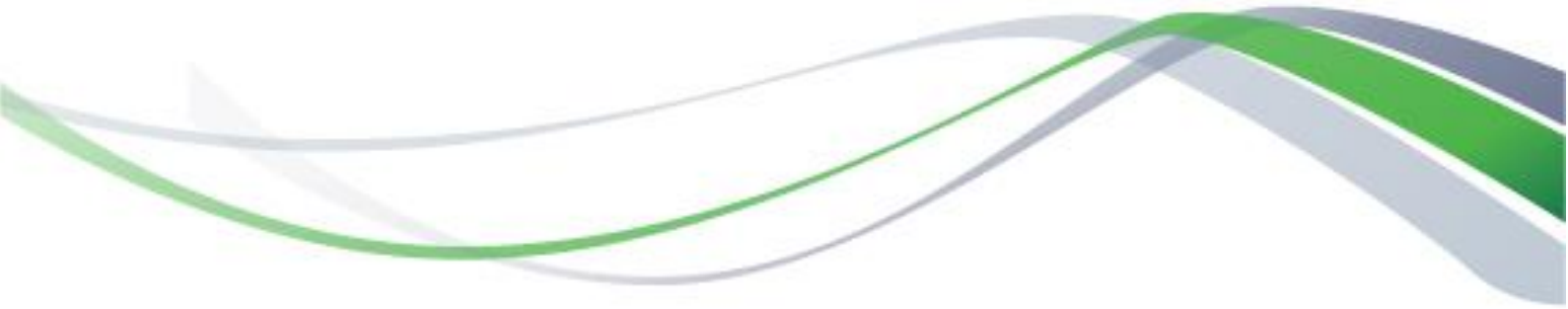
BUNDESNOTARKAMMER
ZERTIFIZIERUNGSSTELLE

PKI Disclosure Statement of the certification authority of the Bundesnotarkammer for qualified certificates



Version	**2.2**
Date	**11.06.2019**

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	24.07.2017
1.1	Editorial changes in preparation of the publication of the English version of the document	27.07.2017
2.0	Update due to the conversion of the PKI-infrastructure of the certification authority of the Bundesnotarkammer 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	31.05.2018
2.2	Editorial changes and actualization with regards to content	11.06.2019

Name and qualification of the document

Document name: Public Disclosure Statement from the certification authority of the Bundesnotarkammer for qualified electronic certificates

Qualification (OID): 1.3.6.1.4.1.41460.5.3.1.1.2.2.2

Version: 2.2

The German version of this PKI Disclosure Statement is decisive. Therefore, in case of any discrepancies between the German and the English version of this document, the German version shall prevail.

This PKI Disclosure Statement is not legally binding. The relationship between the TSP BNotK and the Certificate Holder or a Relying Party is solely governed by the contractual agreement or, if no contractual relationship exists, by the applicable statutory law. This PKI Disclosure Statement does not contain any representations, warranties or guarantees unless explicitly stated otherwise.

Contents

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
E-Mail: zs@bnotk.de

1.2. Revocation of certificates

Certificate holders are obligated to revoke issued certificates if

- the QSCD or the certificate is lost, has been misused or potentially compromised,
- the information contained in the certificate no longer corresponds to the facts, in particular if there is a violation of professional and/or the notarial code of conduct or other legal provisions.

Revocation requests can be submitted (1) by phone at (0800) 3550 400, (2) in writing with a handwritten signature to the following address: Zertifizierungsstelle der BNotK, Burgmauer 53, 50667 Köln as well as – by notaries – via (3) the web interface of the TSP BNotK at: https://zertifizierungsstelle.bnotk.de.

Persons entitled to revoke a certificate who wish to submit a revocation request by phone have to authenticate themselves by mentioning the agreed revocation password and other personal data.

The written revocation request has to be signed by hand and has to clearly describe the certificate to be revoked by providing information relating to the certificate and the certificate holder.

In addition to the certificate holder, the following persons are entitled to request a revocation of the certificate:

- the TSP BNotK,
- third parties who have confirmed the information in the certificate on representative powers or related to the profession or any other information (*third parties entitled to revoke a certificate*) as well as
- the Federal Network Agency (*Bundesnetzagentur or BNetzA*).

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

2. Qualified trust service

2.1. Type of qualified trust service

Trust service	Applicable directives	Relevant OID
Qualified certificates for natural persons	▶ Certificate policy (CP) of the certification authority of the Bundesnotarkammer	▶ 1.3.6.1.4.1.41460.5.1.1.1.2.1.3
	▶ Certificate practice statement (CPS) of the certification authority of the Bundesnotarkammer	▶ 1.3.6.1.4.1.41460.5.2.1.1.2.2.3
	▶ ETSI EN EN 319 401, 319 411-1 and 319 411-2 (QCP-n-qscd)	

The trust service provider (TSP) BNotK disposes of a conformity assessment for the trust service made by a recognized conformity assessment body (*TÜV Informationstechnik GmbH*) which confirms the compliance with the requirements set out in the eIDAS regulation and by the ETSI EN 319 401, 319 411-1 and 319 411-2 (QCP-n-qscd) standards.

2.2. Restrictions of the qualified certificates

Qualified certificates subject to the Certificate Policy of the TSP BNotK are used to create certified electronic signatures.

Certificate holders shall only use the certificates for professional purposes and not export the private key from the QSCD. The certificate holders are responsible for ensuring that the certificates issued by the TSP BNotK are used in accordance with the contractual and legal provisions.

The use of the certificate can be restricted in general or financially. Possible restrictions of the certificate can be found in the certificate itself (e.g. restriction of the certificate holder's power of representation).

A qualified electronic signature creation device (***QSCD***) is required for the use of the certificates.

2.3. Retention period

The TSP BNotK archives all legally required documents for the purpose of complete documentation of the certificate life cycle for qualified certificates. The retention period of the documentation meets the legal requirements for qualified certificates and extends over at least 30 more years from the end of the year in which the certificate expires.

2.4. Trust in qualified certificates

The certificate holder and relying third parties shall only trust the public key and the certificate if the following conditions are met:

- the certificate is used in accordance with the allowed types of use and the possible restrictions of the certificate have been observed,
- the certificate chain can be verified and traced back to a trusted root certificate,
- the validity of the certificate has been confirmed through the Qualified Certificate Status Service (OCSP),
- all further agreements and other precautionary measures have been observed.

3. Obligations of the certificate holders

In accordance with Sec. 45 of the General Terms and Conditions of the TSP BNotK, the certificate holder is in particular obligated to

1. pay the agreed fees on time according to the price list valid at the time of conclusion of the contract;

2. provide the cooperation services necessary for the Bundesnotarkammer in order to fully provide the services

3. provide all data necessary for the request completely and truthfully and provide the required evidence; changes of data have to be notified to the Bundesnotarkammer without delay;

4. designate a bank account of a bank entitled to do business in Germany for banking transactions related to the collection of fees and to issue a valid SEPA direct debit mandate and to make sure that sufficient coverage in the designated bank account is provided;

5. electronically acknowledge receipt of the QSCD upon delivery;

6. keep the QSCD in safe custody and to not to make the PIN or request number accessible to employees or third parties;

7. immediately give notice to the Bundesnotarkammer of any obvious system defects (error message);

8. immediately report any loss or misuse of the QSCD or the certificate and request the revocation of the concerned certificate;

9. immediately revoke certificates if the information contained therein no longer corresponds to the facts, in particular if subsequent use would breach professional law, the notarial code of conduct or other legal provisions;

10. verify if a pseudonym used is consistent with the rights of third parties, e.g. trademark, copyright or other protective rights, as well as with general laws;

11. immediately revoke the certificate if four weeks after the delivery of the electronic signature or chip card he has not yet received the transport initial PIN notification as well as to properly destroy the electronic signature or chip card and to apply for a new electronic signature or chip card at the Bundesnotarkammer.

12. observe restrictions (e.g. the restrictions of the certificate holder's power of representation) of the certificate known to him and not to use the certificate or the chip and signature card if he is aware that the certificate has been revoked or the root certificate has been compromised.

If, following identification, the certificate holder does not provide necessary cooperation services as requested by the TSP BNotK, he/she has to reimburse the expense incurred to the TSP BNotK unless the certificate holder proves that no costs or costs to a substantially lower amount were incurred. In case of unsuccessful delivery of the signature card for a reason which is in the responsibility of the certificate holder costs amounting to 3, 00 EUR are incurred per delivery attempt and in case of issuance of an incorrect continuation card and the exchange by a replacement card for a reason for which the client is responsible the costs incurred amount to 20, 00 EUR.

After termination of the contract, the certificate holder has to make sure that the certificate is revoked and properly destroy the electronic signature or chip card.

Furthermore, the certificate holder is subject to the obligations arising from the statutory provisions as well as, if applicable, to further or deviating obligations based on individual contractual arrangements.

4. General information

4.1. Applicable agreements

The General Terms and Conditions of the TSP BNotK as well as individual contractual agreements apply.

4.2. Disclaimer

A disclaimer is set out in the General Terms and Conditions or in individual contracts.

4.3. Data protection concept

See no. 9.4. of the Certificate Policy of the TSP BNotK.

4.4. Withdrawal

It is not possible to withdraw the declaration of consent made for the conclusion of a contract on the subscription of certification services provided by the TSP BNotK.

4.5. Dispute resolution procedure

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

4.6. Applicable law

German law applies if foreign law is not mandatory.

4.7. Publications and directories

Certificates issued by the TSP BNotK are kept publicly accessible if the certificate holder approves the publication. For this purpose, the TSP BNotK publishes the certificates in a publicly accessible LDAP directory. Besides, the TSP BNotK provides an online service (OCSP) to check the validity of the certificates issued by the TSP.

The qualified certificates are published at the following internet addresses: ldap://ldap.zs.bnotk.de and ldap://ldap.bnotk.de.

The status of the qualified certificates issued by the TSP BNotK can be verified for at least up to 10 years after the expiration date of the certificate.

The trusted list of the Federal Network Agency (*Bundesnetzagentur*) is available at the following internet address: https://www.nrca-ds.de.

***

BUNDESNOTARKAMMER
ZERTIFIZIERUNGSSTELLE

https://zertifizierungsstelle.bnotk.de/