BUNDESNOTARKAMMER
ZERTIFIZIERUNGSSTELLE

PKI Disclosure Statement of the Certification Authority of the German Federal Chamber of Notaries for qualified certificates

Version	**2.8**
Date	**08 May 2024**

Document history

Version	Remarks	Date
1.0	Preparation of the document in the course of the assessment of compliance with the requirements set out in the Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EG (**eIDAS Regulation**) by an accredited conformity assessment body	20/06/2017
1.1	Editorial changes in preparation of the publication of the English version of this document	27/07/2017
2.0	Update due to the conversion of the PKI infrastructure of the Certification Authority of the German Federal Chamber of Notaries to a native eIDAS PKI as well as editorial changes following the entry into force of the Act on Trust Services	18/09/2017
2.1	Editorial changes	13/08/2018
2.2	Editorial changes and updating	27/05/2019
2.3	Editorial changes as well as extension by contents for the introduction of remote signature pursuant to EN 319 411-2.	24/11/2020
2.4	Annual review	15/03/2021
2.5	Annual review	13/07/2022
2.6	Annual review and updating of directory service	02/02/2023
2.7	Review, adaptation of OID labelling and extension of written revocation request to include qeS	29/01/2024
2.8	Introduction of the new qualified seal service (QCP-l-qscd)	08/05/2024

Name and identification of the document

Document name:	PKI Disclosure Statement of the Certification Authority of the German Federal Chamber of Notaries for qualified certificates
Qualification (OID):	1.3.6.1.4.1.41460.5.3.1.1.2
Version:	2.8

The German version of this PKI Disclosure Statement is decisive. In case of discrepancies between the German and the English version of this document, only the German version shall apply.

This PKI Disclosure Statement is not legally binding. Instead, the relationship between the Trust Service Provider of the German Federal Chamber of Notaries (Vertrauensdiensteanbieter Bundesnotarkammer - hereinafter referred as TSP) and the certificate holder or the relying third party shall be governed exclusively by the contractual provisions or, in the absence of a contractual relationship, by the statutory provisions. This PKI Disclosure Statement does not contain any representations, warranties or guarantees unless explicitly stated otherwise.

Content

1. Contact information

1.1. General contact information

Zertifizierungsstelle der Bundesnotarkammer
Burgmauer 53
50667 Köln

Tel.: +49 (2 21) 27 79 35-0
Fax: +49 (2 21) 27 79 35-20
Email: zs@bnotk.de

1.2. Revocation of certificates

- Qualified certificates for natural persons (for qualified signatures)

Certificate holders are obliged to have issued certificates revoked if

- the certificate is lost, misused or possibly compromised,
- there is a suspicion that the signature creation data can be used by third parties,
- the information contained in the certificate no longer corresponds to the facts (e.g. change of name due to marriage), in particular if its continued use would constitute a breach of professional and/or ethical law or other legal provisions,
- the certificate issued by the TSP, which enables authentication to the TSP, has been lost, misused or possibly compromised.

Certificates should also be revoked if they are no longer needed before their validity expires. Chip cards can be rendered unusable by mechanical destruction of the chip on them or by entering the PIN incorrectly several times. The chip cards must be disposed of in accordance with the ElektroG.

- Qualified certificates for legal persons (for qualified seals)

Certificate holders are obliged to have issued certificates revoked if

- the certificate has been misused or possibly compromised,
- there is a suspicion that the signature creation data can be used by unauthorised third parties,
- at least one of the software certificates issued by the TSP, which enable authentication to the TSP, has been lost, misused or possibly compromised,
- the information contained in the seal certificate no longer corresponds to the facts (e.g. change of name of the organisation or relocation), in particular if continued use would constitute a breach of professional and/or ethical law or other legal provisions.

Certificates should also be revoked if they are no longer needed before their validity expires.

In addition to the certificate holder, the following persons are also authorised to request the revocation of the certificate:

- TSP
- authorised applicant (for qualified seals)
- third parties who have confirmed information in the certificate concerning the power of representation or professional or other information (third parties authorised to revoke)
- Federal Network Agency of Germany (Bundesnetzagentur or BNetzA).

Please note that the revocation of a certificate cannot be reversed.

1.3. Procedure for submitting a revocation request

- Qualified certificates for natural persons (for qualified signatures)

Revocation requests for qualified signature certificates can be submitted in the following ways:

1) By phone at: **(0800) 3550 400**

2) In written form

- with a handwritten signature to the following address:

  Zertifizierungsstelle der Bundesnotarkammer, Burgmauer 53, 50667 Köln

- with a qualified electronic signature via email or EGVP to the TSP

Persons authorised to revoke, who wish to submit a revocation request by telephone, must authenticate themselves by naming the agreed revocation password and providing additional personal details. If a certificate holder submits a revocation request by telephone without knowing his revocation password, he must confirm the revocation request via a one-time link sent to the email or EGVP address stored with the TSP.

A written revocation request must be signed by hand or a qualified electronic signature and the certificate to be revoked must be clearly identifiable by specifying the certificate (e.g. product or serial number) and certificate holder.

The written revocation request is checked on the basis of a specimen signature made during the application process. For certificates issued on the basis of the eIDent procedure, a written revocation is not possible due to the lack of a specimen signature.

- Qualified certificates for legal persons (for qualified seals)

Revocation requests for qualified seal certificates can be submitted in the following ways:

1) By phone at: **(0800) 3550 400**

2) In written form

- with a handwritten signature to the following address:

  Zertifizierungsstelle der Bundesnotarkammer, Burgmauer 53, 50667 Köln

- with a qualified electronic signature via email or EGVP to the TSP

Persons authorised to revoke, who wish to submit a revocation request by telephone, must

a) authenticate themselves by naming the agreed revocation password and providing additional personal details.

b) Once the revocation password and personal data have been passed on correctly, a one-time link to confirm the revocation request will be sent to the business contact address (email or EGVP mailbox) stored with the TSP.

A written revocation request must be either signed by the person authorised to revoke or signed with a qualified electronic signature. The qualified certificate to be revoked must clearly be identifiable by details of the certificate (e.g. product or serial number) and the certificate holder. In addition, the person authorised to revoke must provide evidence of legally valid power of representation of the legal person. This proof can be provided in the form of an official extract from the commercial register (not older than four weeks) or a valid power of attorney.

2. Qualified trust service

2.1. Type of qualified trust service

Trust service	Applicable policies	Relevant OID
Qualified personal certificates for natural persons on a secure signature creation device (remote signature)	▶ Certification Policy of the Certification Authority of the Federal Chamber of Notaries	▶ 1.3.6.1.4.1.41460.5.1.1.1.2
	▶ Certification Practice Statement of the Certification Authority of the Federal Chamber of Notaries	▶ 1.3.6.1.4.1.41460.5.2.1.1.2
	▶ ETSI EN 319 401, 319 411-1 und 319 411-2 (QCP-n-qscd)	▶ 0.4.0.194112.1.2
Qualified seal certificates for legal persons on a secure signature creation device (remote signature)	▶ Certification Policy of the Certification Authority of the Federal Chamber of Notaries	▶ 1.3.6.1.4.1.41460.5.1.1.1.2
	▶ Certification Practice Statement of the Certification Authority of the Federal Chamber of Notaries	▶ 1.3.6.1.4.1.41460.5.2.1.1.2
	▶ ETSI EN 319 401, 319 411-1 und 319 411-2 (QCP-l-qscd)	▶ 0.4.0.194112.1.3

With regard to these trust services, the TSP has a conformity assessment by a recognised conformity assessment body (TÜV Informationstechnik GmbH) confirming compliance with the requirements laid down in the eIDAS Regulation and the standards ETSI EN 319 401, 319 411-1 and 319 411-2 (QCP-n-qscd and QCP-l-qscd).

2.2. Restrictions of qualified certificates

- Qualified certificates for natural persons (for qualified signatures)

Qualified certificates, which are subject to the TSP certificate policies, are used to create qualified electronic signatures.

The certificate holders are responsible for ensuring that the certificates issued by the TSP are used in accordance with the contractual and legal provisions.

The use of the certificate may be restricted generally or financially. Possible restrictions of the certificate are evident in the certificate itself (e.g. restriction of the certificate holder's power of representation).

A qualified signature creation device (**QSCD**) is required to use the certificates.

- Qualified certificates for legal persons (for qualified seals)

Qualified certificates, which are subject to the TSP certificate policies, are used to create qualified electronic seals.

Applicants are responsible for ensuring that the certificates issued by the TSP are used in accordance with the contractual and statutory provisions.

A qualified signature creation device (**QSCD**) is required to use the certificates.

2.3. Retention period

The TSP archives all legally required documents for the complete documentation of the certificate life cycle for qualified certificates. The qualified certificates issued by the TSP are also stored beyond the period of their validity along with the associated revocation information and the associated records in accordance with Article 24 para. 2 lit. h of Regulation (EU) No 910/2014 for the entire period of operation of the TSP.

2.4. Trust in qualified certificates

Certificate holders, applicants, end-users and relying third parties may only trust the public key and the certificate if the following requirements are met:

- The certificate is used in accordance with the permitted types of use and any restrictions in the certificate have been observed
- The certificate chain can be successfully verified up to a trustworthy root certificate
- The validity of the certificate has been confirmed via the status request service (OCSP)
- All other agreements and other precautions have been observed

3. Obligations of applicants and certificate holders

- Qualified certificates for natural persons (for qualified signatures)

In addition to Section 5 of the TSP General Terms and Conditions, applicants or certificate holders are obliged

- to only use the certificate in legal transactions once the data it contains has been checked for correctness; the certificate is deemed to have been accepted when it is used in legal transactions,
- to stop using the certificate if there have been changes to the certificate data (e.g. change of name as a result of marriage),
- to have sole control over the signature creation data, to keep it securely in direct possession when it is provided and inaccessible to employees or third parties,
- to notify the German Federal Chamber of Notaries immediately of any obvious defects or damage to the system or procedure (malfunction notification),
- to have certificates revoked immediately if one of the reasons mentioned under 1.2 occurs,
- to check a pseudonym used for its compatibility with the rights of third parties, e.g. name rights, trademark rights, copyrights or other property rights, as well as with the general laws, to observe the restrictions (e.g. restrictions of the certificate holder's power of representation) of the certificate known to him and to use it in accordance with the usage specifications in the certification practice statement,
- not to use the certificate if it is known that the certificate has been revoked, the root certificate has been compromised or the end date of the certificate validity has passed.

Furthermore, applicants or certificate holders are subject to obligations arising from the statutory regulations and, if applicable, to further-reaching or deviating obligations based on individual contractual provisions.

- Qualified certificates for legal persons (for qualified seals)

In addition to Section 5 of the TSP General Terms and Conditions, applicants and certificate holders are obliged

- to only use the certificate in legal transactions once the data it contains has been checked for correctness; the certificate is deemed to have been accepted when it is used in legal transactions,
- to stop using the certificate if there have been changes to the certificate data (e.g. change of organisation name),

- to have control over the seal creation data, to keep it securely in direct possession when it is provided and to keep it inaccessible to unauthorised third parties when it is used by authorised employees or authorised third parties,
- to keep the password for software certificates, which enable authentication to the TSP, secret and not to pass it on to unauthorised third parties,
- to immediately notify the German Federal Chamber of Notaries of any obvious defects or damage to the system or procedure (fault report),
- to have certificates revoked immediately if one of the reasons mentioned under section 1.2 occurs,
- not to use the certificate if it is known that the certificate has been revoked, the root certificate has been compromised or the end date of the certificate validity has passed.

Furthermore, applicants or certificate holders are subject to obligations arising from the statutory regulations and, if applicable, to further-reaching or deviating obligations based on individual contractual provisions.

4. General information

4.1. Applicable agreements

The respective General Terms and Conditions of the TSP as well as any individual contractual provisions shall apply.

4.2. Exclusion of liability

An exclusion of liability is regulated in the GTC or in individual contractual.

4.3. Data protection concept

See section 9.4. of the Certificate Policy of the TSP.

4.4. Right of revocation

In the case of a contract for the provision of trust services, there is no statutory or contractual right of revocation.

4.5. Dispute resolution procedure

Complaints can be submitted in writing (Zertifizierungsstelle der Bundesnotarkammer, Burgmauer 53, 50667 Köln) or by email ((zs@bnotk.de or bea@bnotk.de) to the TSP.

4.6. Applicable law

German law shall apply exclusively to the exclusion of the United Nations Convention on Contracts for the International Sale of Goods of 11 April 1980 ('UN Sales Convention') and such provisions that may lead to the application of foreign law.

4.7. Publications and directories

In addition, the TSP provides an online service (OCSP) for querying the validity of the certificates issued by the TSP. The status of the qualified certificates issued by the TSP can be retrieved for a period of at least 10 years after the end of the validity of the respective certificate.

The EU Trusted List in accordance with eIDAS Regulation (EU) No. 910/2014, for example, can be used to check the trust status. The EU Trusted List is available via the following link:
https://digital-strategy.ec.europa.eu/en/policies/eu-trusted-lists

***

https://zertifizierungsstelle.bnotk.de/