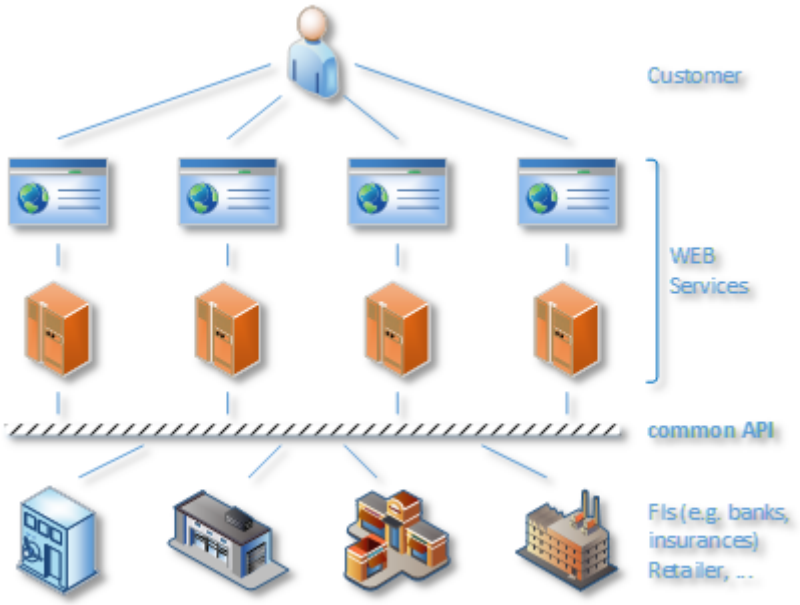
SFTI - working group 'Common API'

API Security

Whitepaper



Authorship: Swiss FinTech Innovations
Release: Version 1.0
Date: 29.7.2021

Team
Common API Working Group@SFTI
https://common-api.ch

About SFTI
Swiss Fintech Innovations (SFTI) is an independent association of Swiss financial institutions committed to drive collaboration and digital innovations in the financial services industry. For more information about Swiss FinTech Innovations, please refer to https://www.sfti.ch.

Content

1. Introduction

The topic of API security is becoming increasingly important as the significance of APIs for the financial industry is growing rapidly. In this industry, the use of APIs roughly falls into three categories:

- Bank-internal IT development, be it in-house programming or integration of third-party software.

- Electronic data exchange with other financial institutions or intermediaries within the financial industry (e.g. SIX).

- Connection of external solution providers such as FinTechs and other Third Party Providers (TPPs).

Depending on the respective area of application, different key aspects of API security are important. Although financial institutions (FIs) have different technologies from different vendors to secure access to their systems, a common standard for accessing the APIs is important for the TPPs in order to efficiently access data of different FIs.

This white paper addresses fundamental aspects regarding API security from all relevant perspectives (business, legal, technical). Furthermore, the specific positions of the companies involved in implementing such a solution are also presented.

1.2 Goals

This paper provides an overview of API Security. In particular, it includes the following areas:

- Achieve a **common understanding** across all target groups:
    - What is API Security?
    - Why is it important?
    - What types of API Security exist?

- Explain **business use cases** and their implication for API Security:
    - Mapping of business use cases and API Security mechanisms.

- Show CH and international (legal) **requirements and best practices**:
    - What are the (CH, Int) legal requirements? In which direction is the journey going?
    - What are the (CH, Int) best practises? In which direction is the journey going?

- Outline the SFTI **recommended approach(es)** for API Security:
    - What is the recommendation of SFTI for PoC, MVP, etc.
    - Next steps

1.3 Target Audience

This white paper on API security is targeted at decision-makers in financial institutions (FIs) and Third Party Providers (TPPs) in the areas of business, legal and information security. Furthermore, standardization bodies and regulatory authorities are also targeted.

1.4 Scope

As already mentioned, depending on the respective area of application, different types of API security with different key aspects are relevant.

This paper focuses on the **API security type where there is a triangular relationship** between customer, TPP and FIs. This is the case, for example, with multibanking or if a FinTech (TPP) provides aggregator services.

See chapter 3.2 Types of API Security for all types and corresponding considerations.

2 Stakeholder Overview

With regard to security and data protection when using API-based banking services, the viewpoints and needs of different stakeholder groups must be considered.

If one does not pick up the respective target audience at its positions, there is the risk that the acceptance of one's own concern suffers.

For **end customers**, the following segments are to be distinguished:[1]

- Technology-savvy customers: I am aware of my risk
- Comfort-oriented customers: Prefer fewer services, but with maximum security
- Legal/regulatory-focused customers: My freedom of action comes first

For **financial institutions**, the following positions are to be considered:

- Business-centric view: We maintain the best possible usage control
- Innovation strategy: We are prepared for future challenges
- End-customer focus: We provide easy-to-use security

The **third-party providers** (FinTechs, WealthTechs, ...) can take the following positions:

- Independent perspective: We want to establish an independent business model
- Role of the supplier: We want to offer financial institutions a solution that they can use as white-label software.

The **legislative-regulatory institutions** can take the following views:

- Market-centered view: the industry itself creates the necessary framework conditions
- Directive view: framework conditions must be set by the government

These distinctions are expressed in more detail in the following sections.

[1] Regardless of the customer's perspective, financial institutions are still responsible for providing a secure authentication infrastructure, at least a minimum of secure functionality in terms of data classification.

2.1 End customers

In the case of end customers, the items outlined below are to be taken into account.

2.1.1 Technology-savvy customers

Positions:

- I am aware of the risks of Open Finance-oriented third-party services.
- My bank should provide me with the best possible access to TPPs that offer me innovative services, in addition to its own up-to-date services.
- If necessary, I am also prepared to assume responsibility for the resulting risks myself if I want to try out or use the services of a new service provider.

2.1.2 Comfort-oriented customers

Positions:

- The bank must guarantee me the greatest possible security at all times when I interact with it.
- The bank should ensure that TPPs that offer me services based on my personal banking data offer the same level of security as the bank itself.
- The bank makes information readily available to me that tells me which TPPs are trustworthy and which ones I should better not work with (yet) if the greatest possible (data) security is important to me.
- If something goes wrong when using TPP-based services, in case of doubt I can rely on my bank to sort it out in my favour.

2.1.3 Legal/regulatory-focused customers

Positions:

- I am critical of the expansion of legal-regulatory restrictions on the Swiss financial centre.
- As a bank client, I want to decide for myself which third parties are allowed access to my data.
- In my view, the existing legal framework is sufficient to regulate the use of new open banking-based services.

2.2 Financial institutions

In the case of financial institutions, the items outlined below are to be taken into account.

2.2.1 End-customer focus

Positions:

- The use of the financial services offered is secured in the best possible way.
- The design of the API security enables easy usability of these services.

2.2.2 Business-centric view

Positions :

- The opening of interfaces/APIs must be carried out in a controlled manner in order not to carelessly risk data loss within the existing customer interface(s).
- For this purpose, the API security must ensure the necessary granularity in authorisations for data accesses that read or change the balance sheet.
- In addition to technical control mechanisms, a code of conduct is established with the partner banks to prevent the aggressive poaching of customers.

2.2.3 Innovation strategy

Positions :

- Basic technical framework conditions are created even if an implementation of services based on them is not immediately planned.
- The aim of this strategy is to be able to react quickly if the development of market trends makes it necessary.
- Otherwise, a smart follower attitude is adopted.

2.3 Other third-party providers

The remaining third-party providers (FinTechs, WealthTechs, ...) can take the following positions.

2.3.1 Independent perspective

The goal of the TPP is to implement its own business model and also to monetize it independently. In particular, the licensing of the solution to or the takeover of one's own company by financial institutions is not sought.

2.3.2 Role of the supplier

The focus here is on licensing the solution to financial institutions. The TPP therefore does not act as a solution provider itself.

2.4 Legislative-regulatory institutions

In the case of legislative-regulatory institutions, the positions outlined below must be taken into account.

2.4.1 Market-centered view

Positions:

- In principle, it is left to the free play of market forces to develop and utilise industry-wide standardised security concepts.
- The legislative-regulatory institutions are mainly limited to the continuous monitoring of the progress of said industry initiatives.
- Steering interventions are the ultima ratio, if the market-based approach is not effective across the board and selective supporting measures become necessary.

2.4.2 Directive view

Positions :

- Due to a lack of sufficient trust in the self-regulatory powers of the market, regulatory bodies such as Finma, for example, make the corresponding requirements binding.
- There is no provision for in-depth coordination with the regulated bodies.

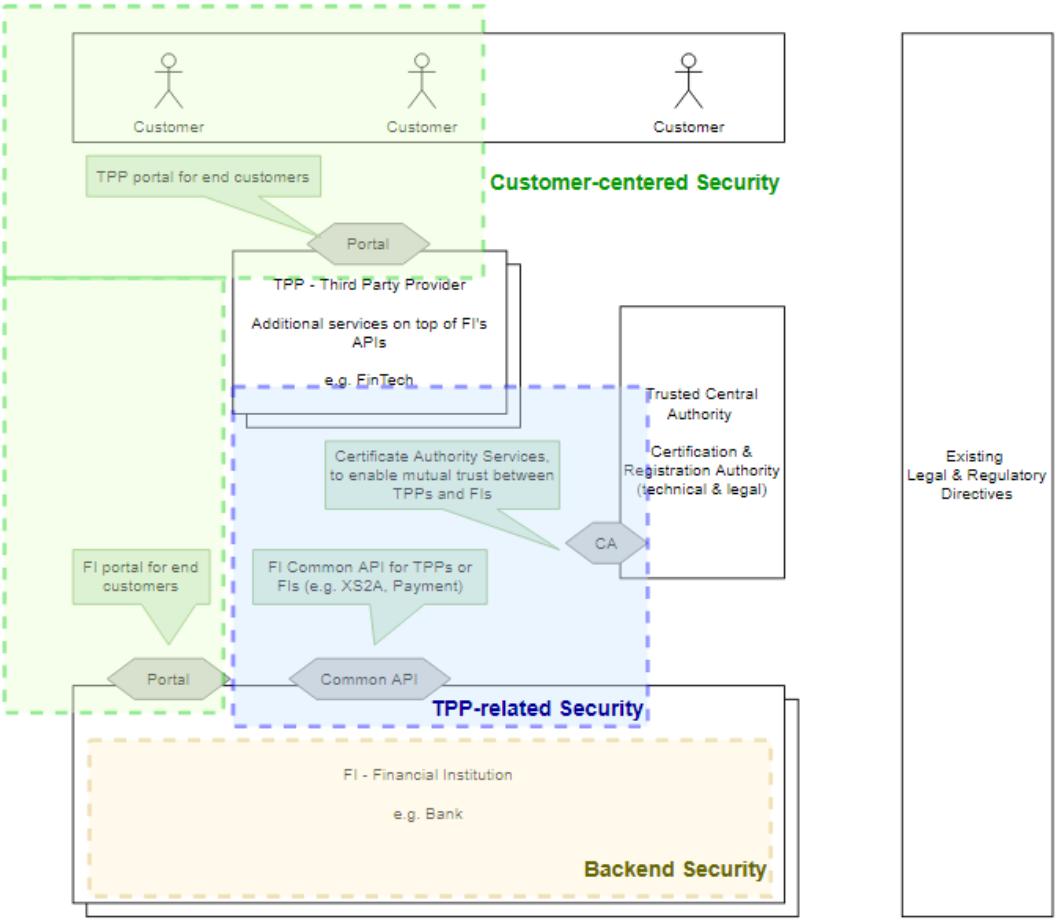
3. Definition

3.1 What is API Security?

In short: API security addresses the protection of confidentiality, integrity, and availability of APIs respectively the corresponding services and information.

It consists of the following elementary aspects, all of which are equally important:

- Secure Communication
- Backend Security
- Customer-centered Security
- TPP-related Security



Remark: For simplicity, Backend Security is only shown for FI in the picture. But of course, Backend Security is an important element for the other entities as well.

In the following sections, we will focus on the API security type where there is a triangular relationship between customer, TPP and FI. Each of the above mentioned aspects will be explored in detail, including a prioritization of the aspects outlined. The latter will also define the scope of this white paper.

3.1.1 Secure Communication

This topic is already best standardized and well documented. As part of the general IT infrastructure, it does not offer a significant choice of means and methods. Therefore, it will not be considered further.

3.1.2 Backend Security

This topic is part of the IT security architecture of the respective company. The concepts e.g. for securing core systems or middleware will therefore also not be considered further.

3.1.3 Customer-centered Security

This part of API security is specifically aimed at end users. It is directly linked to the use of the respective API-based services and is therefore a central part of the considerations in this document. In addition to ensuring the highest possible level of security, ease of use is an important prerequisite in the further considerations.

3.1.4 TPP-related Security

Last but not least, the topics of trust and security related to external access of API based services will be addressed. Thereby, it is useful to distinguish between three scenarios:

1. **Cross-bank scenarios**
   Here, API use is limited to financial institutions that are registered participants in a dedicated ecosystem. Basically, this is a special form of the 2nd scenario. But in contrast to that scenario, trust is not an issue here, as each participating financial institution is already certified by the national regulatory authority. However, a coordinated, cross-bank concept for API security must be developed.

2. **Other TPP scenarios**
   In this scenario, TPPs that are not financial institutions (e.g., FinTechs) access APIs of the financial institution. Here, a distinction must be made between a TPP that is already known to the financial institution and access of unknown origin.

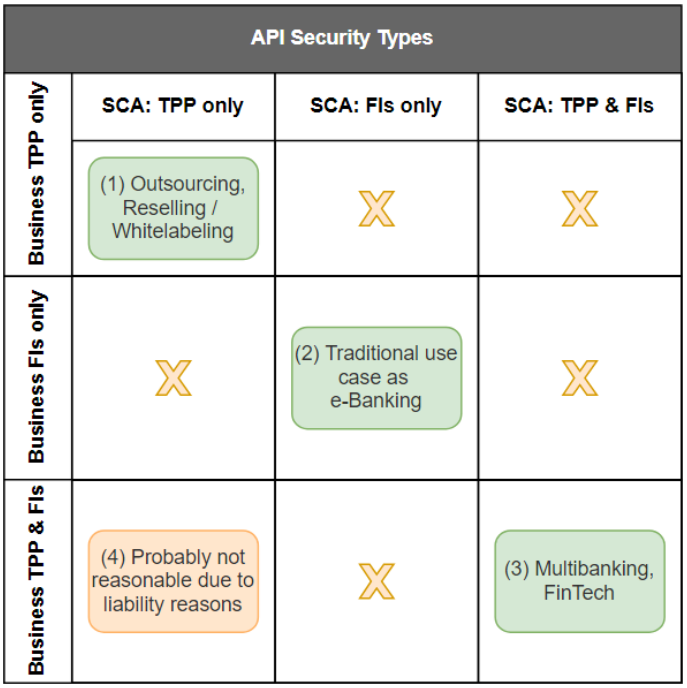
3. **Intermediary-based scenarios**
   Finally, there is the possibility of an intermediary taking on the role of a hub through which banks and third-party providers connect with each other. A typical example of such an intermediary is the bLink platform of SIX.

3.2 Types of API Security

Depending on the respective area of application, different types of API security with different key aspects are relevant.

The following is an outline based on the Business Relationship and Strong Customer Authentication (SCA) requirements between the customer, TPP and FIs.

- **Business Relationship**: Does the customer have a direct business relationship to
    - **TPP only**: e.g. customer has an account @ TPP only
    - **FIs only**: e.g. customer has an account @ FIs only
    - **TPP & FIs**: e.g. customer has an account @ TPP & FIs
- **Strong Customer Authentication**: Towards whom is strong authentication needed
    - **TPP only**: SCA towards TPP only
    - **FIs only**: SCA towards FIs only
    - **TPP & FIs**: SCA towards TPP and FIs



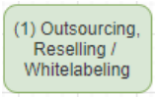
3.2.1 In focus

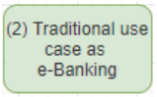
This paper focuses on the most sophisticated API security type where there is a triangular relationship between customer, TPP and FI (= Business Relationship & = SCA for both required).

This is the case, for example, with multi-banking or if a FinTech (TPP) provides aggregator services.

3.2.2 Not in focus

To keep the scope of this white paper manageable, the following types are not in focus.

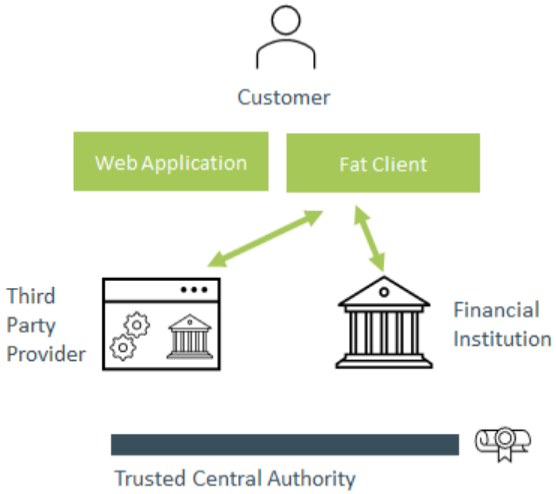




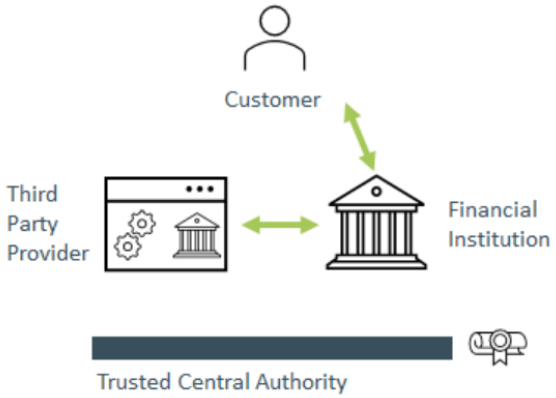
Use cases in which no TPP exists **(2)** or no authentication and authorization from the customer towards the FIs is needed **(1)**.

Examples:

- EBICS based corporate customer use cases.
- API security related to use cases where the customer runs software on premise to connect directly to a FI or a TPP.



- An insurance company offers its own products white labelled to bank customers. Insurance has no information about product customers except the business reference.



The above delimitation does not mean that these aspects are not addressed elsewhere in the context of API standardisation.

3.3 Strong Customer Authentication

SCA is not a standardized term but is mostly referred to the following core requirements:

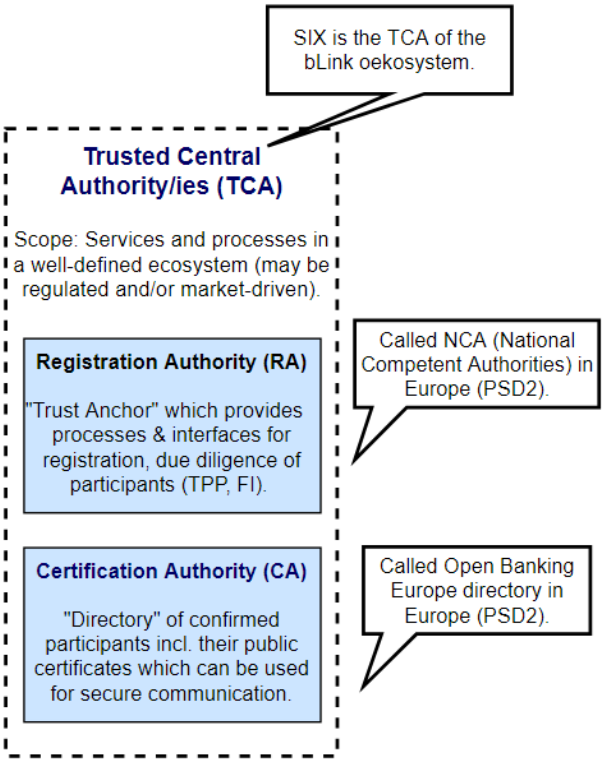
- Users must authenticate with at least two factors (something you know, something you have, something you are).
- Each sensitive action has to be legitimated by an authentication mechanism (derived from the above authentication) which is cryptographically linked to the essential details of the action: e.g., payment amount, origin-URI.

Strong Customer Authentication thus primarily addresses customer-centered security and TPP-related security. Of course, secure communication and backend security must also be guaranteed.

Remark: Many regulations or standards require adequate and state of the art security mechanisms to secure sensitive information. This includes certainly also secure authentication for customers. The PSD2 regulation (scope: EU) is more precise and requires strong customer authentication where a player accesses accounts, initiates payments or carries out any action which may imply a risk of fraud or abuse. See chapter *5. Legal & Compliance Requirements* for more details.

3.4 Trusted Central Authority (TCA)

In any digital service ecosystem with a (more or less) dynamic number of participants, a Trusted Central Authority (TCA) is needed. This central authority ensures that the rules of the game are defined on the one hand and complied with on the other. By trusting this central authority, collaboration aspects can be centrally facilitated, since otherwise peer-to-peer (everyone with everyone) negotiations, clarifications, coordination, etc. would be necessary.



The TCA must serve the following two roles:

- **Registration Authority (RA)**: Processes & interfaces for registration, due diligence of participants (TPP, FI)
- **Certification Authority (CA)**: Directory of confirmed participants incl. their public certificates which can be used for secure communication

These two roles can be assumed by a single entity or by different entities.

Examples

- CH / bLink ecosystem: SIX takes on both roles.
- EU / PSD2 ecosystem: The RA is called “Open Banking Europe Directory” and the CA “NCA - National Competent Authorities”.

3.4.1 Registration Authority (RA)

The registration process to onboard new FIs and TPPs has two main aspects:

- Due Diligence based on regulations: Who can participate in the financial ecosystem?
- Processes to apply for technical certificates.

Resulting requirements:

Topic	**Requirements**
Registration Process	● Portal with all relevant information for the registration process (accreditation request) ● Processes to handle the accreditation requests (provide support, process requests, …)
Due Diligence	● Verify compliance of requested parties to relevant requirements and policies ● (technical, legal, …) ● Ensuring periodical reviews

3.4.2 Certification Authority (CA)

The CA's main duty is to manage directory information needed to establish a trust and a secure communication between FIs and TPPs:

- **Manage Certificates and Keys**: The ability to upload, manage and remove certificates. The ability to issue, manage and revoke certificates.

- **Manage and Provider Directory Information**: The ability to update and find information maintained in the Directory - either through APIs and / or a self-service user interface (UI) delivered as a web application.

Resulting requirements:

Topic	**Requirements**
Certification Signing	● Signing of the public certification of the parties involved
Directory	● Directory of confirmed participants incl. their public certificates which can be used for secure communication

3.5 International overview

3.5.1 European Union

The second Payment Services Directive (PSD2) offers many FinTechs high growth potential. But with the opportunities also come challenges. For the first time, payment service providers that access sensitive user information are subject to government regulation. To use the banks' interface (API), they need a license from their financial regulator.

In Germany, for example, this licensing is done by BaFin (https://www.bafin.de). The corresponding requirements are based on a law named "*Gesetz über die Beaufsichtigung von Zahlungsdiensten*" (https://www.gesetze-im-internet.de/zag_2018/). D-TRUST (https://www.d-trust.net), a company of *Bundesdruckerei* is currently the only German provider listed in the *EU Trusted List* as a so-called *Qualified Trust Service Provider* authorized to issue QWACs[2] and QSeals[3]. D-TRUST was also the first company in Europe to offer qualified certificates.

3.5.2 UK

A binding prerequisite for providing or participating in Open Banking services in UK is to possess the required regulatory permission from the FCA[4]. Getting regulated is a detailed process of due diligence. For example, the applicant has to prove to the FCA (or European Equivalent) that it has a PSD2-compliant business model and appropriate data privacy and security measures in place.

Checklist for getting a permit by the FCA:

- **FCA guidance** – Make sure you have read the FCA's guidance. Chapter 3 provides information about authorisation and registration.
- **Know your regulatory definitions** – are you offering an Account Information Service (AISP), a Payment Initiation Service (PISP) – or both? It's really important to be clear about how your service fits the regulatory definitions.
- **Show a clear business model** – you'll submit details of the service you want to provide in the application. Make sure it includes clear and simple explanations of the business model and typical transactions.
- **Policies and procedures** – make sure you have in place all of the policies and procedures that being regulated requires.
- **Compliance** – you'll need to demonstrate how your security, data storage, IT and policies comply with the relevant regulations.
- **Insurance** – you must have professional indemnity insurance that complies with the regulations.

[2] A qualified website authentication certificate (QWAC certificate) is a qualified digital certificate under the trust services defined in the eIDAS Regulation.
[3] Qualified certificate for electronic seals (QSeal certificate)
[4] https://www.fca.org.uk/firms/applications-under-psd2

3.5.3 Australia

Only providers accredited by the *Australian Competition and Consumer Commission* (ACCC - https://www.accc.gov.au) can offer services using *Consumer Data Right*.

To become accredited, applicants must demonstrate that they:

- are a fit and proper person/organisation to manage Consumer Data Right data
- have taken steps to adequately protect data from misuse, interference, loss, unauthorised access, modification or disclosure
- have internal dispute resolution processes meeting the requirements of the Consumer Data Right Rules (for banking, this means their processes must comply with provisions of the Australian Securities and Investments Commission's Regulatory Guide 165 *Licensing: Internal and external dispute resolution*)
- belong to a relevant external dispute resolution scheme
- have adequate insurance to compensate Consumer Data Right consumers for any loss that might occur from a breach of the accredited data recipient's obligations
- have an Australian address for service.

4. Use Cases

4.1 API Sec related Use Cases

4.1.1 Overview

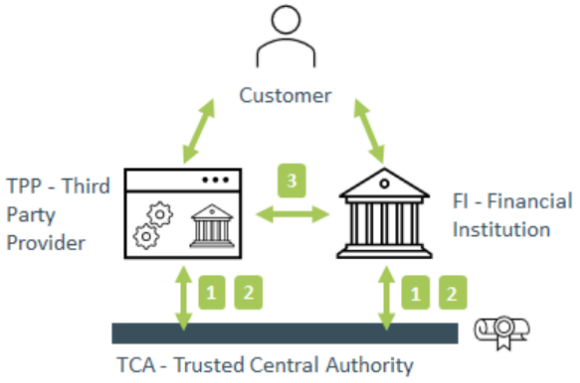
There are five basic use cases related to API security that should be considered:

- Establishment trust relationship and secure communication between FI and TPP (with help of the TCA)
- Initial consent of a customer to share information between a TPP and an FI
- FI/TPP data exchange **with** additional authorization by the customer
- FI/TPP data exchange **without** additional authorization by the customer
- FI/FI consent & data exchange: Same flow as for FI/TPP (a second FI takes the role of the TPP). e.g. for Multibanking use cases

The first use case is relevant for each TPP/ FI double, the remaining four use cases for each Customer / TPP / FI triple.

4.1.2 Establish trust relationship and secure communication between FI and TPP

With the help of the central authority, FIs and TPPs can establish a business relationship and a trust, respectively. This is done by the central authority using due diligence to check conformity with defined criteria (legal, technical, etc.). Commercial conditions can also be predefined.

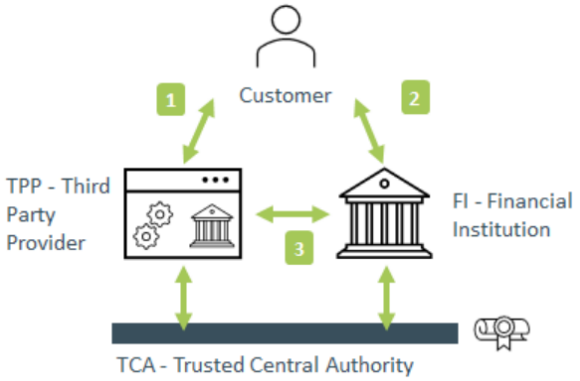


1. FI and TPP register themselves at the TCA (by fulfilling certain criteria)
2. FI and TPP make a secure lookup at TCA to identify each other
3. FI and TPP establish a secure communication

4.1.3 FI/TPP initial consent

After the secure communication respectively the trust between the TPP and the FI has been established, an initial consent has to be done for each customer, TPP, FI triple. This usually takes place when the customer in the TPP or in the FI requests the connection to the FI or TPP respectively (e.g. customers account information from the FI shall be displayed in the TPP).

This initial consent is usually valid for a longer time period (or until revocation) and therefore suitable for less critical use cases such as read access to account data.

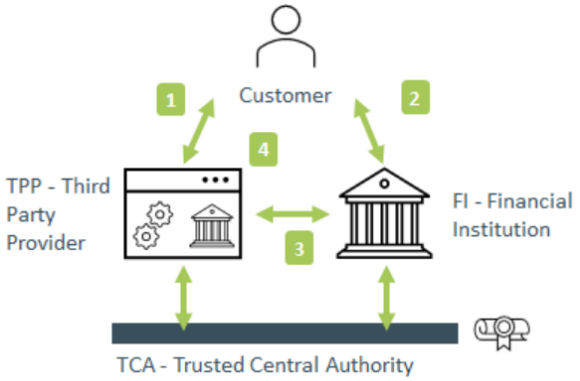


Precondition: «Establish FI/TPP secure communication»

1. Customer login to TPP and selection of FI for initial consent (e.g. account list)
2. Redirected customer login to FI and approval of initial consent
3. TPP gets a (long life) access token

4.1.4 FI/TPP data exchange with additional authorization

If the initial consent is not sufficient for the requested action, e.g. for a payment initiation, an additional authorization (at the FI) of the customer will be necessary to perform the action.



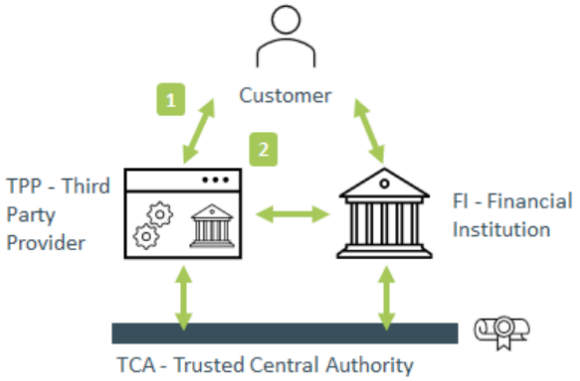
Precondition: «Establish FI/TPP secure communication» & «FI/TPP initial consent»

1. Customer login to TPP and wants to do a financial use case which needs an additional authorization (e.g. initiate payment)

2. Redirected customer login to FI and approval the additional scope
3. TPP gets an access token for the required financial use case
4. TPP executes the financial use case with the received access token and shows the result to the customer

4.1.5 FI/TPP data exchange without additional authorization

If the initial consent is sufficient for the requested action, e.g. account list, the action can be executed without any additional authorization (at the FI) from the customer.



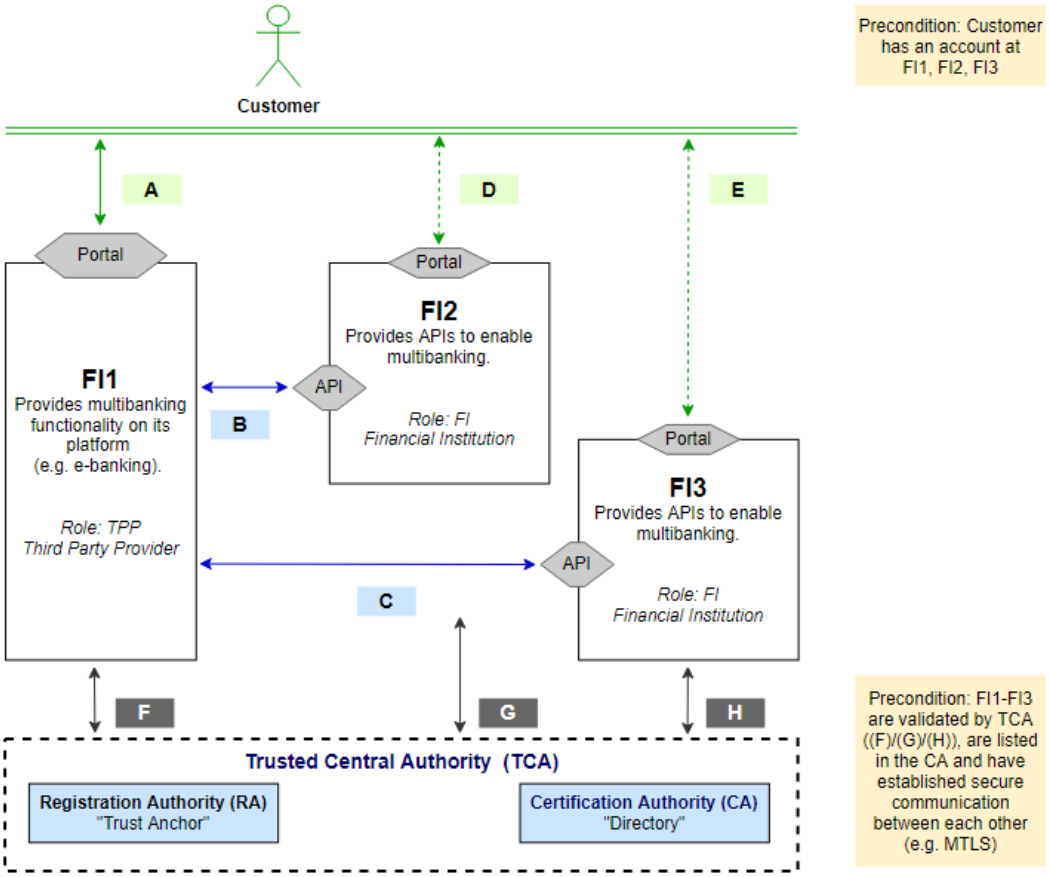
Precondition: «Establish FI/TPP secure communication» & «FI/TPP initial consent»

1. Customer login to TPP and wants to do a financial use case which doesn't needs an additional authorization (e.g. account listening)
2. TPP executes the financial use case with the existing access token from the initial consent and shows the result to the customer

4.2 Business Use Cases

The following subsections show some examples of business use cases.

4.2.1 Multibanking



The process of Initial Consent / Mapping comprises the following steps:

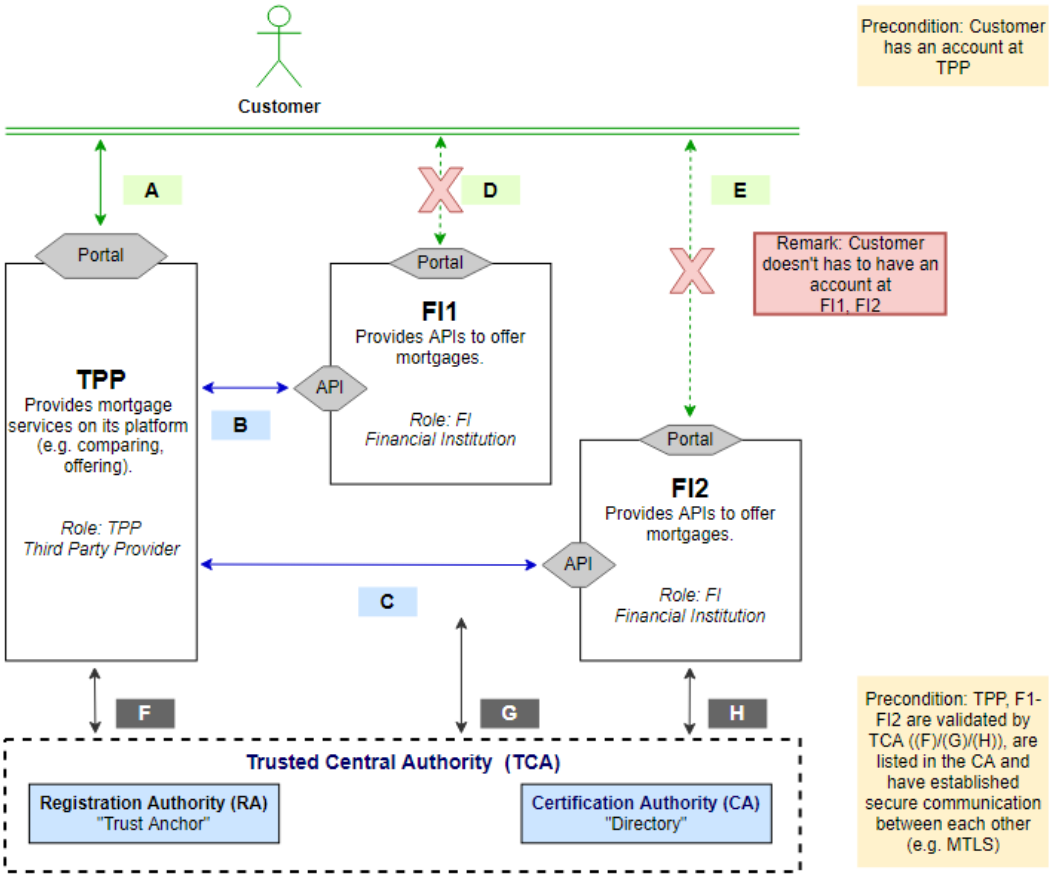
1. **(A)** The customer authenticates himself securely to the FI1 portal (SCA).
2. The customer wants to add additional FIs to his e-banking.
3. **(F)** FI1 checks the directory for available FIs to add and shows the result to the customer.
4. The customer chooses the FIs to add (& where he has an account already).
5. For each choosen FI to add (here on the example FI2)
    a. Customer has to give his consent to FI1 for adding FI2 ("I'm aware of the risks" etc.)
    b. **(B)** FI1 initiates the mapping to FI2 based over APIs
    c. **(D)** Customer is redirected to FI2 to authenticate (SCA) and to give his consent to FI2 ("I'm aware of the risks and want to add account X" etc.)
6. The customer can use multibanking

The actual use of multibanking services works as follows:[5]

1. **(A)** The customer authenticates himself securely to the FI1 portal (SCA).
2. The customer has access to his accounts and services of FI1 as well as to mapped accounts and services of FI2 & FI3 over secure APIs **(B)** **(C)**.
3. Some sensitive actions for the mapped accounts and services of FI2 & FI3, MAY initiate an additional approval request over secure channels **(D)**, **(E)** (e.g. transaction signing)
4. From time to time (to be defined) the customer has to reapprove the consent / mapping of the FI2, FI3 integration **(D)**, **(E)**.

Remark: The rules on whether an action requires additional approval are defined by the assigned FIs based on their risk policy.

4.2.2 Mortgages



The actual use of mortgage services works as follows:

1. **(A)** The customer authenticates himself securely to the TPP portal (SCA).
2. The customer enters all the necessary information into the TPP portal, which is required for the requested service (offer, prolongation).
3. The TPP obtains the necessary information from the connected FIs via the APIs **(B)** **(C)** for the services requested by the customer.

[5] Assumption: The customer initiated multibanking FI1 for FI2 & FI3.

5. Legal & Compliance Requirements

5.1 Anti Money Laundering (AML)

Description:

Under the Swiss Criminal Code money laundering is defined as any act "that is aimed at frustrating the identification of the origin, the tracing or the confiscation of assets which, as the perpetrator knows or must assume, originate from a felony" (Art. 305bis SCC); English translation). This includes any act which conceals or disguises assets of criminal origin or assets that have been obtained through serious crime. The perpetrator's aim is to give the impression that the funds have been obtained legally. This act of disguise occurs in the legal financial market through all sorts of investment activities. The originally "dirty" money is thus "laundered" and can enter normal circulation within legal trading circles.

Combating money laundering is an important part of the overall fight to thwart drug dealing, organised crime and, since a number of years, also against terrorist financing. The extensive data that is required to be collected and stored for the purpose of combating and prosecuting money laundering, has proven useful for investigations into terrorist activities; for this reason, the original regulations governing the fight against money laundering are also applied today, in a slightly adapted form, in countering terrorist financing. In the international context, the terms AML/CFT Regulations (Anti-Money Laundering / Countering the Financing of Terrorism) have therefore emerged becoming the current technical term among experts.

As the laundering of money most often takes place in another country compared to where the predicate offence was committed, it is important that the fight against money laundering is internationally coordinated in order to close loopholes, as far as possible, in regulations or in criminal prosecution law. This requires national regulations that are comparable and consistent with each other. In order to achieve this, international, multilateral standards have been drawn up to provide the foundation for national regulations.

Scope:

CH

Source:

https://finma.ch/FinmaArchiv/gwg/e/themen/bekaempfung/index.php

5.2 Financial Market Infrastructure Act, FinMIA

Description:

This Act governs the organisation and operation of financial market infrastructures, and the conduct of financial market participants in securities and derivatives trading.

It aims to ensure the proper functioning and transparency of securities and derivatives markets, the stability of the financial system, the protection of financial market participants and equal treatment of investors.

Scope:

CH

Source:

https://www.admin.ch/opc/en/classified-compilation/20141779

5.3 FinSA, FinIA, FinSO

Description:

On 15 June 2018, Parliament adopted the Financial Services Act (FinSA) and the Financial Institutions Act (FinIA). FinSA contains code of conduct provisions with which financial service providers must comply vis-à-vis their clients. FinIA essentially standardises the authorisation rules for certain financial institutions. On 6 November 2019, the Federal Council, by issuing the Financial Services Ordinance (FinSO), the Financial Institutions Ordinance (FinIO) and the Supervisory Organisations Ordinance (SOO), also issued the implementing provisions for FinSA and FinIA. These will come into force at the same time as FinSA and FinIA, on 1 January 2020.

Scope:

CH

Sources:

https://finma.ch/en/authorisation/fidleg-und-finig
https://www.admin.ch/opc/en/classified-compilation/20152661 (FinSA)
https://www.admin.ch/opc/en/classified-compilation/20152662 (FinIA)
https://www.admin.ch/opc/en/classified-compilation/20192374 (FinSO)

5.4 PSD2 - Revised Payment Services Directive

General Provisions

This Regulation establishes the requirements to be complied with by payment service providers for the purpose of implementing security measures which enable them to do the following:

A. apply the procedure of **strong customer authentication** in accordance with Article 97 of Directive (EU) 2015/2366;

B. exempt the application of the **security requirements** of strong customer authentication, subject to specified and limited conditions **based on the level of risk, the amount** and the **recurrence** of the payment transaction and of the **payment channel** used for its execution;

C. protect the **confidentiality and the integrity** of the payment service user's personalised security credentials;

D. establish **common and secure open standards for the communication** between account servicing payment service providers, payment initiation service providers, account information service providers, payers, payees and other payment service providers in relation to the provision and use of payment services in application of Title IV of Directive (EU) 2015/2366.

PSD2 SCA Considerations

Article 4 - Definitions.
(30) ‘strong customer authentication’ means an authentication based on the **use of two or more elements** categorised as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data;

Article 74 - Responsibility
Where the payer’s payment service provider does not require strong customer authentication, the payer shall not bear any financial losses unless the payer has acted fraudulently. Where the payee or the payment service provider of the payee **fails to accept strong customer authentication, it shall refund the financial damage** caused to the payer’s payment service provider.

Article 97 - Authentication
1. Member States shall ensure that a payment service provider applies **strong customer authentication** where the payer: **(a) accesses** its payment account online; **(b) initiates** an electronic payment transaction; **(c) carries out any action** through a remote channel which may **imply a risk** of payment fraud or other abuses.

Scope:

EU

Sources:

PSD2 Directive (EU) 2015/2366:
https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32015L2366

Commission Delegated Regulation regarding regulatory technical standards (RTA) for strong customer authentication and common and secure open standards of communication:
https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32018R0389

5.4 GDPR

Description:

The General Data Protection Regulation (GDPR) is the toughest privacy and security law in the world. Though it was drafted and passed by the European Union (EU), it imposes obligations onto organizations anywhere, so long as they target or collect data related to people in the EU. The regulation was put into effect on May 25, 2018. The GDPR will levy harsh fines against those who violate its privacy and security standards, with penalties reaching into the tens of millions of euros.

Scope:

EU (will be adapted in the revised DSG CH)

Source:

https://gdpr.eu

6. Implementation View

6.1 Standards

6.1.1 OAuth 2.0

OAuth 2.0 (Open Authorisation) is the name of an open protocol that allows standardised, secure API authorisation for desktop, web and mobile applications. It was published in 2012 by the IETF (Internet Engineering Task Force).[6]

With the help of this protocol, an end user (aka *User* or *Resource Owner*) can allow an application (aka *Client* or *Relying Party*) to access his data provided by another service (aka *Resource Server*) without revealing secret details of his authentication to the client.

The end user can thus allow third parties to use a service on his behalf. Typically, this avoids the transmission of passwords to third parties.

Many open banking initiatives are already focusing on **OAuth 2.0** based flows, where the end customer is redirected to the FI for authorization and authorization (Redirected SCA Approach).

OAuth 2.0 can be individually secured by selecting or prohibiting specific parameters (e.g. encryption algorithms). Further, individual extensions are often built around **OAuth 2.0** to mitigate specific attack vectors.

Consent 2.0 from bLink, for example, is based on **OAuth 2.0** with individual extensions based on the identified attack scenarios.

6.1.2 OpenID Connect

OpenID Connect (OIDC) is an authentication layer based on the authorization framework **OAuth 2.0**.

OpenID Connect is a layer above the **OAuth** framework that allows clients on the one hand to verify the identity of a user with the help of an authorization server and on the other hand to obtain basic profile information in an interoperable way.

Technically formulated, **OpenID Connect** specifies an HTTP programming interface with REST mechanisms that uses the JSON data format.

[6] See OAuth 2.0 specifications for details: https://oauth.net/2

6.1.3 Financial-grade API (FAPI)

FAPI is an initiative of the OpenID foundation which is also responsible for **OpenID Connect**. **FAPI** is hardening the basic / regular **OAuth 2.0** standard to be suitable for high-risk use cases. This is accomplished by adding restrictions, defining mandatory data, parameters - e.g. *always https*.[7]

Knowledge and protocols that are developed in the context of the FAPI initiative are already included as substandards in OAuth, e.g., OAuth Token Binding.

The API Security approach consists of three layers

(*Security logic only:*)

1. Foundation Standard: OAuth 2.0 / OIDC
2. Hardening: FAPI Profile

(*Security & Business logic:*)

1. Customizing: Common API Profile

As API Security relies on keys / certificates, a trusted Central Authority is needed (for Certification Handling and Request Authority).

[7] See FAPI specification for details: https://fapi.openid.net

6.2 Solutions

6.2.1 Existing Platforms and Implementations

- EU: SCA with 3 variants (embedded, redirect, decoupled)
- (EU), UK, Australia, Japan, Brazil, Mexico: FAPI
- CH: bLink platform based on OAuth 2.0

6.2.2 Service Providers - API Security Components

In April 2021, the mayor Swiss providers for security software

- Ergon (Airlock)
- Nevis Security (Nevis Platform)
- United Security Providers (Secure Entry Server)

were asked to outline their roadmaps towards future API Security capabilities.

As a further development or refinement of OAuth 2.0, all companies indicated that they are (technically) ready to support FAPI, but are still waiting for clearer signals from the market (market adoption).

An international list of Certified Financial-grade API (FAPI) OpenID Providers can be found at the website of the OpenID Foundation: https://openid.net/certification/#FAPI_OPs. Current status:

- 35 deployments for FAPI conformance profiles
- 3 deployment for FAPI Client Initiated Backchannel Authentication Profile (FAPI-CIBA) conformance profiles

6.3 Recommendations

6.3.1 Dependencies to international initiatives

The question of the extent to which the Swiss banking centre can decouple itself from international developments in the long term could not be finally clarified. Therefore and in view of the clear preferences from the bank side, all those present eventually welcomed the pragmatic approach of taking the steps towards the planned multi-banking MVP with bLink, monitoring the international efforts in parallel and, if necessary, reviewing the chosen procedure again at a later date.

6.3.2 Legal

It was found that the assessment of the possible technological solution architecture alone is not adequate. In addition, the specific requirements of the Swiss market in terms of business needs and legal as well as regulatory requirements must be taken into account.

Furthermore, the fact that in Switzerland, in contrast to, e.g., the EU, no regulatory rules determine the implementation of open banking also means that the rather costly EU setup is not necessarily the first and only choice here.

6.3.3 Initial Multibanking Proposition

On the question of how the multi-banking MVP should be implemented with regard to API security in concrete terms, SFTI members diverged into two factions:

- Many bank representatives preferred the platform approach of bLink, with the majority of them already having previously established a bLink connection.
- Others pointed out that a scenario where a central platform as an operative intermediary is necessary would not fit to an internationally compatible approach.

6.3.4 Trusted Central Authority

In the context of FAPI, the role of a Trusted Central Authority was also discussed. The role of trusted central authorities is essential, e.g. in the area of PSS2 validity. In this part of Europe, TCAs are a core element when it comes to bringing Open Finance to life.

However, since there are no corresponding regulatory requirements in Switzerland, a model without TCAs is beginning to gain acceptance. It is based on the use of SIX's bLink platform, which implicitly performs the essential duties of a TCA, among other tasks.

As a consequence, there is no TCA in Switzerland, although besides SIX also companies such as SwissSign, Swisscom or Swiss Post could perform this role. However, as long as the use of the bLink platform remains the dominant model in Open Finance in Switzerland, there is no need for a TCA - at least not in the banking environment.

7. Outlook

The API security and consent management considerations in this white paper focus primarily on retail and micro-business (SMB) clients. For companies with multiple employees or for constellations where a user has roles in multiple companies, however, elementary additional questions arise, such as:

- On the client side, who is entitled to enable the interface on behalf of the company at all?
- At what level (employee vs. company) should API unlocks be managed?
- What happens to the Bank<->TPP connection if the user who made the original activation leaves the company or gives up their e-banking account?
- For transactions where something is "delivered" to the bank via the API (e.g. payment proposals), what should be the "origin" of such data: The identity of the person who established the connection, or a generic identity of the company, or what else?

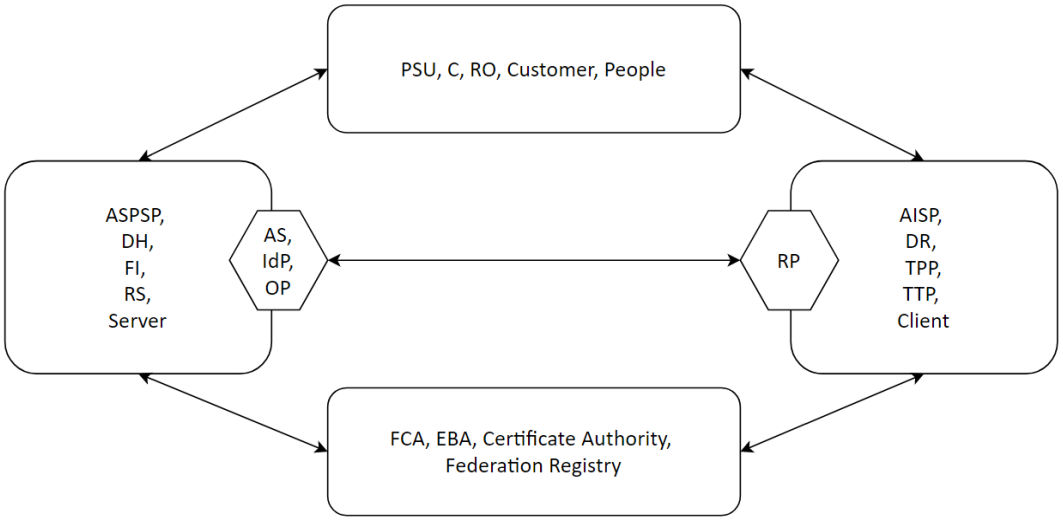
By addressing such and other challenging questions regarding API security and consent management for business customers as concretely as possible, a significant added value could probably be created.

As a possible template, the EBICS specifications could be used. There are at least some technical answers to the questions mentioned, e.g. by differentiating between different signature classes for dedicated authorization levels, and more or less explicitly distinguishing between situations with Corporate Seal and those with Distributed Electronic Signature.

On the other hand, there would still be a considerable amount of work involved in addressing these issues, and that would be beyond the scope of this white paper. At this point, only the urgent hint can be given to investigate this topic in more detail in a follow-up activity.

Appendix

A.1 Glossary



Abbreviation	**Explanation**
AISP	Account Information Service Provider
ASPSP	Account Servicing Payments Services Providers
AS	Authorization Server
C	Consumer
CIBA	Client Initiated Backchannel Authentication
DH	Data Holder
DR	Data Recipient
EBA	European Banking Authority
FAPI	Financial-grade API
FCA	Financial Conduct Authority
FI	Financial Institute
IdP	Identity Provider
JWT	JSON Web Token
JWK	JSON Web Key

JWKS	JSON Web Key Sets
OB	Open Banking
OIDC	OpenID Connect
OP	OpenID Provider
PSU	Payment Service Users
RO	Resource Owner
RP	Relying Party
RS	Resource Server
TPP	Third Party Providers
TTP	Trusted Third Parties