We build the BEST digital identification and signature services in Europe.

Swisscom Trust Services

White Paper

The new "Smart Registration & Signing Service"
A smile is all it takes to sign electronically.

Status April 2024

Contents

_

Swisscom Trust Services

Introduction

Electronic signatures offer significant advantages, such as time and cost savings when signing documents. However, several challenges can make their use more difficult. One of the major hurdles is the identification and authorization of the signature, which is often perceived as tedious and can be an obstacle to the use of electronic signatures.
In the past, there were several obstacles associated with electronic signatures, such as

- offline registration,
- long waiting times for video identification, and the need to download additional apps for identification.
- The process of approval of the signature often involved the use of a password, a one-time code text message, or a signature approval app, which could be unreliable in certain situations.
- Moreover, the complex registration process often kept the signature process separate from the actual registration, making it necessary to ensure correct identification at the beginning of each signature process.

To address these challenges, an ideal electronic signature process should be as simple as signing by hand, with a comprehensive and seamless process that accompanies the signatory from registration to the signature, without the need for additional installations or disruptions.

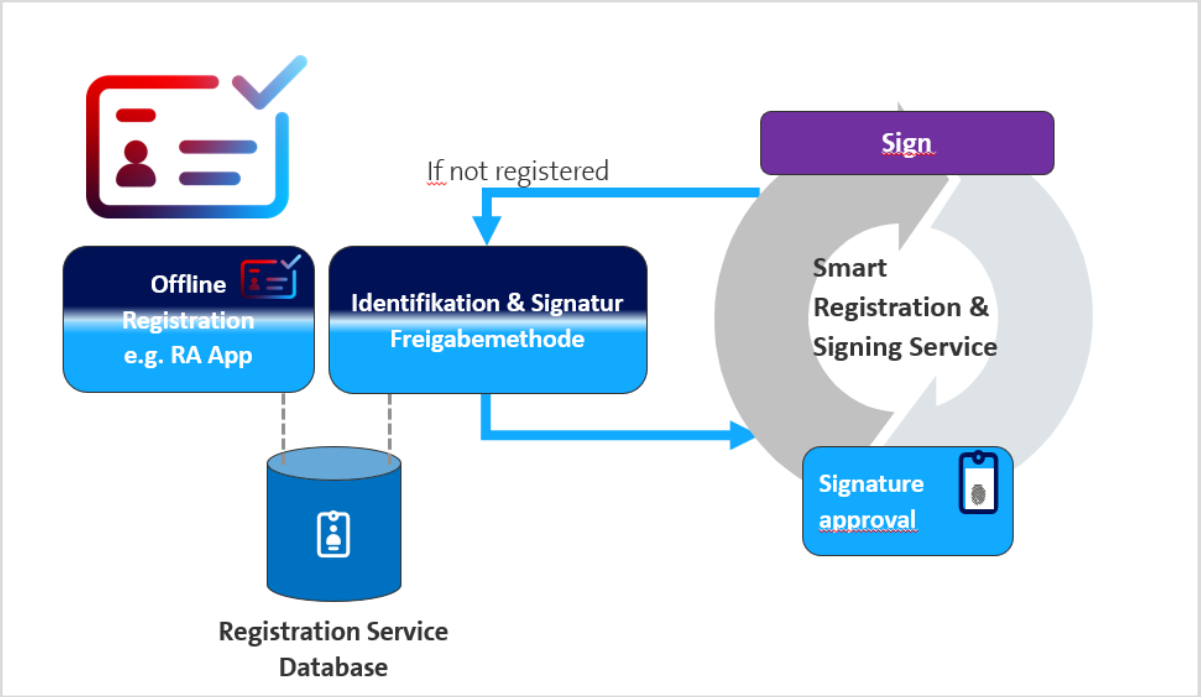


Figure: Standardised process for registration and signature

With the broker-controlled Smart Registration & Signing Service, Swisscom Trust Services offers a flexible solution for an optimized user experience. The focus is on simplifying the registration and identification process, integrating existing biometrics/login procedures, and reducing the effort required for audits. By relying on open standards and standardizing interfaces and processes, the service aims to make it easier for partners and customers to integrate or change modular functions.

The focus is in detail on the following aspects:

- Registration and identification are now considered a seamless process. This means that if registration has already been completed and repeated signatures are required, the process can be considerably simplified / shortened.
- We use existing biometrics/login procedures or installed apps on the signatory's PC or mobile device to avoid app installations and context switches as far as possible.
- We integrate customer- or partner-specific identification and IDP solutions and at the same time reduce the effort required for audits when integrating with the recognised Swisscom signature.
- We consistently rely on open standards such as OIDC, PAR, CIBA and the ETSI interface 119432 for remote server signing. Investments in proprietary interfaces are no longer necessary.
- Standardising interfaces and processes makes it easier for partners and customers to integrate or change modular functions. For example, the integration of additional identification procedures or functionalities.
- By using the broker, business processes and the guided signature experience no longer have to be modelled on the partner side based on requested statuses. The open interfaces make it possible to embed broker decisions directly into the partner's user experience (UX).

Process silos

As previously mentioned, today's processes still suffer from silos. For instance, the registration process and the signature process are separate, with the latter only occurring after the completion of registration.

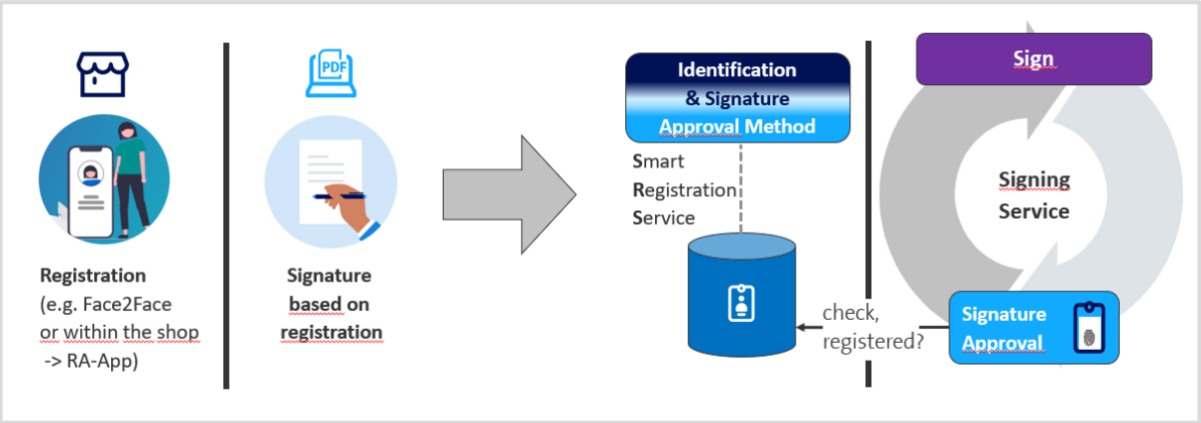


Illustration: The historically separate process of registration and signature

The historical separation of these processes can be attributed to the fact that, for a long time, Face2Face identification was the sole option for registration, and even until 2022, it was the only option for non-banks in Switzerland. Additionally, in some EU countries, remote identification procedures for trusted services are only temporarily authorized.
Subsequently, problems with user guidance arise during the signing process. For example, if it is discovered that the registration was unsuccessful or is no longer valid (e.g., due to the expiration of the ID card or the invalidation of the certificate), the signatory must return to the registration process. This situation is akin to having to buy a new pen when signing by hand. Furthermore, with pan-European services such as Swisscom's signature service, a registration may be valid for the EU but not in Switzerland due to different regulations. This highlights the increased complexity of user guidance when the processes are separated, given the different legal areas and their regulations for implementing electronic signatures.
From the signatory's perspective, a standardized process is crucial. The signatory desires to read and approve their document. Therefore, if they are unable to approve the document for any reason, such as being incorrectly registered or no longer validly registered, the (remote) re-registration should take place within the same process. This approach helps ensure that the signatory can always obtain the desired result of a digital signature in a simple and uncomplicated manner.

The advantage: A guided process instead of a process break!

Signature approval with existing means - the IDP

Many organizations, such as banks, have already registered and verified our data. We frequently use the banking app on our mobile phones or PCs, which these organizations can leverage to act as an Identity Provider (IDP). This collaboration allows for the identification and approval process, leading to an enhanced user experience.

The integration of existing apps on our mobile devices and the use of pre-existing identification data offers the advantage of saving time and effort. There is no need for re-identification, installing additional apps, or memorizing extra passwords. Such redundancies are undesirable for users and do not align with the seamless experience expected in the digital world.

In practical terms, we are already accustomed to third-party identification for numerous "logins.":

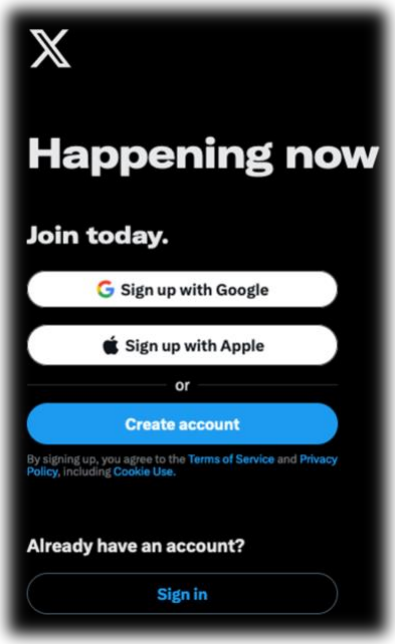


Illustration: Example of a standard market platform and different registration methods

And we are already familiar with the use of existing 3rd party payment services when paying:

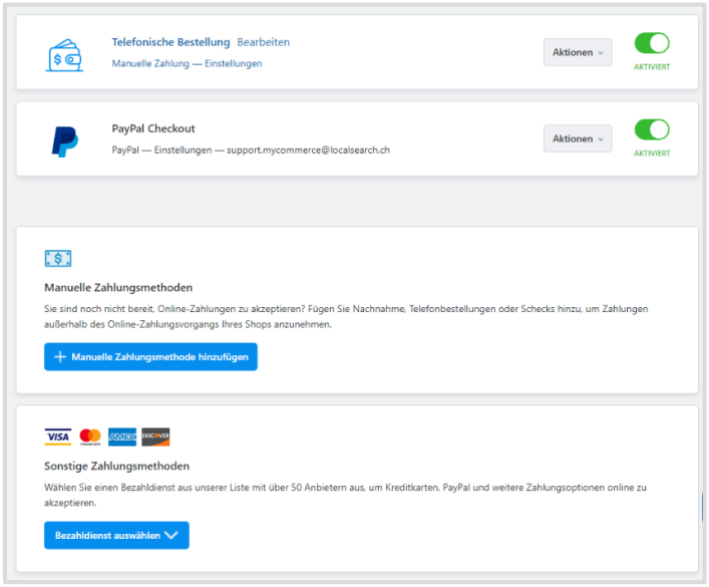


Illustration: Example of a standard market platform and different payment methods

The legislation on digital signatures permits the outsourcing of identifications and authorizations through delegations, such as the registration authority delegation (RA delegation), provided that all relevant legal and regulatory requirements are met. These are typically verified through initial and regular audits and approved for the trust service.
The Identity Provider (IDP) not only furnishes the identity but also facilitates the approval or authentication process, allowing the individual to confirm and authorize their signatures. For instance, in the banking sector, the online banking app often serves this purpose.
Similar to other web services, an IDP can offer alternative signature approval. For instance, within the e-banking app, which signatories are already familiar with, users may have to accept the terms of use for the first time only and can then electronically sign a document, as demonstrated by the integration of Postfinance.

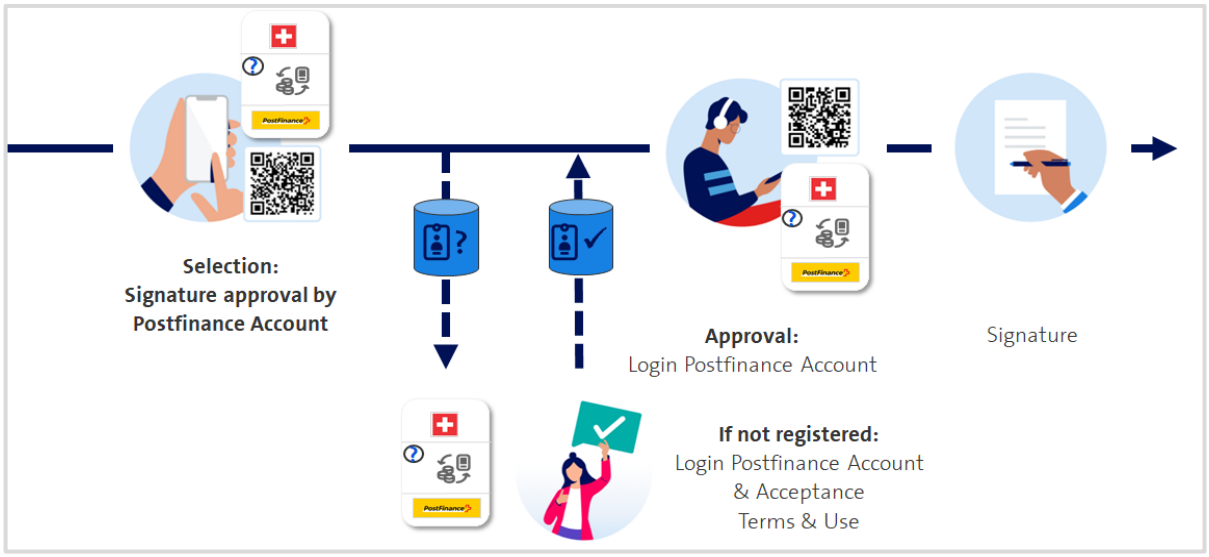


Illustration: Example integration of Postfinance Bank (CH) as IDP including your authentication

In a structured onboarding process, we assist all Identity Providers (IDPs) that comply with the regulations in transitioning to their new role as a registration and signature approval method. They can utilize this for their internal processes or offer their method to other participants via Swisscom, thereby generating revenue for registration or approval. A specially pre-audited Software Development Kit (SDK) also facilitates the integration of signature approval into the existing app, reducing audit costs. Additionally, organizations have the option to conduct a comprehensive audit of their own procedures.

Advantage: Don't install any additional apps, but use what you have and, above all, what you know - e.g. the familiar app from your bank
No additional registration procedure, no incorrect registration, no waiting time, fast and uncomplicated

Signature approval with existing means - Passkey

In the past, Swisscom's signature authorization methods were primarily limited to mobile phone-based procedures, such as the Mobile ID app or a combination of one-time passwords via SMS and a password. However, with the redesign of the Signing Service and the introduction of the interface in accordance with ETSI TS 119 432, along with the expansion of the Smart Registration Service to include an Authentication Broker, there are now fewer technical restrictions on the use of identification and authentication methods.
The adoption of the new FIDO2 standard, in conjunction with Passkeys (Passkey Authentication / fidoalliance.org), has made it possible to completely eliminate the need for app installation. This advancement allows for an even smoother process when registering and approving signatures.
Passkeys, defined by the FIDO Authentication Alliance, which includes companies such as Google, Apple, and Microsoft, have been heralded as the end of passwords. They offer a two-factor process that is already installed on most devices. For instance, when logging into a protected account, users are typically asked for a PIN, fingerprint, or facial recognition, which is also used to unlock the screen on their PC or mobile phone. This fulfills the regulatory requirement that qualified electronic signatures must be approved by two factors, such as possession and knowledge or possession and biometrics. Additionally, approvals are synchronized across multiple devices, including different ecosystems such as Apple and Google.

As a result, a trust service provider can now use these passkeys to request approval for a signature without the need to install an app. Approval can be as simple as using a biometric feature like a smile (FaceID) or a fingerprint

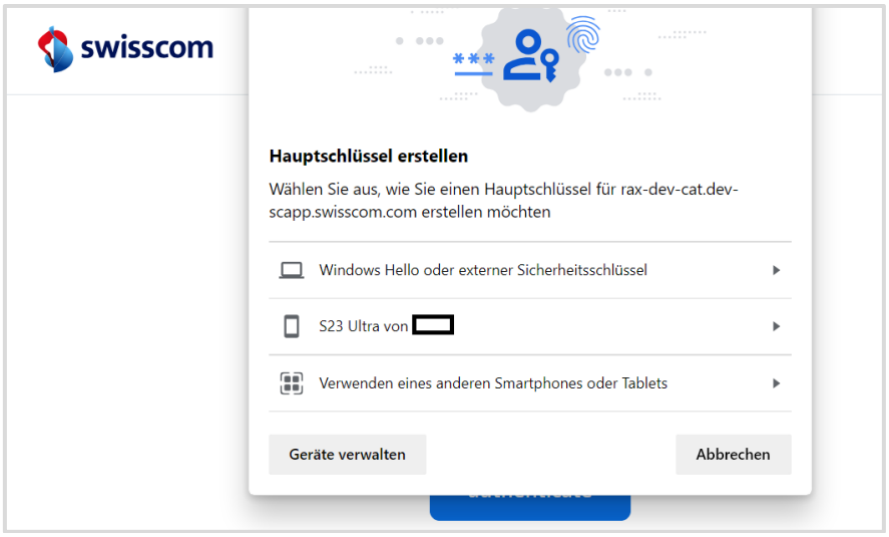


Illustration: Example of passkey approval in the flow

The introduction of Passkeys represents a significant advancement in authentication technology, offering a more secure and user-friendly alternative to traditional passwords and multi-factor authentication. This innovation aligns with the ongoing efforts to enhance the security and usability of digital authentication across various devices and platforms.

Advantage: No need to install an app, just use what the PC/mobile device already offers: Passkeys according to the FIDO standard!

The store concept

While it is possible in principle to designate a specific identification method as the registration method for signature applications and, if necessary, to define a fixed signature approval method, such as passkeys, in practice, the variety of options is much more beneficial. There is no one-size-fits-all solution.

In practical terms, this means that an inexperienced PC signatory may prefer to use operator-guided video identification, while a signatory who already possesses an ID card with an NFC chip may opt for identification via NFC, which is a faster process. Alternatively, their bank may already be authorized as an Identity Provider (IDP) for registration, enabling a quick login at the bank to handle the entire registration process.

Ultimately, the decision of what to offer signatories rests with our signature platform partner, the participant. Swisscom Trust Services will provide various "best-of-breed" procedures that are tested, regulated, and approved in so-called stores. These include video identification, auto-identification, NFC chip identification, bank account IDPs, and eIDs, allowing signatories to freely choose from the options offered. Conversely, the signature platform partner can also limit the selection or even favor a single procedure. The advantage here lies in the various modular solutions, options, and project-specific configurations. Participants can select from a rich pool and implement the best combination of solutions for their use case.

Swisscom then invoices the subscriber according to the established procedure and per use. This applies to both identification and signature approval procedures. While some partners may continue to use Mobile ID or a one-time password text message, others may prefer to use Passkey.

Advantage: Broad, selectable best-of-class range of methods for identification and signature approval
Fully embedded in the signature process!

User experience (UX) is key!

The signature process should guide and support the signatory at each step. If the signature approval method is not known to the signature application, the signatory can first select a suitable signature approval method. If Swisscom Trust Services finds that the signatory is not registered or that the registration is not valid, the signatory will be offered the possible registration methods for the signature type and jurisdiction. The registration then proceeds as described above. The signature is then approved and signed. The scope of possible signature approval methods and registration methods can be defined for each signature application.

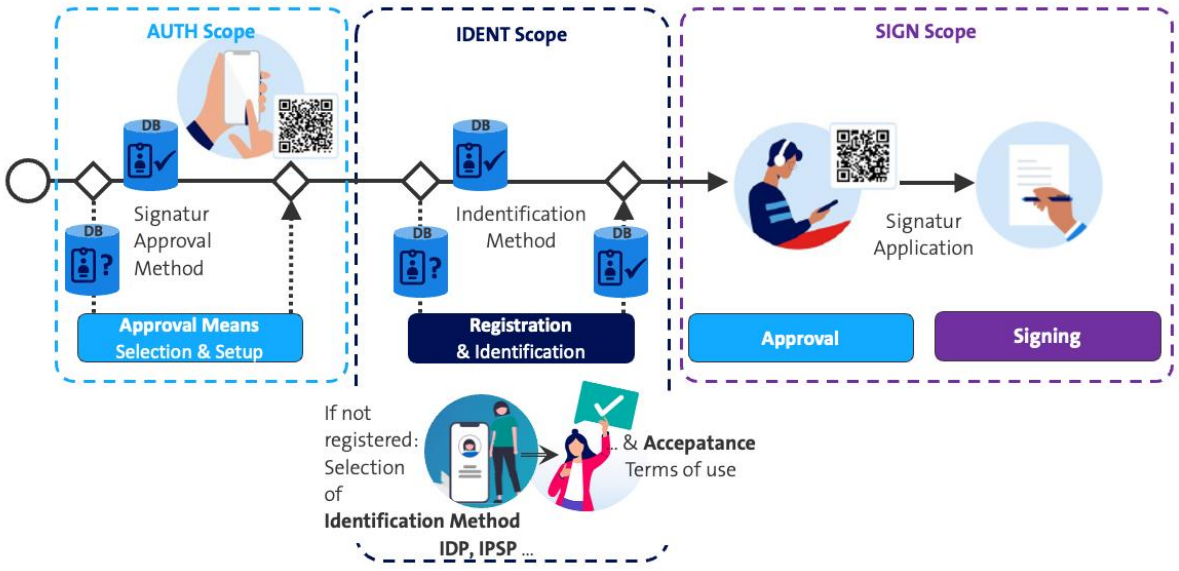


Illustration: Signature approval method selection process - registration - approval - signature

The selection of signature approval and registration methods can take the form of web browser content hosted and provided by Swisscom, or the partner can create its own user interface (UI).

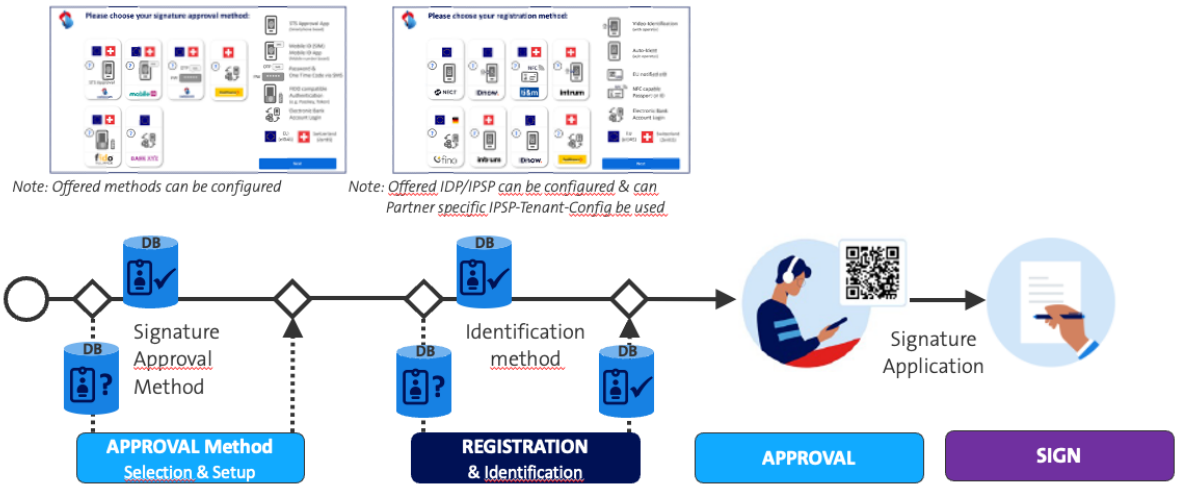


Illustration: Possibility of direct display of the identification and authorisation methods by Swisscom

If the partner wants to create the user guidance themselves, the calls are made via standardized interfaces: OpenID Connect Standards (OIDC) via Pushed Authentication Request (PAR) or Client-Initiated Backchannel Authentication (CIBA) call. This means that the Swisscom UI display of the identification and signature approval methods used can be replaced by a "look and feel" of the partner's signature application. It is then even possible, for example, to display prices for the various methods, if desired. In other words, the stores' offerings can be realized in a design and UI completely determined by the partner.

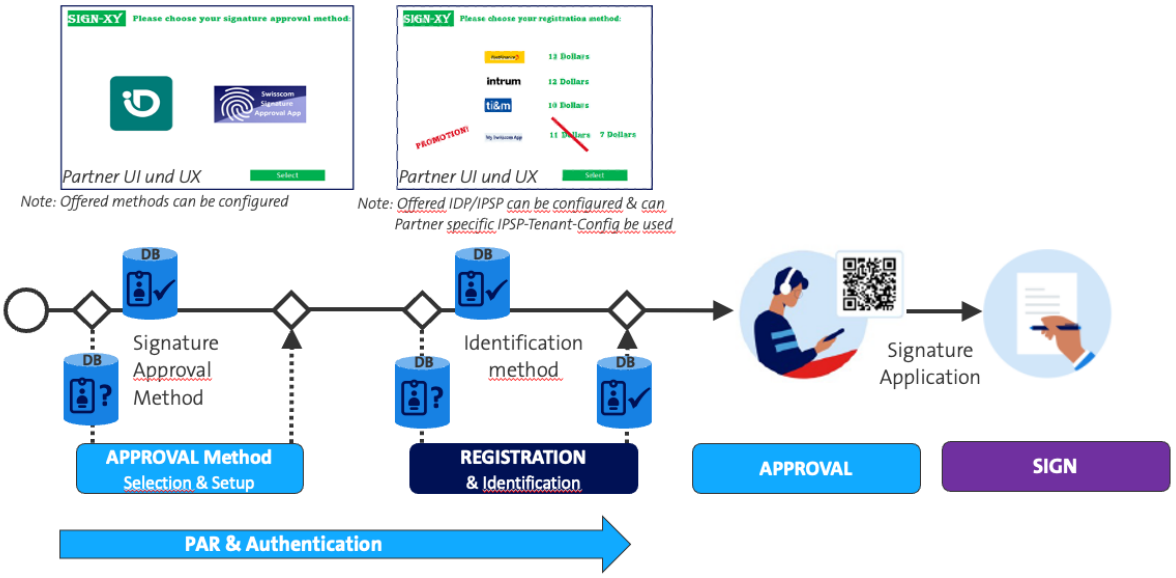


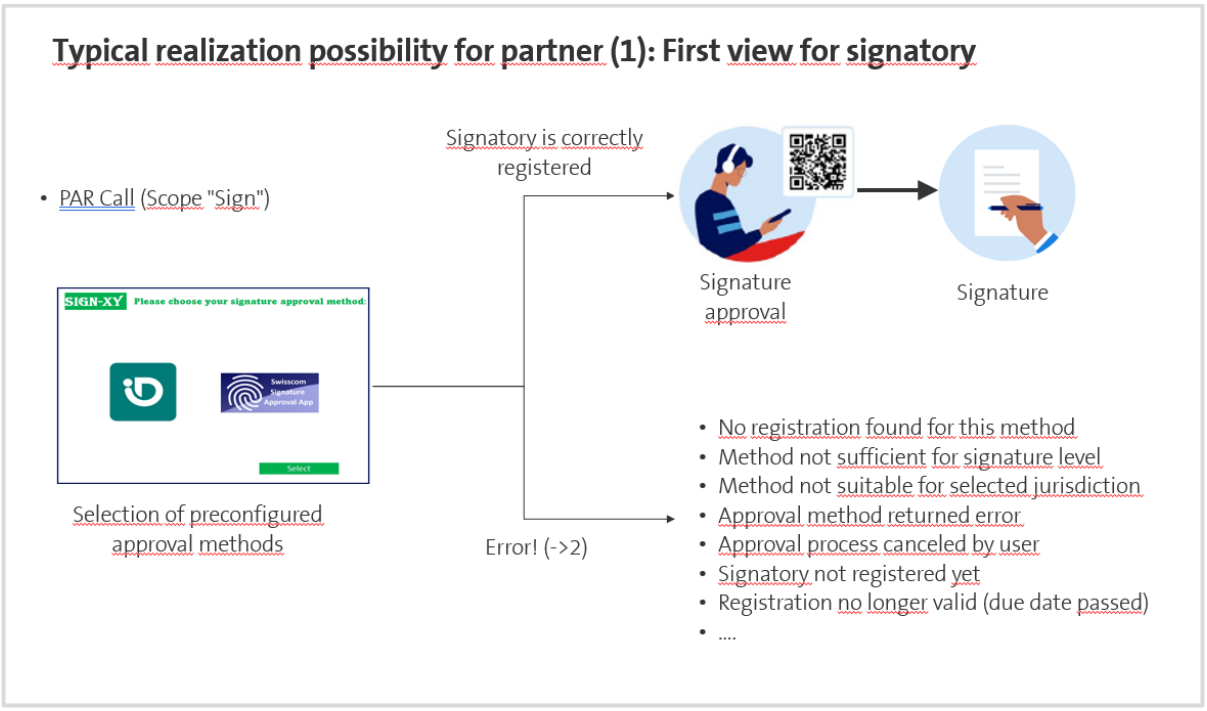
Illustration: Option to directly display the identification and approval methods with the partner's look and feel

Advantage: The signature application partner can fully customise the process and the selection of methods and relies on industry standards for implementation!

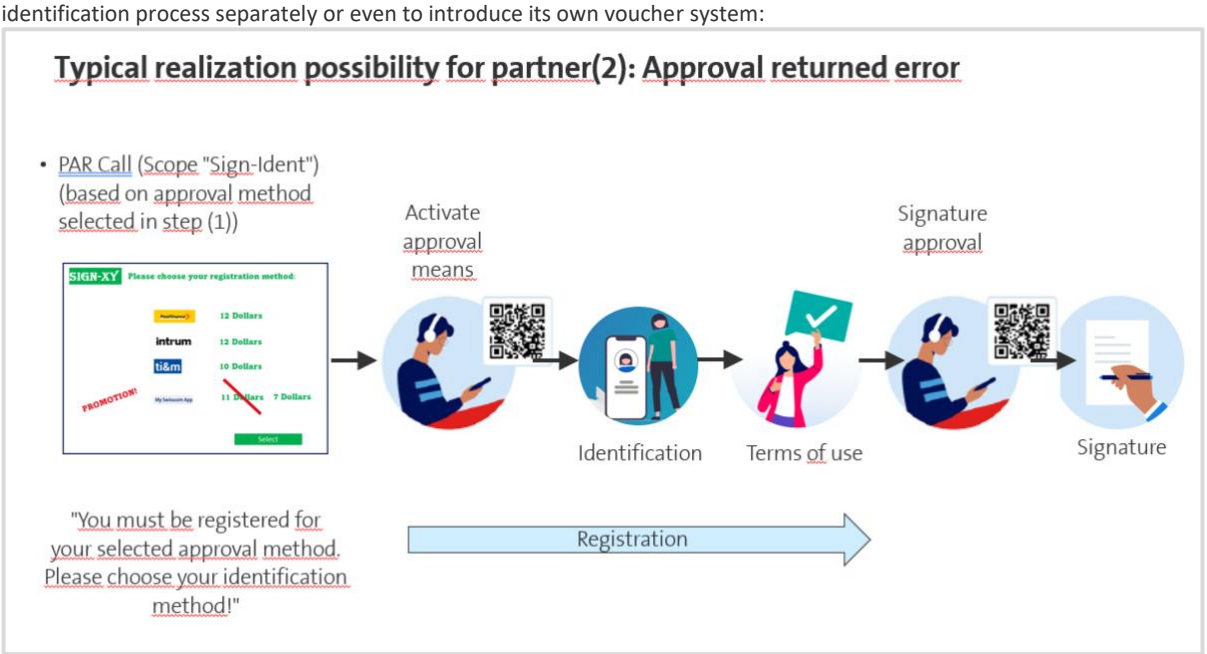
Integration in the signature flow of a partner solution

Using the Pushed Authentication Request (PAR) approach, a partner has the option of creating their own complete user experience (UX) flow and guiding the user through the process. This is demonstrated in the following two steps:

The signatory is first prompted to choose their preferred signature acceptance method. If the signatory is already registered with another provider at Swisscom Trust Services, they can use their registered method for the subsequent signature. If the selected method is unknown or not feasible for any reason, the broker returns an error message and delegates the process back to the partner application (via redirect URL):



In the event of an error, the partner can then offer a selection of permitted identification methods and, based on this selection, specifically initiate the identification and signature process with the chosen signature approval method and identification method. The partner also has the option, if desired, to price certain procedures separately or to bill the identification process separately or even to introduce its own voucher system:



Once the signatory is registered with the selected identification and signature approval method and accepts the terms of use, the signature is created directly. If the process ends with an error, the partner application is informed, and the user is

referred back to the partner application. If necessary, the partner can, for example, restart the identification process and the user can select a different identification method. If the process is successful, the partner application also receives a response event about this and could use it for finalizing the billing process. Identification processes are triggered directly at the identification partner, as are the signature approval processes. If an app is used for approval via a QR code, this QR code can still be displayed in the design and UX of the partner. The Client-Initiated Backchannel Authentication (CIBA) flow can be utilized for this purpose.
The partner application can operate with a process sequence based on scope "Sign" (signature only including prior signature approval) or based on scope "Sign Ident" (registration and signature) in its PAR calls. Various parameters can already be optionally specified e.g., the intended signature approval method and/or the intended identification method.

Legal framework

A new ETSI specification, EN TS 119 461, published in 2021, provides an overview of the requirements for identity verification from a trust service perspective for the first time. All new identification providers will be audited with regard to the identification methods they use. This standard is legally binding in Swiss legislation, and the new eIDAS legislation in 2024 will also require the use of this standard. The conformity assessment body already accepts the fulfillment of the standard as a prerequisite for the registration of a qualified electronic signature.

Identification procedures that have already undergone an EN TS 119 461 audit for their method can be directly integrated into Swisscom's Smart Registration Service. The interfaces, transfer parameters, and relevant implementation criteria must be described in an implementation concept.

The use of Identification Providers (IDPs) and their means of authentication as a signature approval is also considered in the standards for remote signatures, specifically EN 419 241-1 and EN 419 241-2, which explicitly mention the IDP and place requirements on the design of the authentication with regard to the triggering of a signature. Chapter 5.7.4.1 of the EN 419 241-1 standard explicitly states: "The TSP MAY transfer the authentication process to an external party (e.g. an identity provider)."

The most important requirement of this standard is that "The signing keys are used with a high level of trust under the sole control of the signatory." This requirement presupposes that the process, protocol, and procedure are protected on the IDP side in such a way that the IDP and Swisscom map a flow that ensures sole control (referred to as "SCAL2," or "Sole Control Access Level 2 Factor Authentication"), and that the protocol connection on the Swisscom side is designed accordingly for the SCAL2 purpose.
By using the optionally provided signature approval SDK or the use of passkeys, the regulatory requirements for a customer-specific means of approval can be met without a further detailed audit (just a one-day short check, known as a walkthrough by the auditor). Otherwise, a customer-specific authentication procedure must be audited.

The ETSI diagrams illustrate the relationships between the standards:

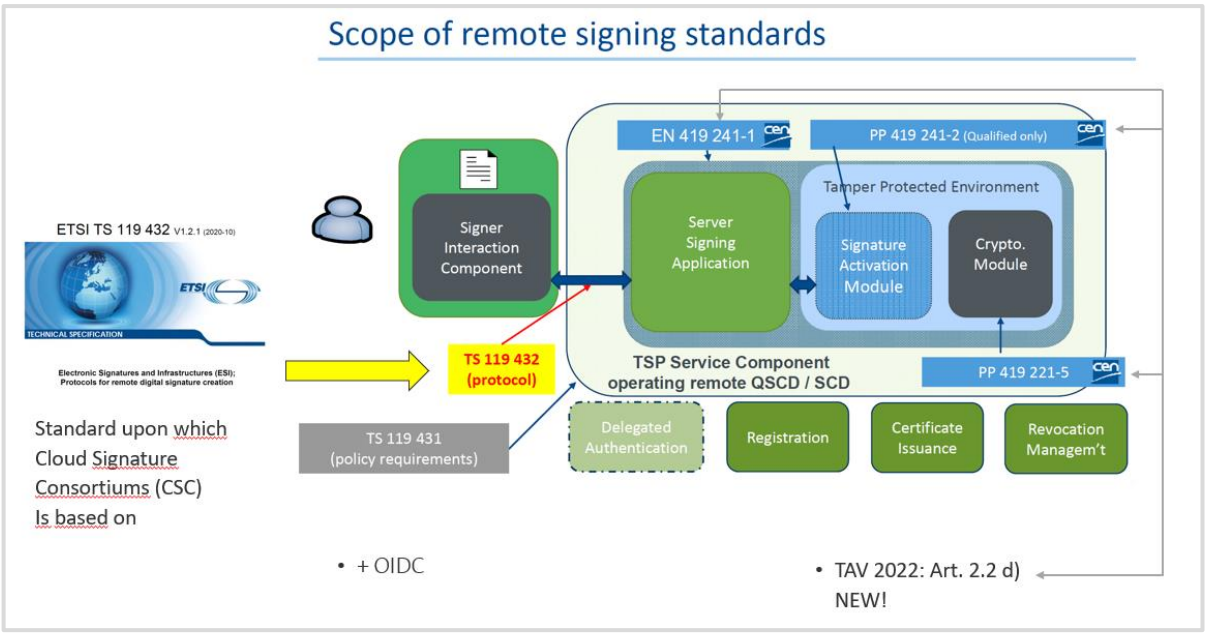


Figure: Classification of the new signing interface TS 119 432 in the ETSI standard environment

The signature application is the "Signer Interaction Component" that is connected to the Trust Service ("TSP Service Component"). The protocol is described in TS 119 432, which references the standards EN 419 241-1/-2 and EN 419 221-5,

which have also been required in Swiss legislation since March 2022 and as part of the authorisation for the EU in Austria. It is expected that they will also generally form the basis of the eIDAS revision in 2024.

The TS 119 432 standard is now also the interface standard for the Swisscom Signing Service. After signature approval and/or registration, the Multiple Authentication Broker of the Smart Registration Service provides the signature application with the necessary token to obtain a signature for a supplied document hash.

Advantage: No proprietary interfaces - use the regulated standards of today and tomorrow!

Signature approval SDK

At Swisscom Trust Services, we understand the importance of simplifying audits and making the process as user-friendly as possible. That's why we offer our Signature Approval SDK (Software Development Kit), which allows you to replicate any authentication request from the signature environment within the look and feel of an existing app, such as a banking or insurance app. This ensures a seamless user experience, as the user does not notice any change of context.

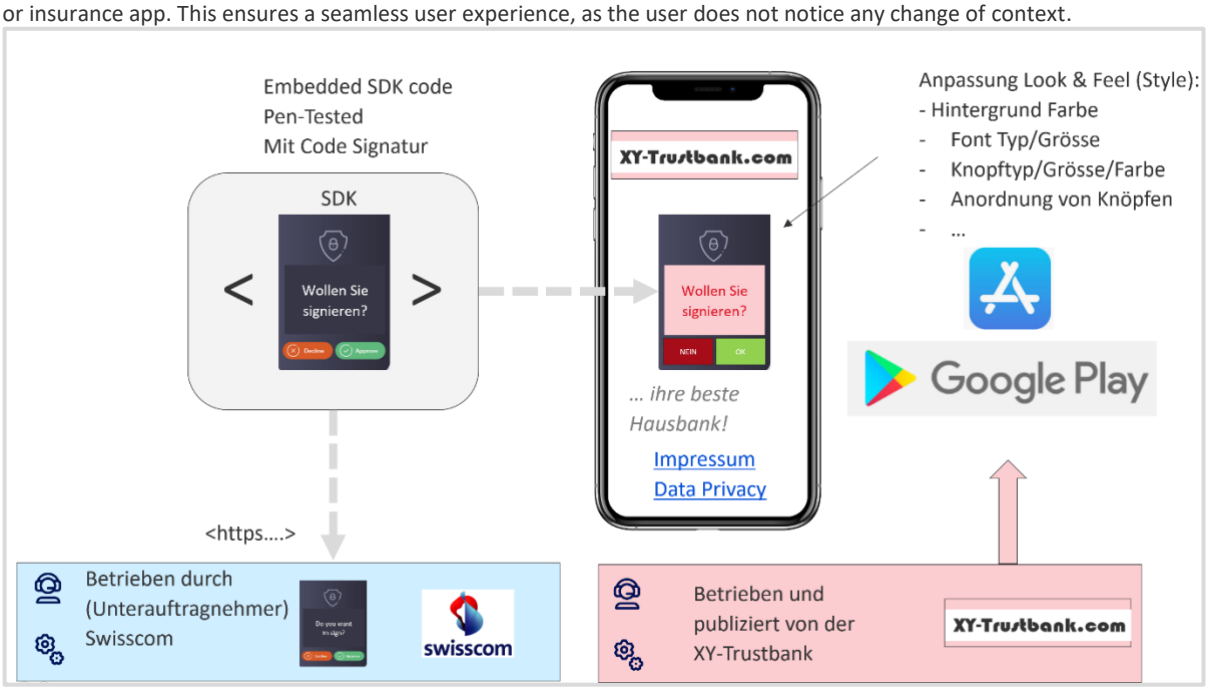


Figure: Use of the signature approval SDK as part of a customised app

The SDK is operated in an environment controlled by Swisscom, which has undergone extensive security tests and audits, eliminating the need for additional full audits on your side. Only a brief inspection by the auditor for embedding in your app is required. In addition, the background colour, font, button shape, etc., can be adapted to the appearance of the target application, enabling signature confirmations to be carried out using methods such as fingerprint or facial recognition.

The SDK is integrated into the target application by the customer company, and a code signature can be used to ensure that the app's functions have not been changed, further eliminating the need for additional audits.

This seamless and transparent experience not only simplifies the signature process but also makes it more cost-efficient and user-friendly for the client organization and the end user. For example, they can perform signature approvals within their banking app, with the same look and feel and user experience as in their other banking context, without realising that the approval process is being performed from a different operating location.

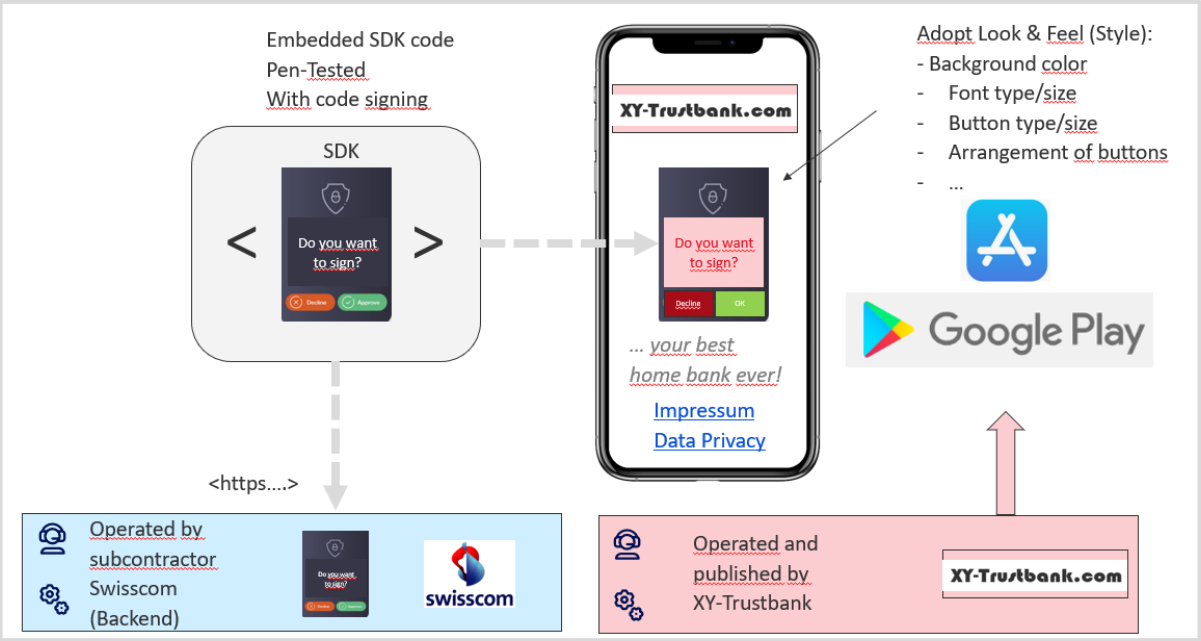


Illustration: Operation of the relevant signature approval in the already audited process by Swisscom

Advantage: Reduce audit costs and still take over user control yourself!
Full customising of signature approval!

The principle of "register once" - "sign as you like"

Swisscom's Trust Service aims to simplify the user experience by minimizing the need for complex identification and general acceptance of terms for every signature process. Instead, a registered person can approve signatures for months or even years using a fingerprint or facial recognition.

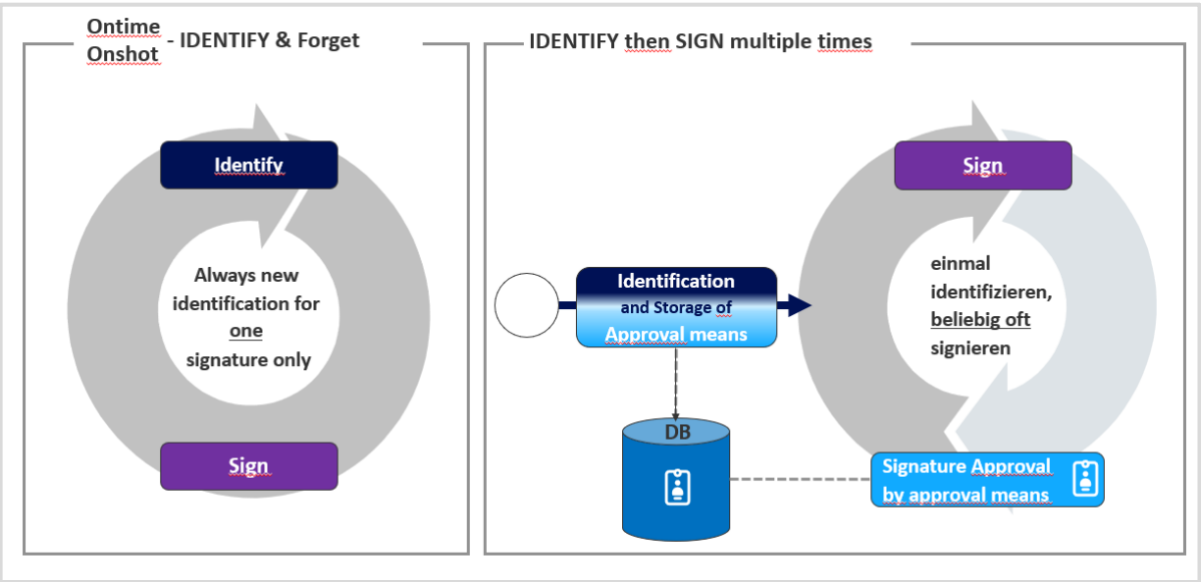


Figure: Differences between one-shot signing (without approval method) and repetitive signing

The service differentiates between an Identity Provider (IDP) and an Identity Proofing Service Provider (IPSP) for identification and authorization:

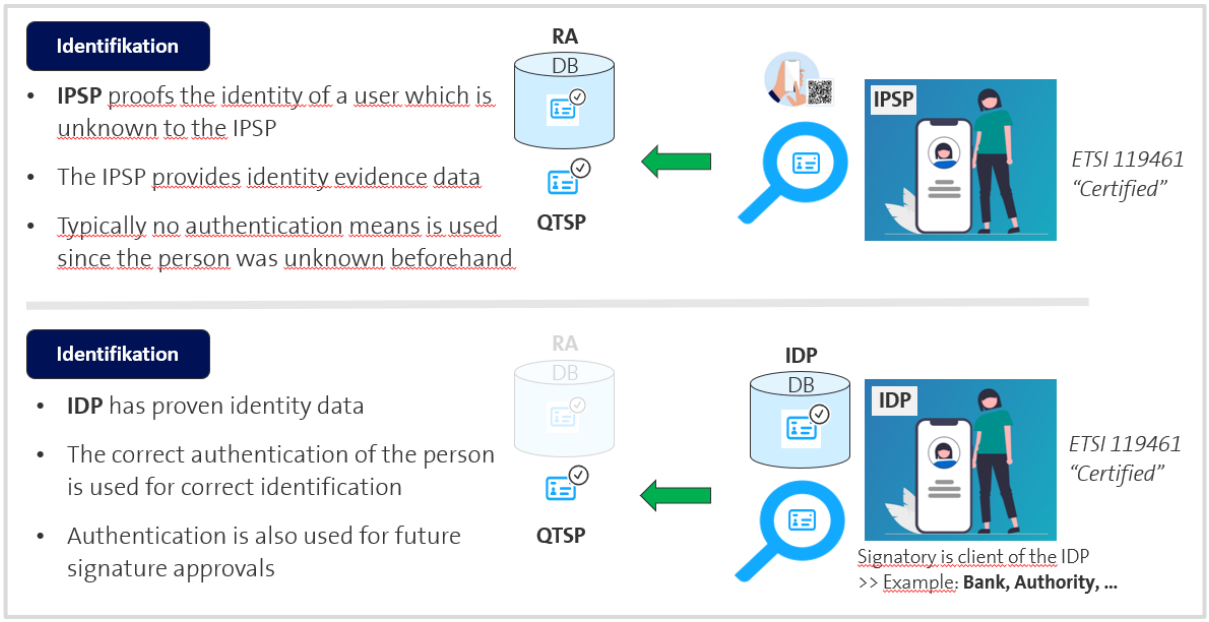


Figure: Differences between IPSP and IDP for the return of results to Swisscom Trust Services

An IPSP verifies the signatory's identity. If you now want to use this identity for future signatures, you also need an authentication method (e.g. passkey or an authentication app), which you initialise in the same registration process for future use.
An IDP recognizes the signatory, requiring a one-time login and confirmation of Swisscom's terms of use. The login can then also be used for signature approvals.

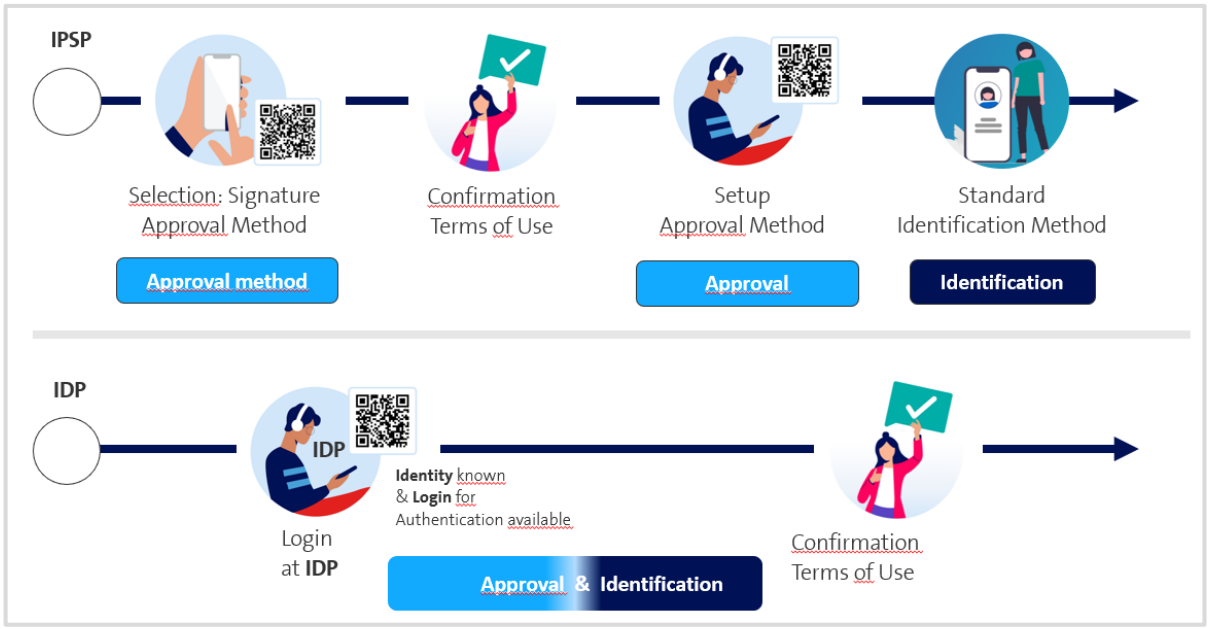


Figure: Differences between IPSP and IDP in the context of registration and signature approval

In the Smart Registration & Signing Service, a Registration Authority database now ensures which means of signature approval the signatory uses and whether registration has taken place. Evidence of identification does not have to be stored in the database itself, but during the signing process the database uses a signatory feature (e.g. UUID, e-mail, etc.) to refer the orchestrating broker to the signature approval or registration with the IDP and the broker forwards the signatory to the IDP.

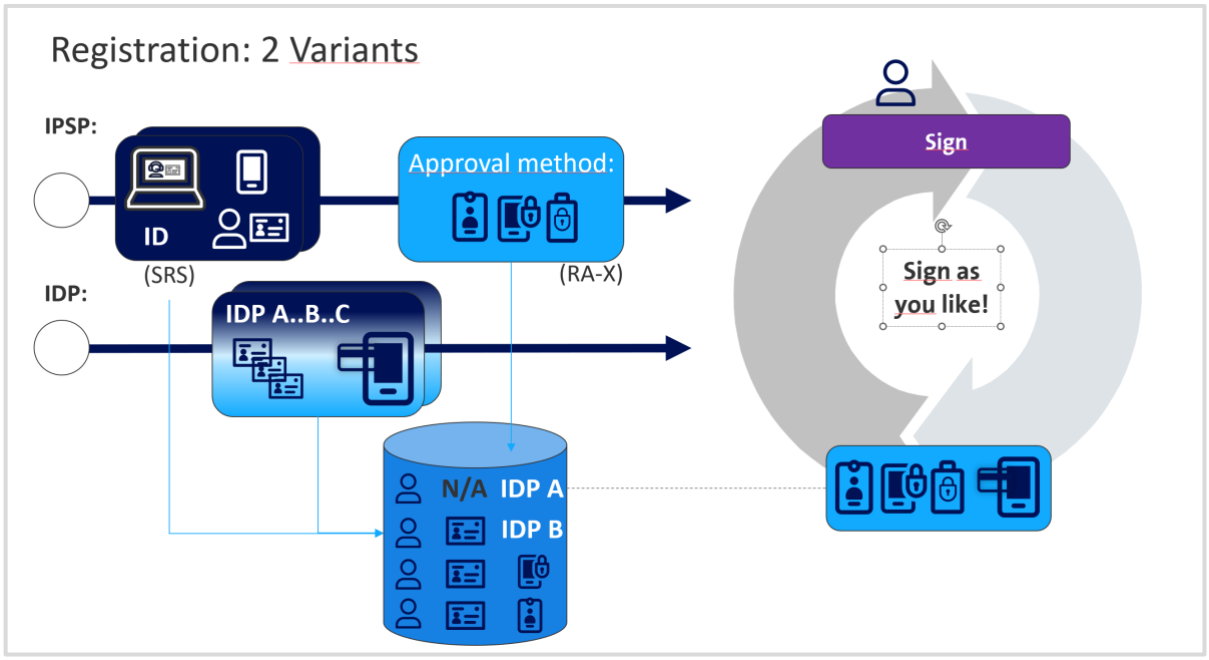


Illustration: The RA database can have a reference to the corresponding IDP instead

No matter how - the current signature is very simple for the signatory - a smile is enough for all signature applications that use Swisscom, as the example with Passkeys shows here:

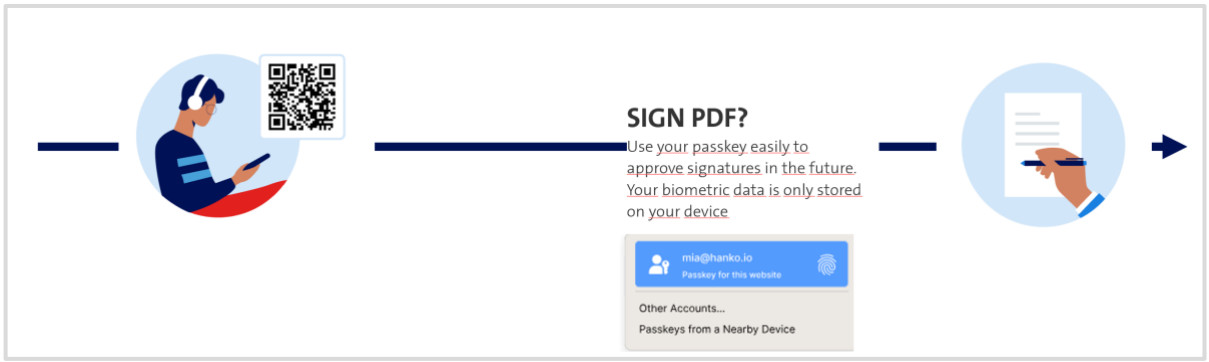


Figure: Typical signature approval for an already registered user

Advantage: Annoying registration only once - otherwise a smile is enough for the signature!

The one-shot signature - sometimes still desirable

In many scenarios, signatories should not be exposed to repeated signatures. In such cases, the signature approval agent should be eliminated, even if this can be achieved simply with passkeys in the future. This shortens the process:

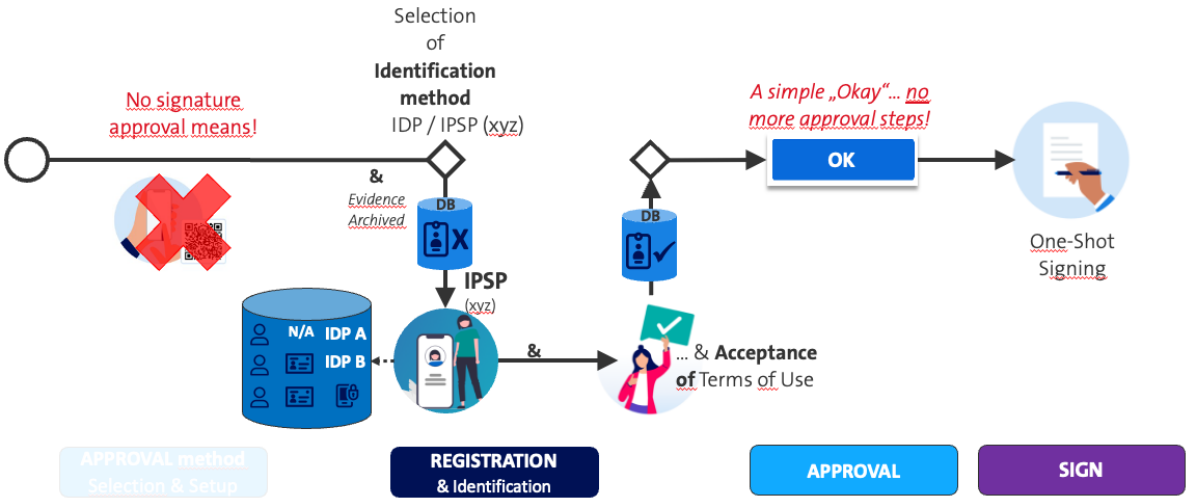


Illustration: One-time signature procedure: Start of the session - Identification - Confirmation of terms of use

his streamlines the process, as the signature then consists of just one process in which the signatory identifies themselves, accepts the terms of use, and authorizes the signature with a simple 'OK' button. The downside is that the signatory must identify themselves again during the next signature process.
Previously, one-shot signature processes had to be individually audited, as the process implicitly included the highly regulated signature approval. However, with the new Smart Registration & Signing Service, all standard identification processes can be used without further auditing. Additional identification procedures in accordance with the EN TS 119 461 standard can be easily added. As described above, there is a Swisscom onboarding procedure for this.

Advantage: One-time signatures can dispense with a means of approval (including SMS)! Without audit!

Technical process of the signature protocol

The signature protocol now complies with the OpenID Connect Standard (OIDC) based on the new ETSI EN TS 119 432 standard, which explicitly allows for the use of IDPs. The signature application communicates with the Multiple Authentication Broker of the Smart Registration Service. After identification and approval, the signature application receives a token to request the signature from the signing service.

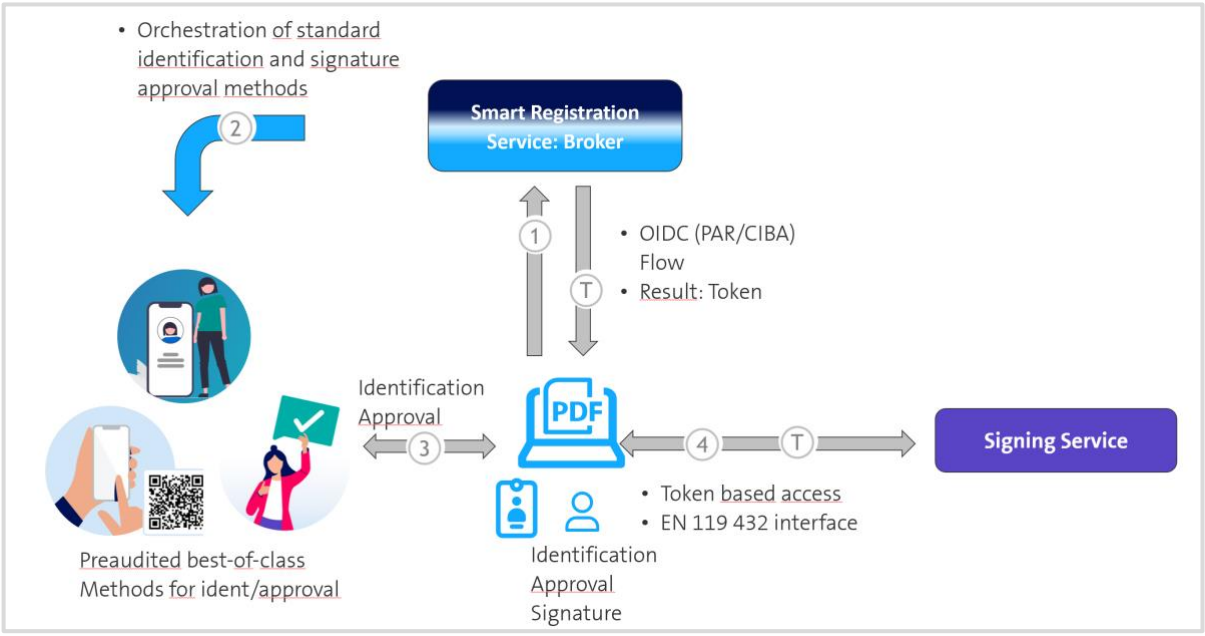


Figure: Communication interfaces for signature approval and signature

The detailed process is as follows:

1. An approval request is made based on an authentication request via a certificate (mTLS)-protected connection with the authentication broker of the Smart Registration & Signing Service. A user feature is also transferred, e.g., an identifier of the installed approval tool, a mobile number, or an email address.
2. If the person has not been registered, an error message is displayed, and the person must first be registered for the first time as described above.
3. If the person has already been registered, the authentication stored during registration is addressed. This can be a standard Swisscom authentication method (e.g., Mobile ID, signature approval app, or a signature approval SDK integrated in the customer app) or the authentication for the signature by an IDP. The signature application, therefore, issues an authorization request (including ACR (Authorization Context Reference) with the document hash and the necessary information, e.g., jurisdiction (EU/CH) or signature level (advanced/qualified)).
4. The authentication authority checks the request, including the URL source, and after successful approval, transmits an authorization code first to the authentication broker, which, after further verification, transmits an authorization code for the signature to the signature application.
5. The signature application can now request an access token with the authorization code.
6. The signature is then requested with this access token.
7. The end user short-term certificate for the signature is now generated, either with the information from the Smart Registration & Signing Service database or - if the data is held exclusively by the delegated IDP - by requesting the first name, surname, and country or pseudonym and country from the IDP.
8. The hash is signed, and the signature application receives the signed hash and can thus create the signed document.

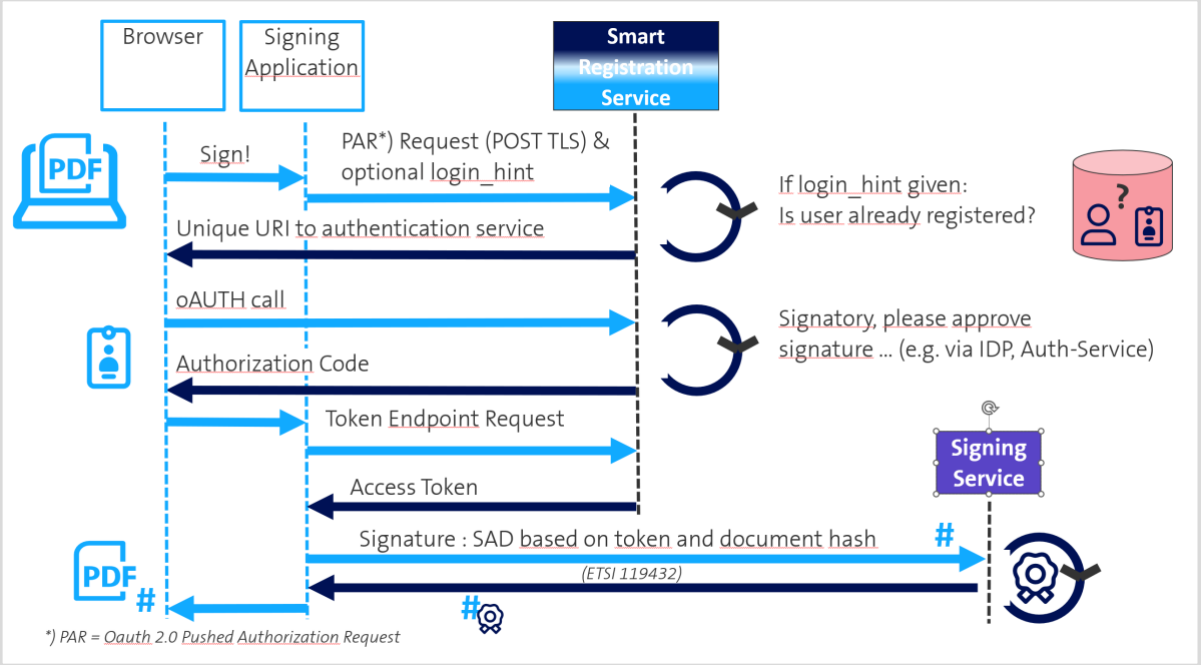


Illustration: Flow chart for the signature

The authentication broker in the Smart Registration & Signing Service will skilfully take over the logic of the authentication assignment. Either the authentication instance e.g., the IDP or the Mobile ID app, is already known from the outset. In this case, the appropriate authentication can be carried out immediately using the registered authorisation method. If it is not known or several authorisation options exist, these are offered for selection in a browser view (web view).

Advantage: OAuth/OIDC standards linked with standard ETSI protocols, fast and clean integration!

New monetisation opportunities for IDPs

By using identification and authentication methods already employed by banks, insurance companies, and other institutions (IDPs), all companies with signature applications (third-party applications) can enhance the efficiency and security of their processes. This eliminates the need for signatories to undergo on-site identification or time-consuming video identification, provided they can leverage the options offered by IDPs.

Swisscom Trust Services, through its stores, provides a marketplace where companies can discover identification methods and approval solutions for signatures from audited IDPs. Acting as a reseller, Swisscom Trust Services enables the IDPs to monetize these offerings by imposing monthly usage fees and/or transaction-based prices on the partner or end customer for initial registration and/or signature approval. This approach allows IDPs to optimize their processes through electronic signatures and reap the benefits of their identification and approval services when utilized by third parties.

Once registered, the signatory typically utilizes the authentication offered by the IDP. Subsequently, the IDP can ascertain if Swisscom Trust Services also provides this authorization method to third parties for the signature application. In this case, monthly or annual usage costs can be levied.

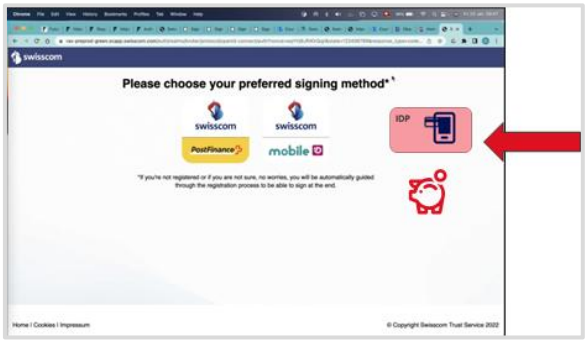


Illustration: Monetisation of IDP's own signature approval for third-party applications

Regardless of marketplace usage, the IDP itself can control its use and, for example, not charge any fees for its use in its own environment but can provide for a usage fee in its price list for each approval for a third party.

Banks and insurance companies have shown a strong tendency to expand their mobile applications in recent years. This is due to the increasing demand for convenience, the rising number of smartphone users, and the competition between banks aiming to increase customer loyalty and strengthen their brand awareness.

One of the latest developments in this area is multi-banking apps, which allow customers to manage their accounts at different banks via a single application, simplifying the monitoring of finances and transactions.

Another development is lifestyle apps that go beyond banking transactions, offering contract management, discounted shopping, or a news platform. The electronic signature is an ideal addition here, increasing customer interaction with the bank and providing added value by offering a variety of services in one place.

By expanding their applications and providing additional services, banks enable their customers to check the app daily, thereby increasing customer loyalty. The use of mobile applications will continue to grow in all sectors, and players will have to adapt to remain competitive.

Advantage: Use your own identifications/authentications and resell them in the Swisscom Store!

Further information

For developers:

Demo videos for the

- Standard approval and signature flow (Swisscom Webviews) (youtube)
- PAR based signature approval/registration
- CIBA based signature approval/registration

Postman examples (github)

Swisscom Broker Call

Detailed product information, in particular the Reference Guide

Order a free test account

For further information please contact:

Swisscom Trust Services AG
Sales Support
Konradstrasse 12
8005 Zurich
Switzerland
https://trustservices.swisscom.com
E-mail: sts.salessupport@swisscom.com

Swisscom Trust Services