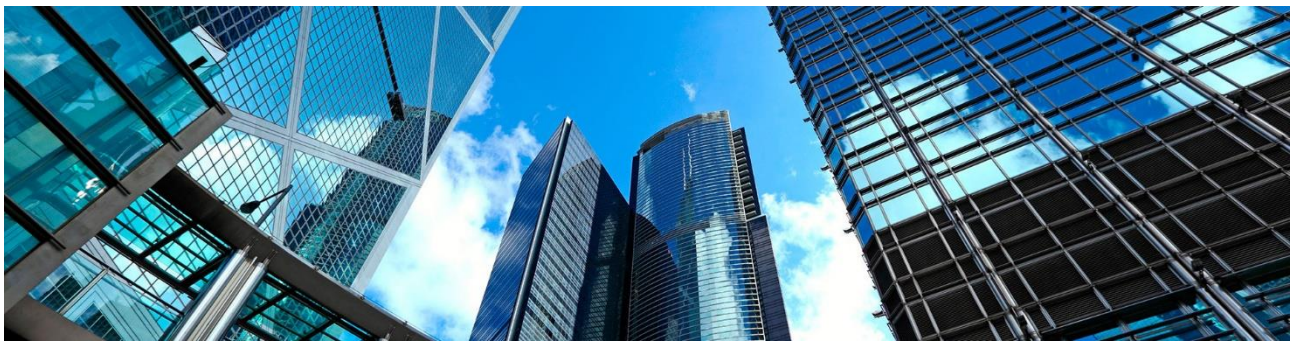


Third Party Provider User Management for PSD2 Access to Account (XS2A)

Open Banking Europe - providing collaborative services to support PSD2 XS2A, in partnership with the financial industry

Contents

1. About Open Banking Europe

Purpose

The revised Payment Services Directive (PSD2) came into force in January 2018. At this point, all regulated entities (Payment Service Providers) had to ensure that they individually comply with PSD2 and the Regulatory Technical Standards (RTS) set out by the European Banking Authority (EBA).

Many experts believe that the financial industry is expected to organise itself to make sure that the implemented solutions for PSD2 are interoperable.

PRETA Open Banking Europe has been launched to support Payment Service Providers (PSPs) and Third Party Providers (TPPs) in meeting the Access to Account (XS2A) requirements of PSD2.

History

PRETA S.A.S. was created in 2013 to develop and innovate market competitive services in digital payment and identity solutions. The company is a wholly-owned subsidiary of EBA CLEARING, a provider of pan-European payment solutions currently owned by 52 shareholder banks.

Following a series of stakeholder consultations that started in 2016 to determine industry requirements, PRETA launched Open Banking Europe to build a PSD2 Directory solution to support PSPs and TPPs in meeting the PSD2 XS2A requirements.

Audience

Open Banking Europe is aimed at the following audiences:

- Competent Authorities
- Payment Service Providers (PSPs), including:
  - Account Servicing Payment Services Providers (ASPSPs)
  - Third Party Providers (TPPs)
- Qualified Trust Service Providers (QTSPs)
- Solution Providers

Disclaimer

The PRETA Open Banking Europe PSD2 Guides are not an in-depth legal analysis of PSD2 and its associated regulations and standards. They are an attempt to summarise the regulatory requirements of PSD2 in a clear and simple way.

Whilst care has been taken to ensure that the information contained in this guide is true and correct at the time of publication, there are still clarifications needed around PSD2's scope and implementation and this may impact on the accuracy of the information contained within this guide.

As such, Open Banking Europe cannot guarantee the accuracy or reliability of any information contained within this guide at the time of reading, or that it is suitable for your intended use.

2. About This Guide

Scope

This guide summarises the considerations and processes that are necessary to enable Account Servicing Payment Services Providers (ASPSPs) to provide secure and controlled Access to Accounts (XS2A) Services to those Third Party Providers (TPPs) who want to offer the new Payment Services available in Europe under PSD2.

The following subjects are covered:

- Internet Security
- Controlled Access
- TPP Onboarding

Audience

This guide is aimed at the following audiences:

- Competent Authorities
- Account Servicing Payment Services Providers (ASPSPs)
- Third Party Providers (TPPs)
- Qualified Trust Service Providers (QTSPs)

References

This guide cites the following sources:

- 'Classification of Security Threats in Information Systems' (Procedia Computer Science)
- The EBA RTS on Strong Customer Authentication & Common Secure Communications Under Directive 2015/2366 (PSD2)
- The General Data Protection Regulation (GDPR)
- The Revised Payment Services Directive (PSD2)

For links to the above sources, please see the Bibliography on page 18.

Terminology

Access to Account (XS2A)
The provision of secure access to accounts operated by ASPSPs using APIs, in order to enable TPPs to provide Payment Initiation Services (PIS), Account Information Services (AIS), and Card Based Payment Instruments Issuing (CBPII) to customers.

Application Programming Interface (API)
A set of definitions, protocols, and tools that can be used to create applications, interact with other applications, and exchange data.

Certificate
An electronic 'passport' used to certify the identity of a person, machine, or organisation over the Internet.

Electronic Seal
An electronic 'signature' used by a legal entity to certify electronic documents as genuine.

European Banking Authority (EBA)
The body responsible for publishing the Regulatory Technical Standards (RTS), Implementing Technical Standards (ITS), and a central register for PSD2.

National Competent Authority (NCA)
A competent authority in Europe with the designated authority to register and authorise PSPs.

NCA Public Register
A national publicly available register of PSPs and their payment services authorisations (roles) in a country, maintained by the country's NCA.

Third Party Provider (TPP)
An entity authorised to access accounts on behalf of customers but that does not operate those accounts themselves. TPPs include PISPs, AISPs, and CBPIIPs.

Trust Service Provider (TSP)
An entity that provides digital services which enable the issuance and proving mechanisms to secure and protect information online. Examples include Certificates and Electronic Seals.

User Profile
The 'account that a TPP holds with the ASPSP to manage the APIs and Services that the ASPSP offers.

3. Overview

ASPSPs can provide secure & controlled XS2A Services to those TPPs who want to offer the new payment services available under PSD2

Internet Security

Account Servicing Payment Services Providers (ASPSPs) must consider the level of Internet security required to enable Access to Account (XS2A) services for the new Third Party Providers (TPPs):

- Infrastructure & Customer Protection: An ASPSP's infrastructure will be susceptible to different types of Internet threats by malicious actors, unless adequate security measures are taken.
- Default Blocking & Controlled Access: ASPSPs must treat all new or unknown entities as possible malicious actors until they can check and validate them.

→ See **3. Internet Security** on page 6

Controlled Access

ASPSPs can identify TPPs trying to connect to their XS2A services, block unknown entities, and provide access to known and trusted TPPs by implementing controlled access measures:

- A User Management System (UMS) will enable an ASPSP to manage TPPs' access to systems.
- Automation & Self-Service will efficiently and cost-effectively handle each TPP access request.
- Guides & Tutorials will explain the controlled access process and give examples to the TPPs.
- Support will help TPPs when they encounter errors or other issues.

→ See **4. Controlled Access** on page 9

TPP User Management

ASPSPs may build a number of key steps into their XS2A services set-up and provision process to safely and securely onboard new TPPs requiring access to their customer accounts to offer PSD2 services:

1. Discovery
2. Sign-Up
3. Access Request
4. Check Identity
5. Check PSD2 Access
6. Access Granted

→ See **5. TPP User Management** on page 11

4. Internet Security

Third Party Internet Security Considerations for PSD2

The Internet already provides the ability for Account Servicing Payment Services Providers (ASPSPs) to offer their services digitally over publicly available infrastructure and digital ports. Over the past few years, this has been widely adopted to the point where now almost every ASPSP in Europe offers both Internet and Mobile payment services.

However, these services have previously only been offered to existing customers with accounts operated by their ASPSP, through their Controlled Access Points, their devices, and their Graphic User Interfaces (GUIs), such as websites and mobile apps.

Under the revised Payment Services Directive (PSD2), new Third Party Providers (TPPs) will be able to access account services from the ASPSPs, through Application Programmable Interfaces (APIs). This change creates new security and control challenges.

Account Servicing Payment Services Provider (ASPSP) Infrastructure & Customer Protection

Not all actors on the Internet are benign. New APIs and 'Internet Available' services create an opening in the ASPSP's infrastructure which will be susceptible to Internet threats by malicious actors, unless adequate security measures are taken.

Technology attacks on the ASPSP as a result of poor security measures could result in any of following impacts if not protected against[1]:

- Denial of Service: Intentionally degrading or blocking computer or network resources by overloading the maximum capacity of that resource channel.
- Theft of Service: Using computer or network services without authorisation and without degrading the service to other users. It can result from theft of service, theft of functionality, theft of data, and/or software/ hardware or data misuse.
- Illegal Service Usage: Using the normal function of the system to achieve the attacker's behaviour for other purposes. For example, an attacker uses the normal network connection to attack other systems, by using vulnerabilities in the system to achieve the attacker's aims.
- Hijack or Impersonation: Using the computer network or services for malicious or illegal activities using valid credentials that have been intercepted/replayed, replicated, stolen, or reset due to poor User Account Recovery operations.
- Disclosure of Information: Disseminating information to anyone who is not authorised to access that information. The following threat actions can cause unauthorised disclosure:
    - Exposure
    - Interception
    - Inference
    - Intrusion
    - Redirection
- Destruction of Information: Deliberately destroying a system component to interrupt system operation.
- Corruption or Sabotage of Information: Also called 'Information Tampering', any unauthorised alteration of files stored on a host computer or data that is in transit across a network. This includes adding, deleting, or modifying the target system's memory, hard drives, or other parts, for example, by implanting a Trojan (a file-like virus invasion that would lead to corresponding file changes). The following threat actions can cause Information Tampering:
    - Spoofing
    - Malicious Logic

[1] See 'Classification of Security Threats in Information Systems' (Procedia Computer Science)

- Falsification
- Repudiation

- Elevation of Privilege: Using weaknesses in the system to get permission (which would should not be normally granted) to access the target system. For example, violating permissions to gain access to user administration controls.

Controlled Access

ASPSPs have an obligation to allow legitimate TPPs to access their accounts with no contracts and no barriers. At the same time, ASPSPs must treat all unknown entities as possible malicious actors to protect their customer resources and infrastructure, until they can check the entity's identity and validate their regulatory access.

To avoid the threats described above, solutions are needed where the ASPSP remains secure, whilst giving Access to Accounts (XS2A) API access to those third parties who are authorised.

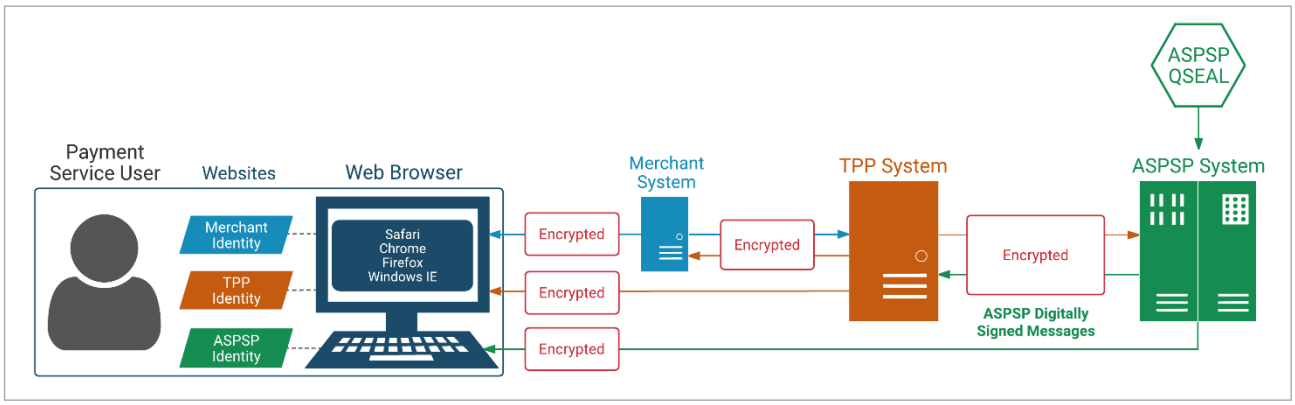
Given the severity of these threats and their impacts to ASPSPs and customer resources, ASPSPs will block XS2A API access by default until the TPP can be validated.

This process of checking the identity and access rights of a TPP is partially detailed within the European Banking Authority's 'Regulatory Technical Standards for Strong Customer Authentication & Common Secure Communications Under PSD2' (EBA RTS for SCA/CSC Under PSD2). However, it needs further development to be fully robust and secure at implementation, whilst ensuring that TTPs only need to meet the minimum requirements and process necessary.

Fundamentally, in order to authorise XS2A API access, the ASPSP will check the following:

- Identity: The entity requesting access to XS2A services is who they claim to be.
- Regulatory Validation:
  - Which EU countries the TPP is authorised to operate PSD2 services in, and
  - Which PSD2 services the TPP has been authorised to operate and/or access.

If the TPP cannot prove their identity or does not have sufficient regulatory permissions, the ASPSP should not allow access to the TPP until they can be checked correctly.



Identity

Public Key Infrastructure (PKI) & Certificates

In modern computing, the use of cryptography allows for information to be bound at source, so that the encrypted information cannot be changed or altered. These result in what are known as certificates.

The use of a PKI allows the owners/holders of such certificates to also uniquely sign a request that proves they are the correct owner/subject of that certificate, using secret information that only they should possess. Using this model, an ASPSP can ask for proof of identification from the TPP and reliably check that they are who they claim to be.

Regulatory Validation

Financial Services License & Permissions

There is a new requirement for ASPSPs to be able to validate TPPs' regulatory access levels with a trusted regulatory source - a National Competent Authority (NCA) Public Register. Such a validation service should

be as standard and secure as possible so as to not allow malicious actors to gain unauthorised access.

This validation may be done directly with the NCA or through a Trusted Service. However, not all NCA Public Registers hold the same information in the same format or are easily machine readable. This may cause issues in TPP checking by the ASPSP and also may require human intervention, which will significantly delay the TPP getting access.

Security Standards & Industry Alignment

If every ASPSP were to implement their own security and controlled access processes, this would have several cost and security impacts:

- Costs to ASPSPs: Each ASPSP would have to consider their own security architecture at a higher cost, rather than shared standards and policies at a shared cost.
- Less Coordination/Mutual Protection: Common issues and attack vectors (with counter measures and policies) could not be addressed by the sector as a whole to secure the industry. Successful attacks on one ASPSP may be replicated successfully across many ASPSPs. This could be prevented by mutual protection and early warning notifications.
- Costs to TPPs: Each TPP would have to implement separate access processes with each ASPSP separately, as well as maintaining separate security polices at each ASPSP, increasing their costs and potential exposure to security threats.

Therefore, it makes sense for the industry to adopt a collaborative approach towards security and controlled access for PSD2, with mutually agreed security standards (typically communicated within the API standard).

5. Controlled Access

What is Access Control?

As an Account Servicing Payment Services Provider (ASPSP) will have many Third Party Providers (TPPs) trying to connect to their Access to Account (XS2A) API services, it is important that the ASPSP is able to identify a TPP each time they attempt to connect and that they are able to:

- Block unknown entities, or
- Provide access to known and trusted TPPs with valid access credentials.

Imagine a security guard checking a guest list at a public event. Attendees that do not have a ticket are turned away. At the event itself, guests may have further area access rights, such as a VIP All Access Pass, or access to the common areas only.

Trusted guests may want to exit the event and return later. In these situations, the trusted guest will be either be recognised or have been given a stamp or marker by the security guard, so that they do not have to queue or be checked against the guest list again. This saves the security guard time and effort and provides convenience for the guest.

The key logistics that enable the security at this event to operate correctly are as follows:

1. Access to the event is at a known Controlled Access Point. It should be impossible to enter the venue from any other locations.
2. The security guard and the guest list are located at the Controlled Access Point.
3. Guests outside of the event go to one line to identify themselves for the first time. Guests that have previously been checked go to another line to quickly re-enter the event.
4. New guests present their ticket or other credentials, such as being on a pre-approved guest list, to be given access to the event.
5. If a guest does not have the correct ticket or credentials, the security guard denies them access to the event.
6. If a guest does have the correct ticket or credentials, they are allocated an identifier that is unique to that event and which may give further access to areas within the event.
7. An additional marker (such as a stamp or the unique identifier) lets the guest exit and re-enter the event.

For XS2A, the situation is the same as the example above, only with the actions happening in a digital, rather than physical, space. 'Event' is replaced with 'ASPSP systems' and 'Guests' with 'TPPs'.

The Controlled Access Point is commonly located on the Developer Portal and should be easily available on the Internet, with instructions on how to access it. At the Controlled Access Point, the ASPSP can offer two channels:

- The first channel is for new TPPs coming to the ASPSP's systems for the first time and who need to identify themselves.
- The second channel is for known TPPs who have previously identified themselves and given a unique access identifier which the ASPSP recognises and can let that TPP into the ASPSP systems to which they are allowed access.

What is a User Management System?

A User Management System (UMS) contains six important capabilities:

1. Generates an identity for specific TPPs and issues unique access credentials.
2. Assigns Access Rights to resources/scopes for each TPP by issuing further area-specific access credentials.
3. Retains a record of previously issued TPP access credentials.
4. Checks against the issued TPP access credentials record when a TPP returns, enabling authorised access.
5. Monitors/logs all TPP activity, including timestamps, areas accessed, and actions taken by the TPP for their own account.
6. Manages the access credentials and rights of a TPP, such as changes or removal.

This can either be automated or a human operated manual action using an Administrator Control capability but would require additional security.

The Benefits of a User Management System

If correctly implemented, the ASPSP should now be able to identify, track, log, and control all TPP access events to the ASPSP's systems. The records and logs from this system can be used for:

- Automated reporting (internal and regulatory).
- User access management, such as removing redundant users, or changing credentials.
- Manual user access control, such as suspending or revoking access, should a security issue occur.
- User notifications, through their stored TPP communication details.
- Investigation and dispute resolution, where access records (and any other information) of an involved TPP needs to be reviewed.

Access Control Considerations

Automation & Self-Service

There are many examples of automation and self-service for Controlled Access Points, most notably online booking and self-check-ins at airports.

For PSD2, both the Controlled Access Point and User Management System can be programmed as automated functions, removing the need for human operators to individually review and handle each TPP access request. This reduces costs and increases the ASPSP's processing ability.

If the User Management System is automated from the ASPSP side, the TPP becomes responsible for the requests and information input required to gain access the ASPSP's systems.

This requires a self-service capability for the TPP to operate, including a User Interface for the TPP's human operator (an Administrator) to complete an initial setup and configure their access, then to manage the access credentials that have been issued by the ASPSP.

By removing the need to interact with a human operator on the ASPSP side, it is more convenient for the TPP and means that the service can be made available outside of normal working hours.

A self-service capability may include the following activities for the end user:

- User Profile setup.

  Normally called an 'account', which has a different meaning for ASPSPs, so the term 'Profile' is used.

- Administrator assignment to the User Profile.
- Association of Access Rights requests to the User Profile.
- User Sub-Profile creation and deletion.
- User Sub-Profile management, including delegation or restriction of inherited access rights from the User Profile and the ability for sub-users to self-service.
- Receipt and storage of access credentials.
- Access credentials management, including voluntary access removal and change requests.
- Profile recovery should the User Profile be blocked or compromised.

Guides & Tutorials

If automating and providing a self-service capability for TPPs, tutorials are required to explain the process steps involved and to give examples of what is required of a TPP to complete the process.

These can be a combination of written text, diagrams, images, and even interactive videos. However, it is up to each ASPSP to decide the level of guidance that is most appropriate.

Support from the ASPSP

Whilst most self-service activities will be successfully operated by the TPP, there will be occasions where they may find it difficult to complete an activity or experience errors that they cannot resolve themselves. In these situations, there will still need to be a level of human operated support and interaction, for example, a Helpdesk Support team available through the ASPSP's normal communication channels.

The ASPSP should provide clear methods and details within their Access Control Point, so that the TPP can request support when needed. The human operators should be given some Administrator control for the User Management System and will need procedural guides, so they can apply the correct ASPSP security procedures for each support request.

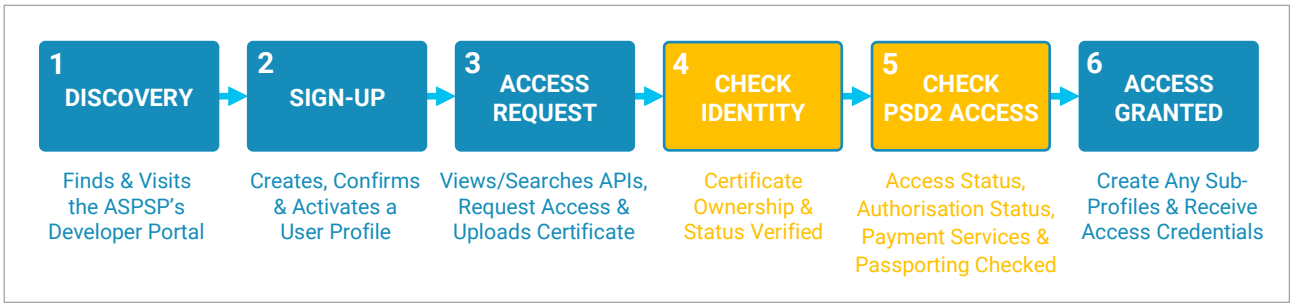
6. TPP User Management

A classic Application Programmable Interface (API) onboarding process contains the following steps. Those steps in orange represent new steps that are used within a PSD2 context to meet the additional identification and regulatory permissions verification requirements.

Onboarding for Third Party Providers (TPPs)

The following diagram shows the normal user journey for an entity signing up to an API on the Internet today. It is drawn from the perspective of the TPP.

The two boxes in orange are specific boxes that exist for PSD2 Access to Account (XS2A) to incorporate the fact that these APIs are not 'Open' but are restricted to certain regulated entities.



To view the user journey from the perspective of the Account Servicing Payment Services Provider (ASPSP), please see the Appendix on page 19.

The TPP Onboarding Process in Detail

This section describes an example flow, containing all of the features that might be present.

This section assumes that:

- The TPP has found the correct website, for example, http://www.ASPSP.com.

  It is often difficult to find the ASPSP information needed by a TPP due to the number of websites, brands, and branches that can exist in many countries. The PRETA Open Banking Europe Directory can assist in this.

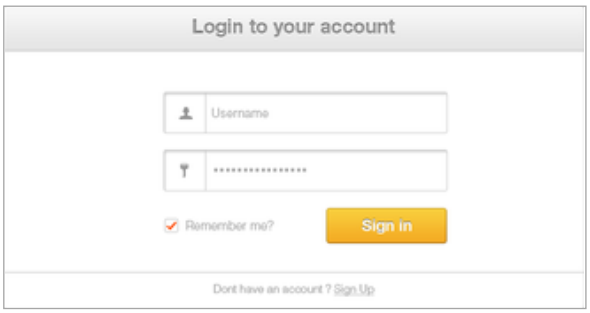
- The ASPSP has a Controlled Access Portal (Developer Portal), for example, http://developer.ASPSP.com.
- The ASPSP has a User Management System (UMS).
- The ASPSP has set up a certificate handling software.
- The ASPSP has set up PRETA for QTSP and PSD2 Directory Services.

This will be further detailed in the **PRETA Open Banking Europe API Catalogue Guide**.

Sign-Up

The TPP finds the ASPSP's Developer Portal and views either a Shop Window or the API Catalogue that the ASPSP offers. To continue, the TPP must self-select either of the following actions:

1. Sign up for a new User Profile with the ASPSP.
2. Log in to their existing User Profile with the ASPSP:

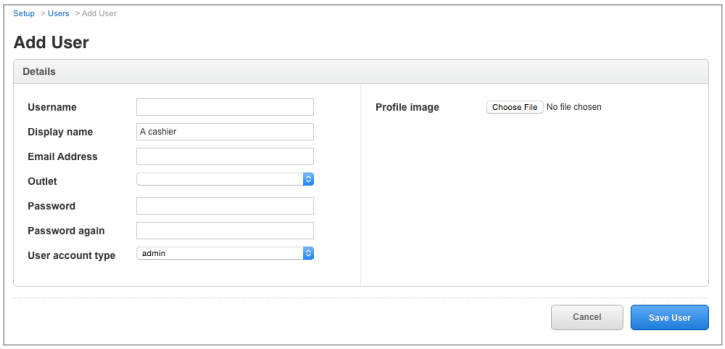


If the TPP tries to log in with User Profile Credentials that are not found within the UMS, they are not given further access. User Profile Recovery options may also be given for:

- Forgotten Username
- Forgotten Password
- Unlocking a Locked Profile

Support options may be also shown on this page, should a TPP be unable to complete self-service without assistance.

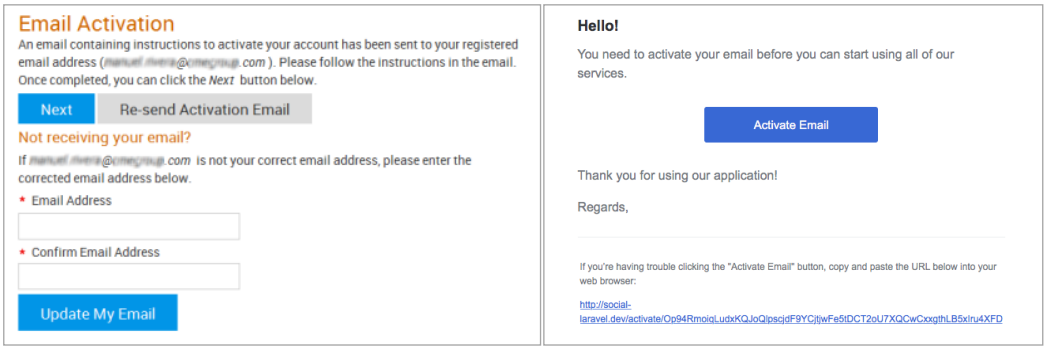
TPPs that are new to the ASPSP will sign up for a new User Profile. The UMS will then automatically create a new User Profile and the TPP Administrator will be asked to manually provide information using a set web form in the Graphical User Interface (GUI):



Once the TPP has provided this information, the UMS should save the User Profile.

It is best practice to use a CAPTCHA or other human verification method at this stage to prevent malicious actors from using Bots to Distributed Denial-of-Service (DDoS) the New User Profile request service.

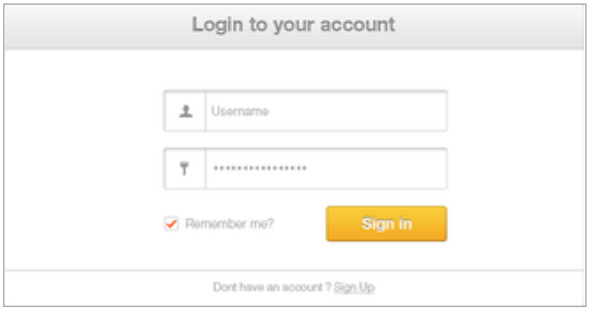
The UMS should then display a message to the TPP asking them to go to their TPP Administrator Contact Email Address and look for a message. The UMS should generate an email to the TPP Administrator Contact Email Address (as provided), asking the TPP to confirm and activate their User Profile:



This process confirms that:

- The TPP Administrator Contact Email Address details are correct.
- The TPP has access to the TPP Administrator Contact Email Address.
- The TPP will be able to use the TPP Administrator Contact Email Address for future actions, such as notifications and user profile recovery.

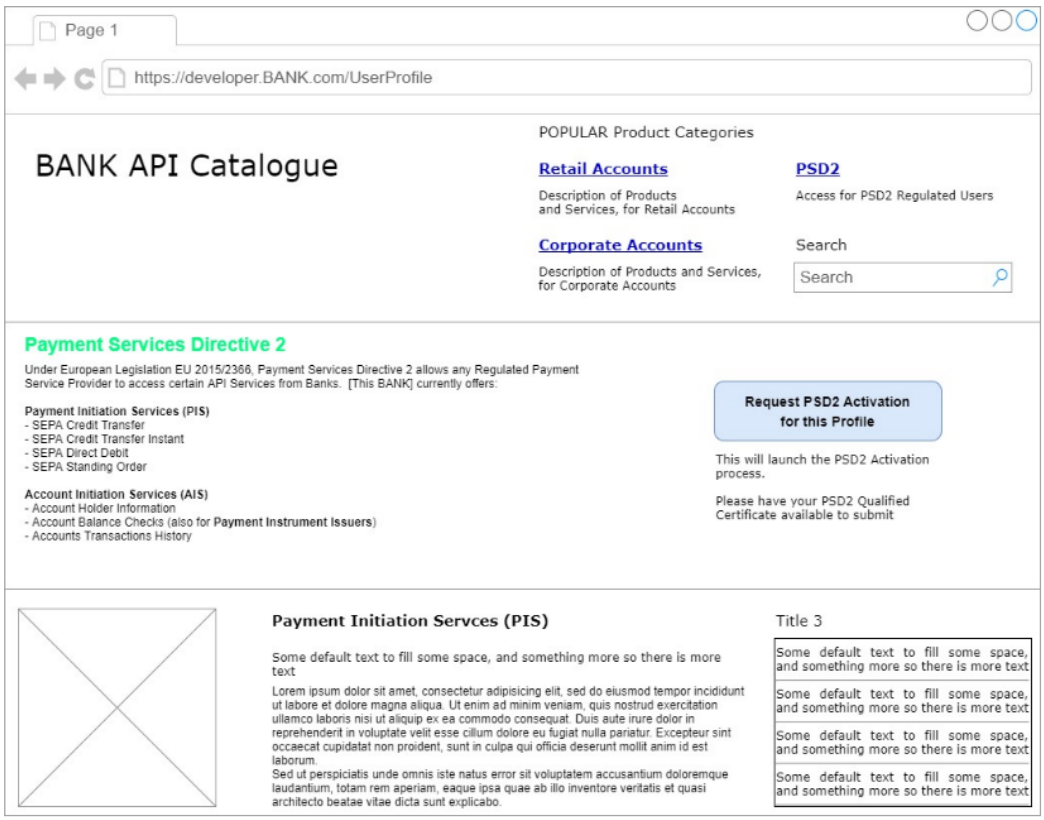
Once the email activation process has been completed, the UMS will mark the TPP's User Profile as 'Active' and allow login requests through the other channel:



The TPP should now be redirected back to the ASPSP's Developer Portal to log in, using the Username and Password that they have just created in their User Profile.

Access Request

Once the TPP is logged in, they will be able to view all the APIs and Services that the ASPSP offers under PSD2, as well as now being able to request that a new API/Service be added to their User Profile:

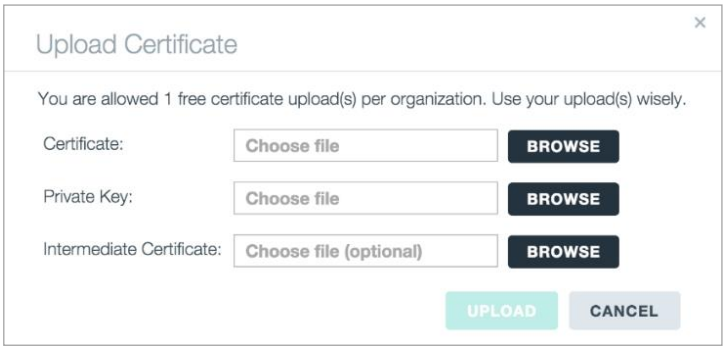


For proprietary APIs and Services, there may be associated Terms of Service, such as 'Free to Use' or 'Service Contract Needed'. If a Service Contract is needed, a Billing and Contract Agreement can be set up through automated self-service. **Get in touch with Open Banking Europe** if you want to learn more.

For XS2A Services, the TPP can now request access to those Services be added to their User Profile.

It is good practice to show a process overview or a progress bar to guide the TPP at this stage:

The TPP should now be presented with a User Interface (UI) that will prompt them to upload their Qualified Electronic Seal Certificate (QSEALC) details, as well as signing an ASPSP generated variable, to prove that the TPP is the owner (or authorised by the certificate owner) of that certificate:



The UMS will then save the QSEALC details and the TPP's Public Key to a secure Trust Store within the ASPSP and begin the PSD2 validation process.

Check Identity (Using the Certificate)

The ASPSP must now check the following:

- Ownership: That the Public Key Infrastructure (PKI) Signature associated with the QSEALC has an outcome that matches. This verifies that the TPP is has access to the Private Key of the certificate, proving that they are the owner. This check can be done locally between the TPP and the ASPSP.
- Certificate Status: That the Qualified Trust Service Provider (QTSP) issuing the certificate verifies that the QSEALC is valid and has not been revoked. This check can be done by either:
  - Checking a local Certificate Revocation List (CRL) or Online Certificate Status Protocol (OCSP) List that has been previously downloaded by the ASPSP, or
  - Directly contacting the QTSP Issuer online using an OCSP Responder (as specified in the QSEAL Certificate Profile information).

In either case, a Service Agreement is required from either a QTSP Aggregator or PRETA.

If the identity validation fails, a log record can be generated, and the request should be rejected. The TPP should be informed of the rejection along with any relevant information. For example:

Rejected Reason [NNN]: "PKI Signature does not match"; Ref [XXXXXXXXXXXX]

Rejected Reason [NNN]: "QTSP Certificate invalid"; Ref [XXXXXXXXXXXX]

Rejected Reason [NNN]: "Certificate has been revoked"; Ref [XXXXXXXXXXXX]

It is up to the ASPSP's own security polices to define further actions and cases that may be needed, for example, multiple failed attempts by a TPP using several revoked certificates in quick succession.

Check PSD2 Access

If the identity of the TPP is valid, then there can be check around what that TPP is allowed to do, i.e. a PSD2 Access Check, using the following reference numbers:

- Unique Reference Number (URN): The QSEALC will contain the name of a National Competent Authority (NCA) and the URN of the TPP supplied by that NCA. The ASPSP can extract this URN from the QSEALC.
- Global Unique Reference Number (GURN): With the correct combination of Country, Competent Authority Name and URN, the ASPSP can generate a GURN that is unique across Europe.

With the URN or GURN, the ASPSP can:

- Check directly with the NCA Public Register for the record details under that TPP URN, or
- Check against the PRETA Open Banking Europe Directory for the details against that TPP URN.

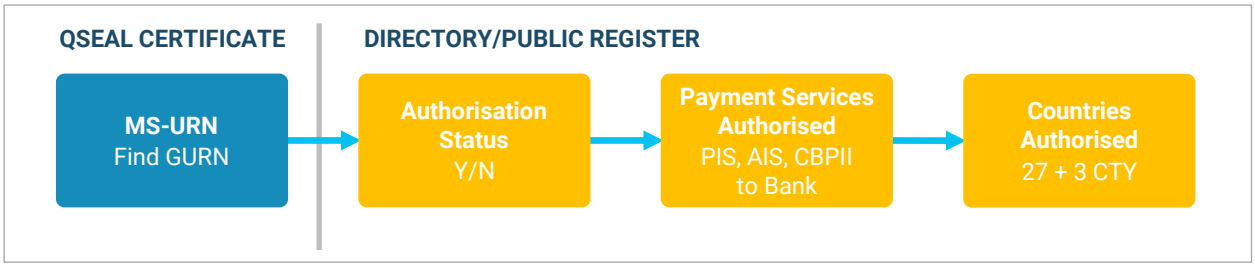
Some NCAs only offer 'human readable' PDF versions of their Public Register, so checking directly with each may be difficult, requiring individual reviews and parsing of the information. This may cause many issues:

- Costs to the ASPSP for a human review of entries.
- Possible delays to the TPP in getting verified, if human operations are needed.
- Errors in human approval in the reading of the information.
- Possible 'Insider Threat' issues within the ASPSP, where a human may deliberately give the wrong validation results and illegal access to services.

The PRETA Open Banking Europe Directory has been developed to resolve these issues by:

- Standardising all European Union Regulator/Competent Authority Register entries into a common data format - the same TPP information regardless of country.
- Having a single Search tool that only requires the URN.
- Providing a Download service that allows ASPSPs to cache a local copy of the Active TPPs List and Revoked TPPs List.
- Providing a Push Notification Service and Change Log that notifies ASPSPs of changes to TPP entries.

1. Access Checks: There are three access checks that the can be performed against the NCA Public Register or the PRETA Open Banking Europe Directory:



Using the GURN with the Open Banking Europe PRETA Directory allows the ASPSP to check all the associated information needed to access to PSD2 Services.

2. TPP Authorisation Status Check: The ASPSP should save all of the information retrieved into the User Profile and check the Status of the TPP Registration:

Field	Data Type	Definition	M/O	Notes
TPP Status	20x	The status found in the NCA lists.	[0..1]	[1] Authorised [0] No Longer Authorised

If the TPP Status is listed as 'No Longer Authorised', the ASPSP should reject the request and return a response to the TPP. For example:

> Rejected Reason [NNN]: Registration Number status check failed; "No longer authorised" Ref [XXXXXXXXXXXX]

If the TPP Status is listed as 'Authorised', the ASPSP can now check the XS2A Services.

3. TPP Payment Services Check: Using the GURN and the lookup, the ASPSP should check which PSD2 Services (Roles) that the TPP is authorised to provide, which will be one or more of the following:

Service	Definition
PIS	Payment Initiation Service. The TPP is authorised to initiate credit transfers for customers online.
AIS	Account Information Service. The TPP is authorised to provide consolidated customer account information services online.
CBPII	Card Based Payment Instruments Issuing service. The TPP is authorised to issue payment instruments and/or acquire payment transactions.

If the TPP does not have any of the listed PSD2 Services authorised, then the ASPSP should reject the request and a return a response to the TPP. For example:

> Rejected Reason [NNN]: PSD2 Services check; "Not Authorised" Ref [XXXXXXXXXXX]

If any of the PSD2 Services are found, the ASPSP can check the passporting and country authorisations.

4. TPP Passporting Check: Using the GURN and the lookup, the ASPSP can check the countries in which the TPP is authorised to provide PSD2 Services.

   All available countries may be extracted and the country of the ASPSP Resource Owner being requested may be checked against the authorised countries of the TPP.

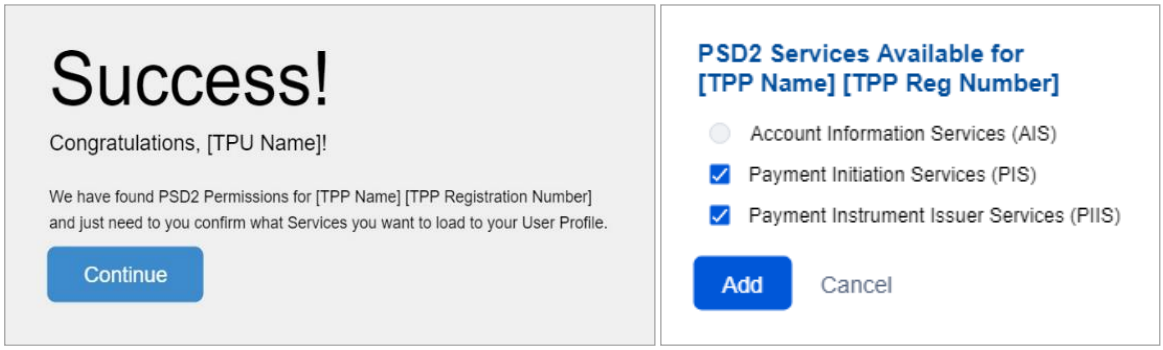
   If there are no matches between the TPP Country Codes and the ASPSP Country Code, the ASPSP can reject the request and return a response to the TPP. For example:

> Rejected Reason [NNN]: "No Permissions for ASPSP Country Code"; Ref [XXXXXXXXXXX]

   For any countries that the ASPSP supports, the ASPSP can then save the details and provide the ability for the TPP configure a Sub-Profile later.

Grant Access

If all of the checks have been successful, the TPP should be informed of the 'Success' outcome and shown the list of permissions available to them for the ASPSP:



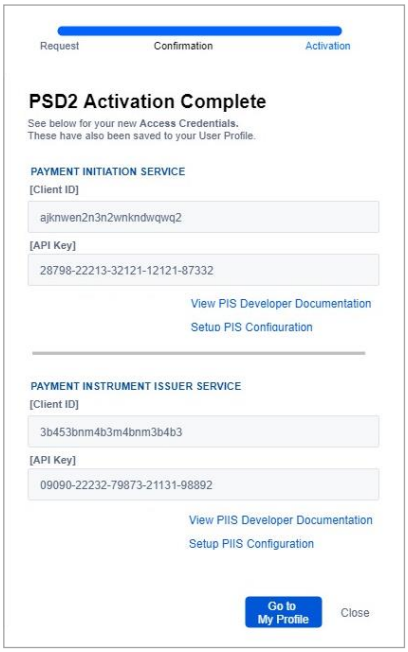
Create Sub-Profiles

Whilst the TPP may have authorisation for several PSD2 Services, the TPP may not necessarily want to access to all of the Services available from the ASPSP. The TPP may be given the option to confirm which Services they want to access, whilst also providing further information to support the business and technical operations of the API itself. ASPSPs may request information from the TPP for each Service that they wish to set up, along with nominated business and operational contacts, in case of later issues.

The TPP can later choose to restart the process with a new certificate, but will have to re-enter the Sub-Profile information to gain new Access Credentials. In addition, the TPP may be given a maximum number of Sub-Profiles they can create, dependent on the ASPSP allowance.

Receive Credentials

Once the TPP has created all of the Sub-Profiles that they wish to enable and have selected which XS2A Services that they want access, new Access Credentials that are specific for the selected XS2A Services may be generated by the ASPSP, saved to the TPP's User Profile, and shown to the TPP.



From here, the TPP may now be given options to:

- View the relevant documentation for a specific API/Service.
- Set up further configurations for the new Services.
- Go to their User Profile to manage users and permissions.

Bibliography

More information about Third Party Provider (TPP) User Management can be found at the following sources:

- 'Classification of Security Threats in Information Systems' (Procedia Computer Science)
  http://ac.els-cdn.com/S1877050914006528/1-s2.0-S1877050914006528-main.pdf?_tid=08523b48-6bc3-11e7-a6b1-00000aab0f26&acdnat=1500387286_ed6b5367cb091cf1793c27feed765d04
- The EBA Regulatory Technical Standards on Strong Customer Authentication & Common Secure Communications Under Directive 2015/2366 (PSD2)
  https://www.eba.europa.eu/documents/10180/1761863/Final+draft+RTS+on+SCA+and+CSC+under+PSD2+(EBA-RTS-2017-02).pdf
- The General Data Protection Regulation (GDPR)
  http://data.europa.eu/eli/reg/2016/679/oj
- The Revised Payment Services Directive (PSD2)
  http://eur-lex.europa.eu/eli/dir/2015/2366/oj

Appendix

Onboarding for Account Servicing Payment Services Provider (ASPSPs)

The following diagram shows the flow from the perspective of the ASPSP, taking into account that the ASPSP may be offering both PSD2 Services (no contract) and Value Added Services (based on contracts).