



Multiple Authentication Broker

E-signature caught between user-friendliness and compliance with regulations

The theft of user identity is the greatest risk with electronic signatures. Hence, there are comprehensive regulatory requirements on how users must be registered for an e-signature and how they approve it remotely. Furthermore, the regulatory provisions vary from country to country, and there are different levels of electronic signature (qualified or advanced), each with different technical requirements. In addition, e-signature approval needs an authentication means, that users set up during e-signature registration process. Moreover, there are time limitations on the validity of the registration.

Orchestration between e-signature, identification and approval

In the past, the signature application had to verify whether their users performed a proper identification verification and registration of signature approval means. In the analog world, signatories usually identified themselves at the post office counter. In the era of online identification and remote e-signing, the Multiple Authentication Broker by Swisscom Trust Services offers new business opportunities.

Broker: balancing simplicity and regulation

Swisscom Trust Services' decision-driven Multiple Authentication Broker relieves the signature application of all concerns regarding the correct onboarding for an e-signature:

It guides the user through the entire e-signature registration process, offers the appropriate selection of signature approval means, and, depending on the registration status, facilitates suitable online identification or alternatively, direct signature approval. Predefined views or interfaces in the partner's own brand are available (customizing). All identification and approval methods available in the broker are certified for e-signature registration by our conformity body.

Broad choice of signature approval methods

Within the browser flow, a range of signature approval methods can be presented for the signatory to select from, e.g. the modern FIDO2 passkey method, a classic combination of password and one-time code via SMS, or convenient mobile apps that can approve e-signatures via fingerprint or facial recognition.

Broad selection of identification methods

All state-of-art identity proofing solutions can be provided within the browser flow and ensure easy online identification of signatories, e.g., video-ident, auto-ident, NFC-scan, eID identification, or identification via e-banking login. These methods are tailored to the legal jurisdiction and the respective e-signature level. It is also possible to have identification and signature approval without signature approval means (one-shot signing). Furthermore, any other compliant identification and authentication solution can be integrated at any time after an audit.





Facts and figures



Easy integration

ETSI EN 119 432 API, Open ID Connect (OIDC) / Pushed Authentication Request (PAR)

The Multiple Authentication Broker provides a standardized remote signature interface in accordance with ETSI EN 119 432 by means of tokens. Open ID Connect standard is used for the connection. Partner applications can customize default screens in their own CI/CD and integrate them using the OIDC-PAR interface or CIBA.



Authentication

Various authentication procedures for e-signature approval according to ISO EN 419 241

E-signature approval can be carried out either via identification and signature approval in one process («one-shot signing»). If partner application intends to implement a repetitive e-signing process, there are diverse signature approval methods available, e.g., passkey (FIDO2), Swisscom Signature Approval app, Mobile ID (Swiss SIM card add-on), Mobile ID app, password / one-time code (SMS), or an SDK for integrating approval procedures in your own apps. If partner or IDPs provide an own authentication solution, they can use them as e-signature approval method once they complete a conformity assessment (audit). All available authentication procedures fulfil the requirements of the ISO standard EN 419 241.



Identification

Diverse identification methods for e-signature registration (qualified signature) according to ETSI EN 119 461)

The broker also enables the inclusion of offline standalone identification, e.g., in Swisscom shops (in Switzerland) or via the RA app. In addition, there are various online identification methods from conformity-assessed partners available within the broker, such as video identification (Intrum), auto-identification (Fidentity, ti&m, NECT, Intrum), passport identification via NFC chip (ti&m, Fidentity), bank identification via bank account login (e.g., Postfinance). If partners or identity proofing solution providers intend to provide their own identification solution, they can use them as e-signature registration method once they complete the conformity assessment (audit). All procedures, available in the broker, are conformity-tested in accordance with the ETSI standard EN 119 461.



Fast

Setup and configuration

After ordering, signature applications can immediately configure and use their selected standard approval and identification procedures for their e-signature processes. Open interface standards such as ETSI EN 119 432 and OIDC, allow fast integration time and enables a high level of investment protection. Broker operation is geo-redundant.

Are you interested in integrating qualified e-signature journeys into your application?

Contact us - We look forward to meeting you! You can find additional information on our website:

www.trustservices.swisscom.com



Facts and figures



Privacy

Data protection - transmission of document hashvalues

Swisscom Trust Services does not infer the document's content because only hash values of the document are transmitted for issuing the e-signature. Identification evidence data is subject to strict dual control access and is only required for e-signature purpose.



Accredited

Qualified recognized

Swisscom IT Services Finance S.E. in Vienna, Austria is a recognized trust service provider for qualified and advanced e-signatures and e-seals in the EU and is a member of the eIDAS Trust List. Swisscom (Switzerland) Ltd is an approved certificate service provider in Switzerland for the Swiss Federal Signature Act (ZertES).



Ready for the future

Fit for the future

The broker's architecture is prepared for integration of European Digital Identity Wallets according to the revision of the eIDAS regulation

Are you interested in integrating qualified e-signature journeys into your application?

Contact us - We look forward to meeting you! You can find additional information on our website:

www.trustservices.swisscom.com