BUNDESNOTARKAMMER
ZERTIFIZIERUNGSSTELLE

Certificate Policy of the Certification Authority of the German Federal Chamber of Notaries

Version: 1.8

Date: 05 April 2024

Document history

Version	Remarks	Date
1.0	Creation of the document as part of the verification of compliance with the requirements of 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/EC (the ***eIDAS Regulation***) by an accredited conformity assessment body.	20/06/2017
1.1	Editorial changes to adapt to the requirements of the German Trust Services Act [Vertrauensdienstegesetz]	28/02/2018
1.2	Editorial adjustment and update due to further development of the application landscape (application, verification and production system) of the certification authority.	31/05/2018
1.3	Editorial changes and updating	27/05/2019
1.4	Editorial changes	11/06/2020
1.5	Editorial changes and updating	30/05/2022
1.6	Review and amendment of service certificates	16/03/2023
1.7	Review and adjustment of OID labelling	29/01/2024
1.8	Expansion to include the new eSiegel trust service	05/04/2024

Content

1 Introduction

1.1 Overview

The German Federal Chamber of Notaries is a qualified trust service provider within the meaning of Art. 3 lit. 20 of the eIDAS Regulation. The trust services offered are qualified certificates for electronic signatures for natural persons (QCP-n-qscd), qualified certificates for electronic seals for legal persons (QCP-l-qscd) and qualified electronic time-stamps. The use of qualified certificates for electronic signatures and electronic seals for remote sealing requires the use of a qualified electronic signature creation device (the ***QSCD***).

With regard to these trust services, the TSP has conformity assessments by a recognised conformity assessment body 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 or ETSI EN 319 421.

This document is the Certificate Policy (**CP**) of the Certification Authority of the German Federal Chamber of Notaries (Zertifizierungsstelle der Bundesnotarkammer [- also the **Trust Service Provider German Federal Chamber of Notaries** –hereinafter referred as **TSP**]) for these trust services and represents the requirements and specifications for Public Key Infrastructure (the ***PKI***) operated by the Certification Authority of the German Federal Chamber of Notaries. The head of the certification authority ensures that the requirements and specifications of the certificate policy are implemented within the TSP.

The structure of the certificate policy is based on the RFC 3647 standard to facilitate comparison with the certificate policies of other trust service providers.

Only the German version of this certificate policy is authoritative. In case of discrepancies between the German and the English version of this document, only the German version shall apply.

The relationship between the TSP and the certificate holder or the relying third party shall be governed exclusively by the contractual, legal or statutory provisions. The certificate policy applies in addition to and is subordinate to the General Terms and Conditions of the TSP. These can be found at: https://zertifizierungsstelle.bnotk.de/agb.

Unless expressly agreed otherwise, the certificate policy does not contain any assurances, guarantees or warranties.

1.2 Name and identification of the document

Document name: Certificate Policy of the Certification Authority of the German Federal Chamber of Notaries

Identification (OID): 1.3.6.1.4.1.41460.5.1.1.1.2
Version: 1.8

1.3 PKI participant

1.3.1 Certification Authority

The certification authority (***CA***) issues certificates and provides information on their status.

The TSP currently issues the following types of certificates:

- Qualified personal certificates for natural persons
- Qualified seal certificates for legal persons
- Service certificates
- Qualified electronic time-stamps

Non-qualified certificates are not included.

1.3.2 Registration authorities

The registration authority (***RA***) identifies and authenticates certificate holders and applicants, records and verifies requests for the provision of trust services by the certification authority. The TSP itself performs the tasks of the registration authority. Requests for revocation of a certificate issued by the certification authority are also recorded, checked and forwarded to the certification authority by the registration authority.

1.3.3 Applicants and certificate holders

Applicants (also known as **subscribers**) are natural persons who apply for certificates issued by the Certification Authority. Certificate holders (also known as **subjects**) are natural or legal persons who hold the issued certificates. The certificate holder's identity is linked to the certificate and the associated key pair.

The applicants for and holders of the certificates for natural persons for electronic signatures (issued according to policy QCP-n-qscd) issued by the TSP are identical.

The TSP only issues certificates within the scope of its responsibilities in accordance with the Federal Regulations for Notaries (pursuant to Section 78 BNotO). This includes, in particular, supporting

notaries in the area of electronic legal and official authority business, as well as operating the video communication system in accordance with Section 78p BNotO.

For certificates issued for electronic seals (issued according to policy QCP-l-qscd), the certificate holder is a legal person and the applicant is a natural person who is authorised to represent the legal entity.

The TSP issues certificates for legal persons for seals exclusively to legal and judicial organisations.

The TSP reserves the right to issue certificates to other persons in the professional environment of the German notarial profession or the German judiciary.

Certificates are issued to employees of the German Federal Chamber of Notaries public body as certificate users if and insofar as this is necessary.

1.3.4 End-users

End-users are all persons who are authorised to initiate a signature or seal process.

The end-user of the key of a qualified signature certificate (signature key) for natural persons is exclusively the certificate holder.

The end-users of the key for a qualified seal certificate (seal creation key) for legal entities are the authorised applicant and natural persons who are authorised by the certificate holder to initiate a sealing process.

1.3.5 Relying third parties

Relying third parties (also the ***relying party***) are natural or legal persons or other third parties, such as authorities, who rely on the trustworthiness of the certificates issued by the TSP.

1.3.6 Other participants

Other participants are third parties to whom the certification authority has transferred functions and/or tasks (the ***other participants***).

In selected cases, the TSP has transferred certification/registration authority tasks to third parties. The requirements and specifications for the transfer of tasks to third parties are described in the security concept of the TSP.

1.4 Use of certificates

- Certificates for electronic signatures for natural persons

Signature certificates subject to this certificate policy may in principle only be used by the certificate holders for professional purposes. 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 TSP accepts no liability in the event that a certificate holder uses a certificate for other than professional purposes.

- Certificates for electronic seals for legal persons

Seal certificates subject to this certificate policy may in principle only be used by the applicants or other end-user for professional purposes. The applicants are responsible for ensuring that the certificates issued by the TSP are used in accordance with the contractual and legal provisions. The TSP accepts no liability in the event that an end-user uses a certificate for other than professional purposes.

Regulations deviating from this require a written agreement with the TSP.

Further regulations are described in the certification practice statement belonging to the certificate.

1.4.1 Use of service certificates

The TSP uses service certificates for internal use to provide trust services in accordance with eIDAS. They are issued by the TSP.

Service certificates are used for following purposes:

- CA certificates for generating CAs and certificates
- Signature of status information (OCSP)
- Signature of time-stamps

1.5 Administration of the Certificate Policy

This Certificate Policy is administered by the Certification Authority of the German Federal Chamber of Notaries. It is reviewed regularly, at least every 12 months, and updated if necessary. A review is carried out in particular in the event of a change in the legal situation as well as in the event of a change in operational procedures. The head of the Certification Authority of the German Federal Chamber of Notaries or, if he is prevented, his designated deputy is responsible.

Amendments may only be made by the head of the Certification Authority of the German Federal Chamber of Notaries or, if he is unable to do so, by his designated deputy. Pursuant to an operational instruction, amendments are only published if approved by the head of the Certification Authority of the German Federal Chamber of Notaries or, if he is unable to do so, by his designated deputy. The amended version is published without delay. The change is indicated by the assignment of a new version number.

The contact person responsible for administration can be reached at the following address:

Zertifizierungsstelle der Bundesnotarkammer
c/o Leiter der Zertifizierungsstelle (head of the certification authority)
Burgmauer 53
50667 Köln

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

1.6 Definitions and abbreviations

Term	Description
GTC	General Terms and Conditions for the Certification Service of the German Federal Chamber of Notaries (German abbreviation "AGB")
Other participants	See section 1.3.6
BDSG	German Federal Data Protection Act (Bundesdatenschutzgesetz)
BNetzA	Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railway
CA/Certificate Authority	See certification authority
GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data, on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation)
eIDAS regulation	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/EC
LDAP	Lightweight Directory Access Protocol
OCSP	Online Certificate Status Protocol

Term	Description
PKI	Public Key Infrastructure
QCP-n	Qualified certificate policy for qualified certificates issued to natural persons
QCP-n-qscd	Qualified certificate policy for qualified certificates issued to natural persons holding a private key for the certified public key in a QSCD
QSCD	Qualified electronic signature creation device as defined in Art. 3 lit. 23 eIDAS
RA/Registration Authority	See Registration Authority
Registration Authority	See section 1.3.2
Root CA	Uppermost certification authority of a PKI
Third Parties Entitled to Revocation	See Section 4.4.3. of the Certification Practice Statement of the Certification Authority of the German Federal Chamber of Notaries
TSP	Certification Authority of the German Federal Chamber of Notaries
Relying third parties	See section 1.3.5
VDG	German Trust Services Act (Vertrauensdienstegesetz)
Certificate	Qualified certificate for electronic signatures within the meaning of Section 3 No. 15 eIDAS Regulation
Certificate holder	See section 1.3.3
Certification Authority	See section 1.3.1

1.7 Transfer of tasks to third parties

The transfer of tasks to third parties takes place on the basis of and in accordance with a private law agreement. The contractual agreements ensure that the legal requirements resulting from the delegation of tasks and the regulations of the certificate policy, the certification practice statement (if required) and the security concept are complied with. The contracts with the third parties also contain the obligation to cooperate in internal and external audits as well as to enable inspection visits by the competent supervisory authority. The tasks and obligations of the third parties are specified in the respective contractual agreement.

The third parties pledge to appoint only reliable, adequately trained and competent employees to perform the tasks transferred to them by the TSP. The TSP has the option to exclude unreliable employees of the commissioned third party from the process. The TSP has the right to inspect the third party's documentation regarding the reliability and expertise of the staff employed.

The TSP has (partially) transferred tasks to third parties in the following areas:

- Hotline for telephone revocation requests regarding qualified certificates
- Operation of the computer centre

Even when tasks are transferred to third parties, the overall responsibility for the operation of the trust service remains in the hands of the TSP. If the third parties violate their contractual obligations, the TSP may be entitled to claim damages.

Details on this are laid down in the security concept.

1.8 Contact

Please address enquiries to the TSP to the following person:

Leiter der 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

2 Directories and Publications

2.1 Directories

The TSP provides an online service (***OCSP***) for querying the validity of the certificates issued by the VDA.

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.

Further details can be found in the applicable certification practice statement of the certificate in section 2.1.

2.2 Publication of information on certificates

This regulation is described in the applicable certification practice statement for the certificate in section 2.2.

2.3 Timing and frequency of publications

This certificate policy, the respective certification practice statements as well as the certifications of the conformity assessment bodies are published and are available on the website of the TSP under the following link: https://zertifizierungsstelle.bnotk.de/veroeffentlichungen

In case of updating, the new versions will be published.

Further regulations are described in the respective applicable certification practice statement for the certificate in section 2.3.

2.4 Access to information

The General Terms and Conditions (https://zertifizierungsstelle.bnotk.de/agb) as well as certificates, the Certificate Policy, the Certification Practice Statement and the PKI Disclosure Statement (PDS) are publicly accessible free of charge at the following address: https://zertifizierungsstelle.bnotk.de/veroeffentlichungen. There are no restrictions on read access. Changes to the content are made exclusively by the TSP. The TSP shall ensure that access is possible at all times. Faults in access will be remedied without delay.

2.5 Accessibility

The promotion and improvement of comprehensive access to and unrestricted opportunities for use of all areas of life for people with disabilities is a particular concern of the German Federal Chamber of Notaries.

Unfortunately, the qualified certificates for electronic signatures and electronic seals offered by the Certification Authority of the German Federal Chamber of Notaries are currently not accessible and usable without barriers. Special hardware and software is required to use the trust service, including

a card reader and a software suitable for creating an electronic signature. These components are currently not available in a version usable by persons with disabilities.

The above applies in the same way to the qualified time-stamps offered by the Certification Authority of the German Federal Chamber of Notaries.

The TSP is striving to offer its services in a barrier-free manner and to provide largely barrier-free internet content (including easy-to-read and sign language) in accordance with the Barrier-Free Information Technology Ordinance (BITV) - BITV 2.0.

3 Identification and authentication

- Certificates for electronic signatures for natural persons

The identification and authentication of certificate holders complies with legal requirements and is based on product- and customer-specific requirements.

- Certificates for electronic seals for legal persons

The identification and authentication of certificate holders and applicants, as well as the verification of the applicant's right of representation, complies with the legal requirements and is based on product- and customer-specific requirements.

Details are described in section 3 of the certification practice statement.

4 Operating requirements

The operational requirements for certificates of the TSP comply with the legal requirements and are based on product- and customer-specific requirements.

Details are described in the certification practice statement.

5 Non-technical security measures

The TSP has introduced non-technical security measures that meet the legal requirements.

Details are described in the certification practice statement.

5.1 Information Security Guideline

The management of the German Federal Chamber of Notaries has issued a guideline on information security which contains the minimum requirements for all IT systems and IT-supported specialist procedures developed and operated by the German Federal Chamber of Notaries, including the TSP, its subordinate authorities, companies and other institutions The guideline applies to all employees of the German Federal Chamber of Notaries, its subordinate authorities, companies and other institutions as well as third parties commissioned by it. It is set down in writing and has been made known to the employees of the TSP concerned. It is implemented and maintained in the TSP and in all trust services offered.

The information security guideline is reviewed and, if necessary, updated at regular intervals, at least every 24 months, and in the event of significant changes. Changes require the approval of the management of the German Federal Chamber of Notaries.

Third parties, including certificate holders (*subscriber*), applicants and third parties, including relying third parties, conformity assessment bodies as well as supervisory authorities, shall be informed of changes to the information security guideline if and to the extent required.

5.2 Asset Management

The TSP ensures an adequate level of security of its assets, including information assets. The procedures for protecting the information assets are documented in the TSP's security concept. The IT systems used are noted in a list of components. The respective security level complies with the legal requirements.

Control mechanisms are in place to prevent (i) loss, damage or compromise of the components used as well as the interruption of business operations and (ii) the theft or compromise of sensitive information.

All media will be stored securely. Sensitive data contained on media that is disposed of will be securely erased.

6 Technical security measures

The TSP has implemented technical security measures in line with legal requirements.

Details are described in the certification practice statement.

7 Certificate profiles, revocation lists and OCSPs

Details are described in the certification practice statement.

8 Compliance check

The TSP operates the trust service in accordance with applicable law.

An accredited conformity assessment body checks at regular intervals that the TSP meets the legal requirements. Regular repeat audits take place. In addition, audits are carried out on an ad hoc basis, e.g. when safety-relevant changes are made to the TSP's work processes.

The results of the audits are not published. If deficiencies are found during the audit, these are rectified in consultation between the TSP and the auditor.

Furthermore, internal audits are carried out regularly, at least every 24 months, to check compliance with the established rules and procedures for the proper and secure operation of the TSP (including the implementation of and compliance with the requirements of the certificate policy and the respective certification practice statement as well as a review of the component list). Details of the audit, the audit objects and processes are specified in the TSP security concept.

In addition, the TSP conducts a risk analysis on a regular basis, but at least every 24 months, in order to identify, analyse and evaluate the risks for the trust services offered. Both technical and operational requirements are taken into account. This also includes a consideration of information assets. The leading roles of the TSP are responsible for this. A new risk analysis is carried out in particular in the event of a significant change in the threat situation. The TSP takes appropriate countermeasures in consideration of the risk analysis. It is ensured that the security level corresponds to the risk level. The residual risks identified in the risk analysis are evaluated and accepted by the leading roles of the TSP. Details are laid down in the security concept of the TSP. In particular, the necessary security requirements and the operational procedures of the TSP are defined in this concept. The security concept is adapted if the risk analysis comes to the conclusion that new risks have arisen and further countermeasures are required.

In order to verify compliance with its obligations, the TSP shall - in accordance with the statutory provisions - submit the relevant books, records, vouchers, documents and other records to the supervisory authority for inspection at the latter's request, even if they are kept in electronic form.

9 Other business and legal regulations

9.1 Fees

9.1.1 Fees for issue of certificates

Fees for issuing and receiving a certificate are based on the agreement concluded with the applicant.

9.1.2 Fees for access to certificates

No fees are charged for access to the directory service.

9.1.3 Fees for revocation of certificates or receipt of status information

No fees are charged for revoking certificates or obtaining status information.

9.1.4 Fees for other services

Insofar as other services are offered, the fees shall be based on the agreements with the applicant or the respective GTC.

9.1.5 Reimbursement of costs

The agreements with the applicant or the respective GTC apply.

9.2 Financial responsibility

The TSP has the necessary funds at its disposal to operate trust services properly. They are obtained by charging fees for the provision and use of the trust services of the TSP.

In addition, the TSP has adequate liability insurance Art. 24 Para. 2 lit. c) eIDAS Regulation.

9.3 Confidentiality of business data

No information provided.

9.4 Protection of personal data

The TSP complies with the statutory provisions on data protection.

9.4.1 Data protection concept

The TSP processes personal data in accordance with the statutory provisions of the European General Data Protection Regulation 2016/679 (GDPR) and the German Federal Data Protection Act (BDSG).

9.4.2 Definition of personal data

Personal data is any information relating to an identified or identifiable natural person.

9.4.3 Non-confidential data

All information and data explicitly or implicitly contained in or derivable from the certificates issued by the TSP and in the directories referred to in section 2 shall be treated as non-confidential data.

9.4.4 Responsibility for the protection of personal data

The TSP is responsible for the protection of personal data.

The data protection officer of the TSP ensures compliance with the legal provisions on data protection. He draws up data protection policies, is available as a contact person in data protection matters and obliges the employees of the TSP to observe the data protection policies.

9.4.5 Notice and consent to the use of personal data

When the application is submitted, the applicant will be informed which personal data will be included on the certificate. Any collection of data from third parties will be in accordance with the provisions of Section 8 para. 1 VDG, as well as the other provisions of the German Data Protection Act. Information in the sense of Art. 14 GDPR is provided in text form in the course of the application procedure.

9.4.6 Disclosure of data in the context of a legal obligation

The TSP is governed by the statutory provisions set out in the European General Data Protection Regulation 2016/679 (GDPR), the German Federal Data Protection Act (BDSG), the German Trust Services Act (VDG) and the laws of the Federal Republic of Germany.

The TSP may transmit personal data to the relevant bodies in the event of a legal claim in accordance with Section 8 para. 2 VDG and under the conditions of Section 6 para. 1c GDPR and Article 24 BDSG.

The transmission of the data is documented in accordance with Section 8 para. 3 VDG and stored for a period of 12 months.

Requests for information should be addressed to the data protection officer of the German Federal Chamber of Notaries:

Datenschutzbeauftragte

c/o Bundesnotarkammer

Mohrenstraße 34

10117 Berlin

Email: datenschutz@bnotk.de

9.4.7 Copyright

No information provided.

9.5 Representations, warranties and guarantees

This certificate policy does not contain any representations, warranties or guarantees of the TSP.

In the relationship with certificate holders, relying third parties and all other persons, only the relevant provisions in the GTC or the respective individual contractual agreement as well as the statutory provisions shall apply.

9.6 Exclusion of liability

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

9.7 Release from liability

No information provided.

9.8 Term and termination

No information provided.

9.9 Notices to and communication with participants

No information provided.

9.10 Amendment of the Certificate Policy

No information provided.

9.11 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.

9.12 Applicable law

German law shall apply unless foreign law is mandatory.

The TSP is operated in accordance with the provisions of the German General Equal Treatment Act (Allgemeines Gleichbehandlungsgesetz).

9.13 Compliance with applicable law

- Certificates for electronic signatures for natural persons

The respective certificate holder is responsible for ensuring that the certificates issued by the TSP are used in compliance with the applicable law.

- Certificates for electronic seals for legal persons

The respective applicant is responsible for ensuring that the certificates issued by the TSP are used in compliance with the applicable law.

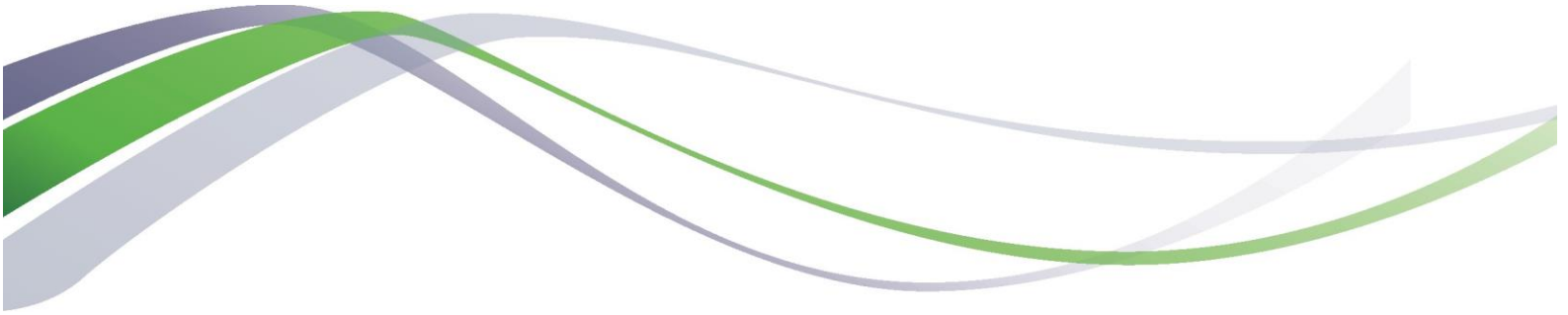
9.14 Other provisions

No information provided.

9.15 Other provisions

No information provided

***



https://zertifizierungsstelle.bnotk.de/