Zürcher Kantonalbank
Practice Statement

concerning the issuing of qualified certificates | 2024 May

Key documents

ETSI EN 119 461	Electronic Signatures and Infrastructures (ESI); policy and security requirements for trust service components providing identity proofing of trust service subjects
ETSI EN 319 401	Electronic Signatures and Infrastructures (ESI); general policy requirements for trust service providers
ESigA	Swiss Federal Act on Certification Services in relation to Electronic Signatures and other Uses of Digital Certificates, SR 943.03
CertESO	Ordinance on Certification Services for Electronic Signatures and other Uses of Digital Certificates, SR 943.032

1 Purpose and content of this document

Zürcher Kantonalbank (ZKB) offers a group of persons ("users") designated by it and in connection with a business relationship with ZKB the option of providing a qualified electronic signature. The qualified electronic signature (QES) meets the highest security requirements and, in combination with a qualified timestamp, is equivalent to a handwritten signature.

This statement about the practice informs users and other parties involved about the identification process and the link to the qualified certificate for the QES.

2 Use of third-party software and/or services

ZKB may use third-party software and/or services to carry out the identification process and link it to a qualified certificate. In principle and unless otherwise communicated, ZKB is responsible for their involvement.

Third parties that provide software or services for a QES are also required to comply with the regulatory requirements and standards of ESigA and ETSI. When evaluating these third parties, ZKB has checked that they meet the corresponding specifications and standards, and ensures that these specifications and standards are also complied with in the future.

3 Procedure for issuing a qualified certificate

The requirements for the use of a QES can be divided into the following two sub-processes:

3.1 (Online) identification

ZKB obtains from the user photographs of themselves and all the relevant pages of their identification document. It checks that the photo taken by the user matches the photo on the identification document. With the support of suitable technical aids that, as a minimum, permit the information in the Machine Readable Zone to be read and decrypted, ZKB checks whether the decrypted information is consistent with the other information on the ID and with the data provided by the user.

ZKB assesses the authenticity of the identification document on the basis of at least two randomly selected security features. ZKB shall also ensure that the user's photograph has been created as part of the identification process.

A list of the identification documents approved for online identification is available at zkb.ch.

3.2 Issuing a qualified certificate for QES

After the identification process has been successfully completed, a qualified certificate can be issued for the QES.

For this purpose, ZKB will forward the necessary data from the identification to a certification service provider. The certification service provider uses the information from the identification to issue a qualified certificate for the QES and the users can then use the qualified certificate to electronically sign selected documents within the context of the business relationship with ZKB.

Electronically signed documents have the same effect as handwritten signatures and represent the original version of the document.

4 Invalidation of a qualified certificate

4.1 Reasons

A qualified certificate will be declared invalid by the certification service provider for the reasons stated below. The documents signed electronically up to this point in time will remain legally signed.

1. There is a suspicion that the private key or other encrypted data for signature creation has been compromised, stolen, disclosed or otherwise misused.
2. The qualified certificate is no longer required by the user.
3. The data used for the qualified certificate has changed or is no longer correct, such as in the case of a name change, for example.
4. After five years (the start date is the successful completion of the identification process), ZKB will automatically declare a qualified certificate invalid.
5. ZKB or the certification service provider becomes aware that a qualified certificate is to be declared invalid.

If ZKB becomes aware of one of the above reasons, it may also request invalidation from the certification service provider.

Once a certificate has been invalidated, if users wish to obtain another qualified certificate, they can have a new certificate issued if they first undergo another identification process.

This list is not exhaustive and there may be other reasons for the certification service provider to declare a qualified certificate invalid or for ZKB to request the certification service provider declare a certificate invalid.

4.2 Restrictions

4.2.1 Requirements when issuing a qualified certificate

For greater security when issuing qualified certificates, ZKB reserves the right to stipulate technical requirements governing the smartphone used for confirmation. These include:

1. Operating system requirements: the following operating systems are a minimum requirement for the issuing of regulated certificates (as of 2024 March):
    1. Android: Android 6
    2. iOS: iOS 14
2. No smartphone that has been rooted or jailbroken: the use of a smartphone with full access to system rights (rooted or jailbroken) is not permitted when issuing regulated certificates and is not allowed by ZKB.
3. Enabled biometrics: only smartphones where biometrics are enabled can be used to issue regulated certificates. If a user has not activated the feature, they will be asked to save their biometric data on their smartphone before using it for the first time.

ZKB can change the minimum requirements if necessary. Changes will be communicated by updating the statement on practice.

4.2.2 Purpose of the qualified certificates issued

The qualified certificates issued by a certification service provider as part of this process can only be used for the business relationship with ZKB.

5 Termination of business

5.1 Information

If ZKB decides not to have any further qualified certificates issued by a certification service provider, it will take the following steps:

1. Information for users: users who have been issued with a qualified certificate for a QES in connection with the business relationship with ZKB will be notified at a suitable time that the certificate will no longer be used at ZKB so that they can take appropriate measures.

2. Information to third parties involved: third parties involved in the identification process or in issuing the qualified certificate or QES will be informed in good time that the certificate will no longer be issued or accepted.
3. Information to the accreditation body and to the recognition body: the Swiss accreditation body and the accredited recognition body that controls the process for issuing a QES certificate will be informed in advance that ZKB will no longer have regulated certificates issued through the certification service provider. They will also be informed of the further procedure for the certificates issued up to this point in time.

5.2 Handling of identification documents and qualified certificates

ZKB is obliged to archive the issued identification documents for the legally prescribed period and to present them to authorised persons or bodies on demand. The certification service provider is also obliged to store issued qualified certificates in an appropriate manner for the legally required period.

From the time the QES is relinquished, the certification service provider will revoke the qualified certificates still valid at that time and no further documents can be electronically signed with these certificates.

6 Security management regarding the IT hardware and software used

Our security assessments for the ZKB IT systems – for both internal IT systems and those outsourced to third parties – are based on the ISO 27002 standard and supplemented by provisions from the NIST (National Institute of Standards and Technology) Cybersecurity Framework. Security assessments are updated at least once a year for critical IT systems. Security assessments are carried out during the year if processes or IT systems are significantly changed or due to event analyses, revisions/audits and other triggering criteria.

We have a programme in place to identify and monitor areas of action in the form of a cybersecurity roadmap.

7 Entry into force and changes

7.1 Entry into force

This statement on practice will enter into force in May 2024.

7.2 Amendments to this document

This document is reviewed to ensure it is up to date each time there is a substantial change to the service and at least once a year. It is approved by the person responsible for the QES process (process chain manager) and a member of the executive management and then made available to users on zkb.ch.