As the leading trust services provider in Europe, we enable the most innovative, digital business models.

White Paper

Procedure as a seal partner

Swisscom Trust Services

Swisscom Trust Services

Table of contents

Regulatory situation

Regulated seals according to ZertES (Switzerland) and qualified seals according to eIDAS (EU) can also be issued within the scope of a remote signature. The conformity assessment bodies in Austria for Swisscom IT Services Finance S.E. and the certification body in Switzerland for Swisscom (Switzerland) Ltd. rely on an audit according to the European standard for remote signatures EN 419241, which provides for the so-called "SCAL2" procedure (Sole Control Assurance Level), which requires a 2-factor authentication. For advanced seals, "SCAL1", i.e. 1-factor authentication, would be sufficient, e.g. “pos-session”. In this respect, seals can be issued via remote signature by establishing a TLS connection between the signing organisation and Swisscom, the signing organisation is then in possession of the private key to the public key in the TLS certificate. This is no longer sufficient for the qualified (EU) or regulated (CH) level. Here, for example, the factor "knowledge" or "biometrics” would also have to be added. For example, a authorization of a signature could be made by a representative of the organisation explicitly authorizing the private key by means of a password, biometric feature, etc.

Procedure for the second factor

Swisscom has an approved procedure for issuing seals in accordance with CP/CPS:
The certificate issuance procedure is as follows:

- It is ensured that an HSM is used,
- from Swisscom, a certificate of the desired class is issued,
- the certificate and the associated cryptographic key are either
    - deposited in the Trust Center and the SSL/TLS client certificate delivered at the time of identification is linked to the associated user account, so that the creation of seals by means of remote access is possible exclusively through possession of the associated private key (signature creation data) or
    - stored at the customer's premises in the HSM after Swisscom has ensured that the customer complies with the required specifications,
- the certificate holder is informed of the provision. »

In concrete terms concerning authentication:
"The registration and use of the means of authentication shall be carried out using a procedure described by the applicant, which is approved by Swisscom and complies with level 2 (Sole Control Assurance Level 2) described in [CEN/TS 419 241]. “

This allows partners to demonstrate how they can comply with the SCAL2 requirements in the form of a small concept.

An example could be an HSM or a cloud HSM with on-site access at the customer's premises, where the key pair is generated in a joint ceremony and thus also the TLS certificate, with the private key being stored in the HSM in the presence of a verified representative of the organisation. To ensure that batch processes with sealing continue to be possible, it is then advisable to release the private key, e.g. for a limited period of time.

Requirements for the procedure

The partner should prepare a solution concept describing the following points:

- Description of the solution and the process flow. Here it is important how to ensure that only the organisation's representative can ultimately influence the TLS channel and not a third party.
- Conformity of the hardware or cloud solution used (e.g. HSM according to FIPS protection level or comparable data base protection)
- Proof of the responsibilities and competences of the role keepers in the process. If the process is completely automated (e.g. approval directly by the person responsible for the organisation), no other roles may exist here. If, on the other hand, a joint ceremony takes place, there may be persons who generate the key, persons who keep the minutes, etc.
- How are the people in their roles regularly trained?

The procedure must then be submitted to Swisscom for approval.

Further procedure

The interested partner who would like to sell seal applications for Swisscom in the future should initially conclude a "Contract for the Provision of a Seal Solution", which regulates the technical solution for the storage of private keys as well as the authority to provide qualified or regulated seals with this solution. In the contract, reference is made to the previously mentioned and released concept. The partner should be willing to enter the seal business with a lot of end customers.

Once the procedure has been approved, the following process steps must be observed for each sealing project:

- The applicant (end customer), i.e. his authorised representative named in the application, should first be identified using the RA app. He can then sign the necessary documents via a Swisscom signature platform or a signature platform operated by the Swisscom partner, in particular the application and the configuration and acceptance declaration. For this purpose, the checklist in the order by the partner must be observed, as the law specifies very many case distinctions and also necessary enclosures (e.g. excerpts from the commercial register) and also the form for this (e.g. certification) must be observed.
- Swisscom then checks the organisation, the authorisation of the representative (e.g. according to the register entry or a general power of attorney signed by a representative of the organisation notified in the register) and the attached documents and deeds and gives its approval for setting up a remote signature.
- If the resolution process provides for a joint key generation ceremony, Swisscom should attend the first ceremony. See further guidance on such a ceremony below.
- At the end of the connection procedure, Swisscom should receive a TLS certificate directly from the applicant, which is used to secure the communication for remote signature and signature application.
- Based on the certificate, Swisscom informs the applicant of the ClaimedID.

Ceremony

In case an automated solution based on the identification by the RA app and e.g. a QES created with it is not possible, the private key and the certificate may have to be generated and stored securely in a common logged ceremony.

The applicant i.e., the representative of the organisation named in the certificate application, the authorised representative of the partner and, if applicable, the operator of the participant application or at least of the access control within the participant application should be present at this ceremony. If necessary, the access control is also operated by the partner itself, but even then, there can be different roles: the technician who generates a key pair, for example, and the authorised representative who logs.

As a conclusion of the ceremony, there should be a protocol signed by all participants, which includes the following:

- Steps (technical) taken to ensure the assignment of the access means (private key of the SSL connection) to the identified requester according to the released SCAL2 solution concept.
- Device designation of the cryptographic module, SW status Version
- Conformity of the solution used (must meet the requirements previously submitted and approved in the solution concept)
- Participant (verified proof of identity should be presented, i.e. shown by passport/ID)
- Signatures

The protocol should be submitted to Swisscom by post or scanned and signed by the authorised representative of the partner with QES.
As already mentioned above, at least the first ceremony(s) should be carried out together with Swisscom. (Training by doing)

Please do not hesitate to contact us for further information:

Swisscom Trust Services Ltd.
Sales Support
Konradstrasse 12

CH-8005 Zürich

https://trustservices.swisscom.com