non-transmittable credentials

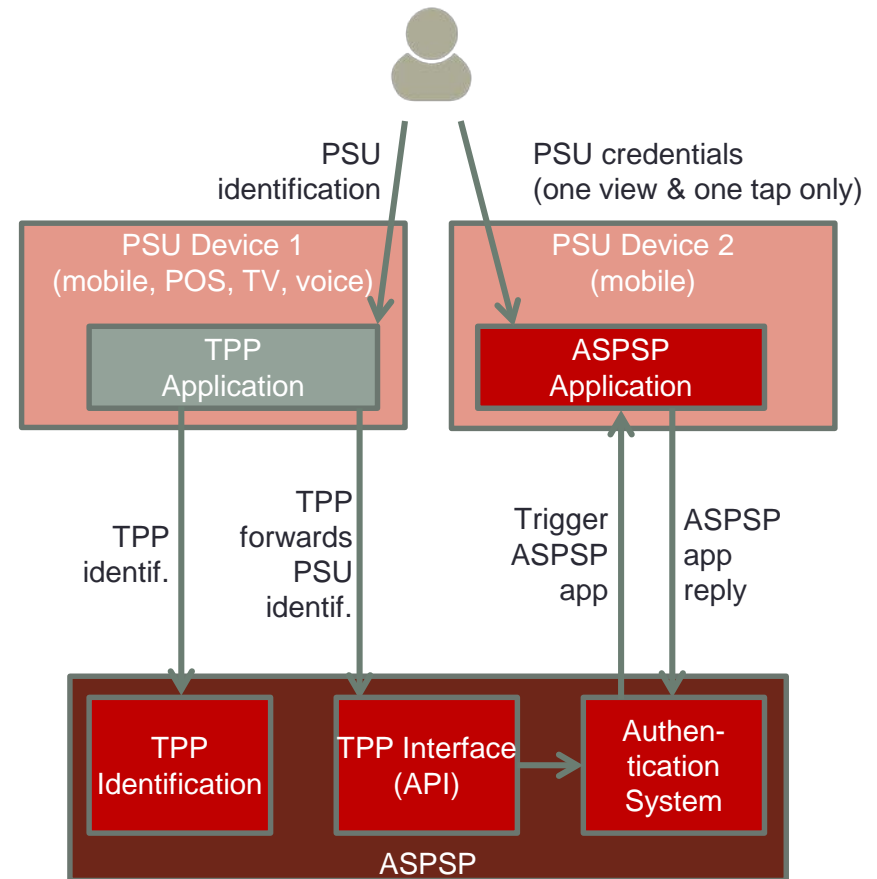
- Credentials which are not transmittable by the PSU include a biometric (for example a fingerprint used either by an ASPSP app or by a trusted third-party app (Mobile BankID in the Nordics))
- APIs shall support authentication methods and processes that support non-transmittable credentials. The process journey for authentication (for example web/app/mobile etc.) of the PSU should be as straight forward as possible and emulate as closely as possible the steps than would be the case when the PSU authenticates to the ASPSP
- The PSP may design the user experience for any device or channel (for example PoS, wearables, voice etc.) with the exception of the authentication step
- Authentication can happen in parallel to the PSU-interaction with the PSP or when the PSP triggers the ASPSP's SCA (for example by sending the user name/identifier and/or IBAN to the ASPSP) which then sends a push message to the associated mobile device upon receipt of which the PSU opens the ASPSP's app or its trusted 3rd party app to authenticate using a biometric
- It is also important that the end-to-end process is not limited to a single device, but that the PSU can interact with the PSP e.g. at PoS while the SCA only is done at the PSU's smartphone, even if it would be possible to do both on the same device (e.g. some smartphones); in other words the payment initiation and authentication processes must be allowed to happen at two different devices

Embedded Flows

Transmittable credentials (e.g. password + TAN)

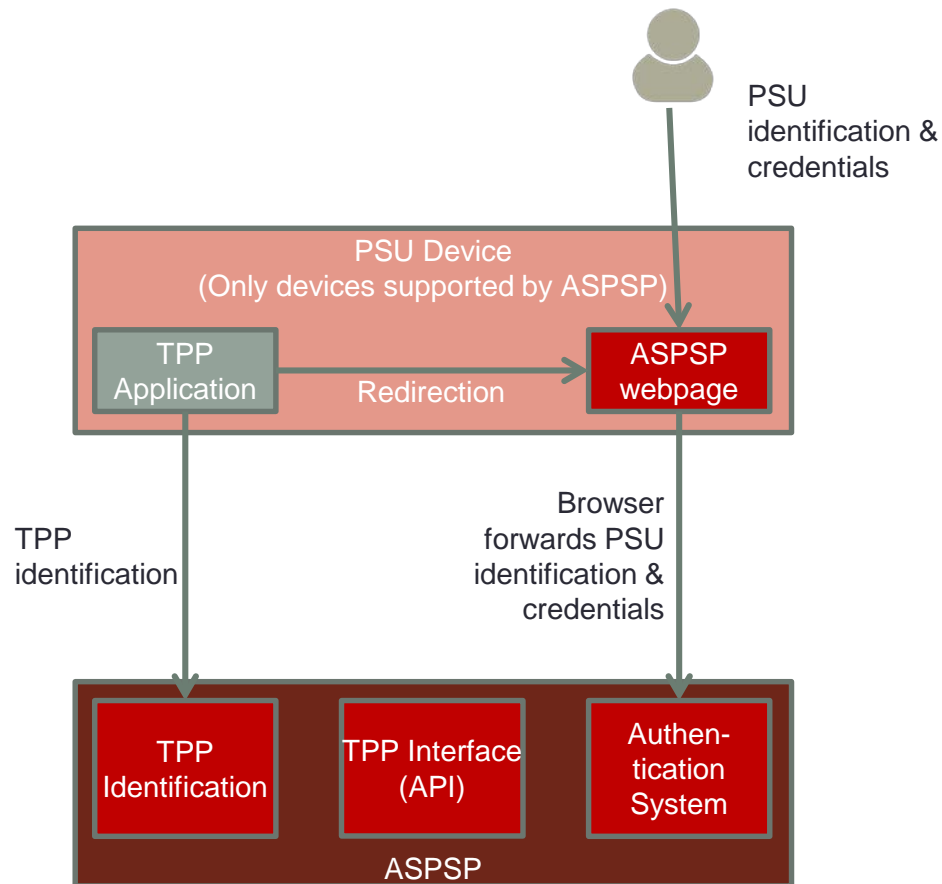


Decoupled / non-transmittable credentials (e.g. biometrics)

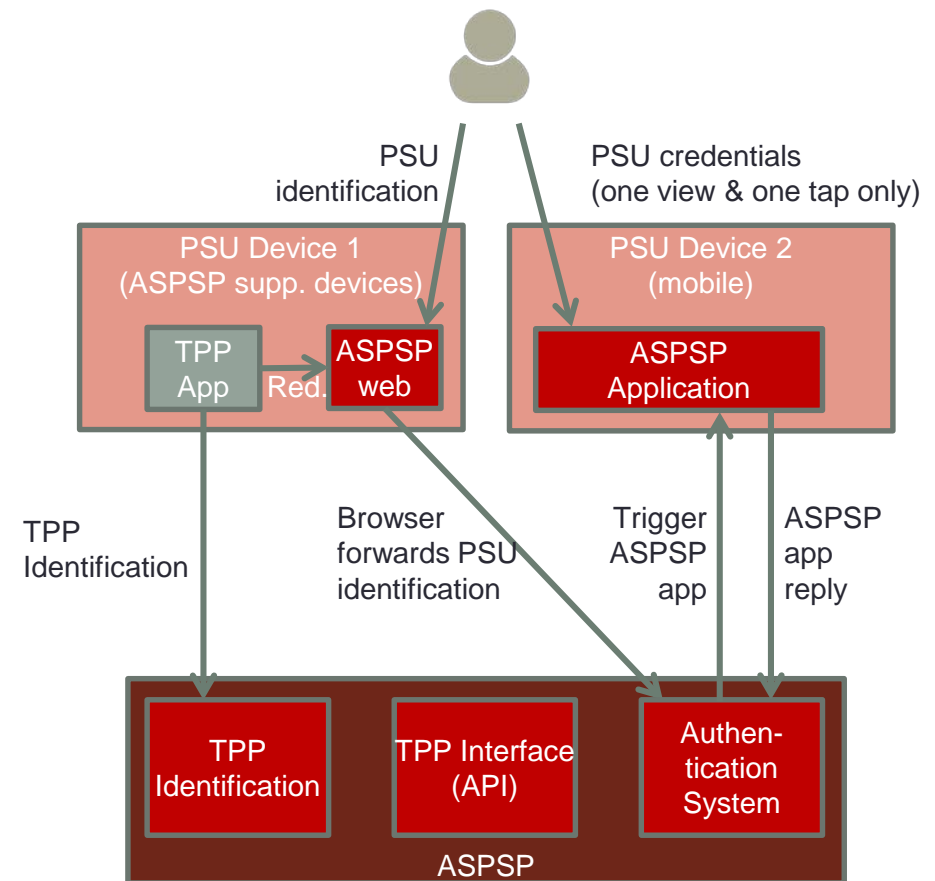


Redirection Flows

Transmittable credentials (e.g. password + TAN)




Decoupled / non-transmittable credentials (e.g. biometrics)



PC/Web Browser – Embedded Approach

TPP	
Payment of Amount:	€ 39.90
To:	Merchant XYZ
Ref:	ABC123
ASPSP Name:	<input type="text" value="Bank XYZ"/> <input type="button" value="v"/>
User Name:	<input type="text" value="12345678"/>
Password:	<input type="password" value="*****"/>
SCA Type:	<input type="text" value="TAN Generator"/> <input type="button" value="v"/>
<input type="button" value="Request to Pay"/>	



TPP	
Payment of Amount:	€ 39.90
To:	Merchant XYZ
Ref:	ABC123
Account #:	<input type="text" value="343766889"/> <input type="button" value="v"/>
TAN*:	<input type="text" value="474824"/>
* As created on TAN Generator	
<input type="button" value="Confirm"/>	

TPP	
Payment of Amount:	€ 39.90
To:	Merchant XYZ
Ref:	ABC123
 Done	

- ASPSP Name: autocomplete & drop down list
- Enter User Name/Identifier
- Enter Password
- Select SCA type from supported options
- Select Account # from drop down list
- Enter TAN generated & confirm

1 screen – 6 inputs – 2 clicks

Mobile App – Decoupled/Embedded (Biometrics)

TPP	ASPSP	TPP
Payment of Amount: € 39.90 To: Merchant XYZ Ref: ABC123	Payment of Amount: € 39.90 To: Merchant XYZ Ref: ABC123	Payment of Amount: € 39.90 To: Merchant XYZ Ref: ABC123
ASPSP Name: <input type="text" value="Bank XYZ"/> <input type="button" value="v"/>	 Touch ID to confirm	 Done
User Name: <input type="text" value="12345678"/>		
Password: <input type="password" value="*****"/>		
SCA Type: <input type="text" value="Fingerprint"/> <input type="button" value="v"/>		
<input type="button" value="Request to Pay"/>		

- ASPSP Name: autocomplete & drop down list
- Enter User Name/Identifier
- Enter Password
- Select SCA type from supported options
- ASPSP to trigger the opening of their mobile app on the PSU phone
- PSU to use provide fingerprint (Touch ID)

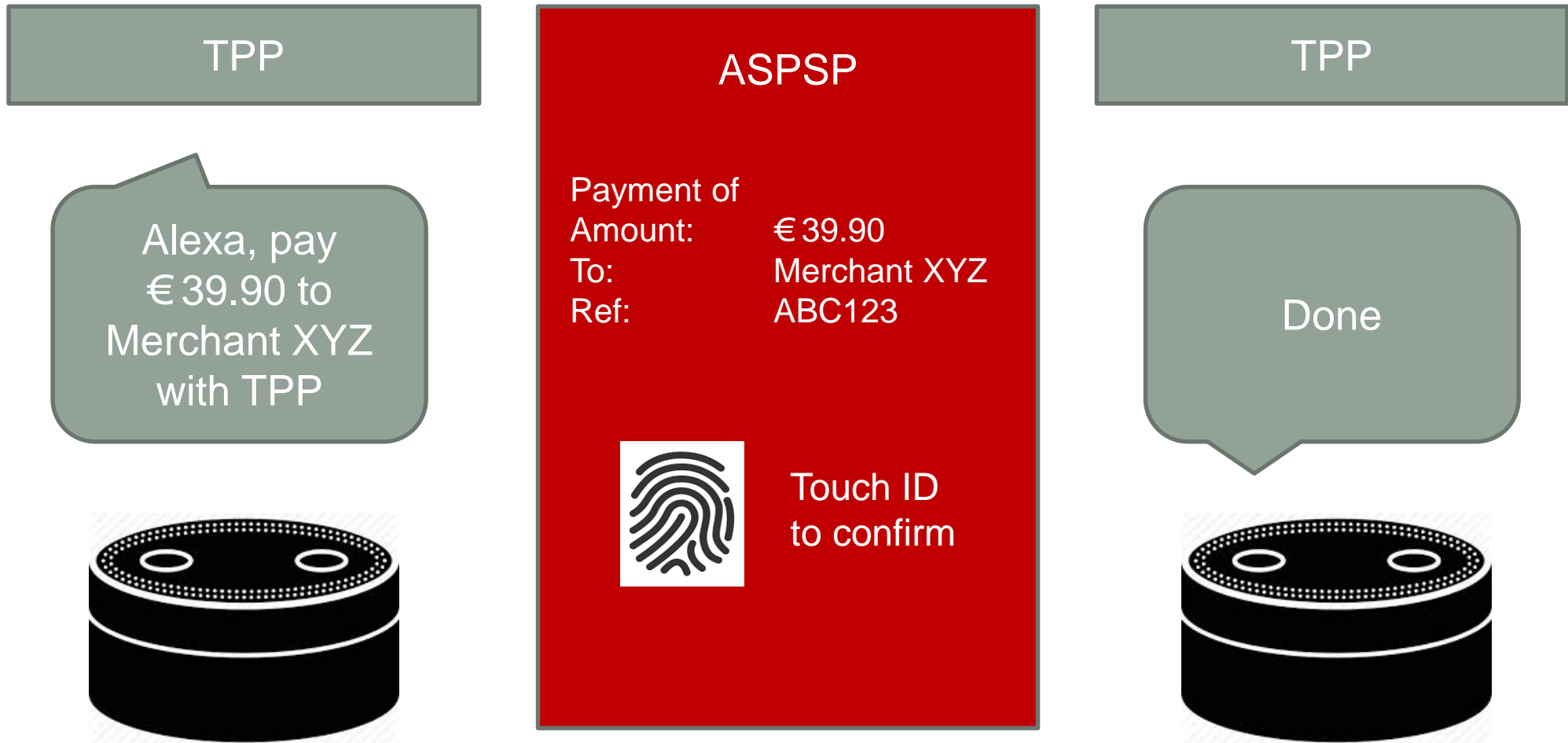
2 screens – 4 inputs – 1 click – 1 touch

POS/Wearable – Decoupled/Embedded (Biometrics)



2 screens – 1 tap – 1 touch – 0 click

Voice – Decoupled/Embedded (Biometrics)



1 command – 1 screen – 0 click