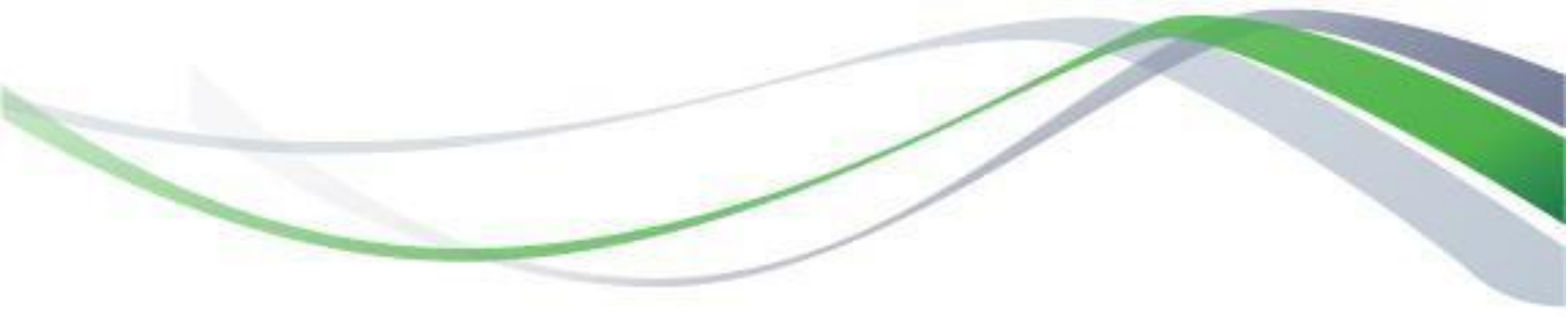
BUNDESNOTARKAMMER
ZERTIFIZIERUNGSSTELLE

Certificate Practice Statement of the Certification Authority of the German Federal Chamber of Notaries for qualified certificates



Version: 3.4

Date: 25 July 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
2.0	Update due to the conversion of the PKI infrastructure of the Certification Authority of the 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.	18/10/ 2017
2.1	Update due to new certificate hierarchy.	28/02/2018
2.2	Editorial adjustment and update due to further development of the application landscape (application, verification and production system) of the certification authority.	15/08/2018
2.3	Editorial changes as well as adjustments with regard to the Federal Network Agency's (BNetzA) decree pursuant to Section 11 VDG on recognised "other identification methods".	07/06/2019
2.4	Update CA hierarchy.	15/06/2020
2.5	Editorial changes as well as extension by contents for the introduction of remote signature pursuant to EN 319 411-2.	09/12/2020
2.6	Review and addition of ECC to certificate profile.	31/05/2021
2.7	Update certificate profile of end-user certificates.	07/12/2021
2.8	Update CA hierarchy.	31/03/2022
2.9	Update eIDent with eIDAS token.	30/05/2022
3.0	Detailing attribute “countryName” in certificate profiles.	07/07/2022

3.1	Introduction of service certificates and OCSP extensions.	28/03/2023
3.2	Update certificate hierarchy after introducing a new TSA signer.	06/06/2023
3.3	Review, adjustment of OID labelling and addition of revocation via qeS.	29/01/2024
3.4	Introduction of new qualified sealing service (QCP-l-qscd).	22/07/2024

Content

1 Introduction

1.1 Overview

1.1.1 About this document

The German Federal Chamber of Notaries is a qualified trust service provider in the sense of Art. 3 lit. 20 of the eIDAS Regulation (EU) No. 910/2014. Trust services offered are qualified certificates for electronic signatures for natural persons (QCP-n-qscd), qualified certificates for electronic seals for legal persons (QCP-n-qscd) and qualified electronic time-stamps. The use of the qualified certificates requires the use of a qualified electronic signature creation device (**QSCD**) or a qualified seal creation device (QSCD).

This is the Certificate Practice Statement (**CPS**) of the Certification Authority of the German Federal Chamber of Notaries (Zertifizierungsstelle der Bundesnotarkammer - hereinafter referred as **TSP**) for qualified certificates for electronic signatures and electronic seals (**qualified certificates** or ***qualified certificate***) and represents the requirements of the certification body of the German Federal Chamber of Notaries for and the procedure in the issue, administration, revocation and renewal of the qualified certificates it issues. Non-qualified certificates are not covered.

The Certificate Practice Statement refers to the Certificate Policy of the Certification Authority of the German Federal Chamber of Notaries with the OID 1.3.6.1.4.1.41460.5.1.1.1.2 as well as the ETSI standards EN 319 401, EN 319 411-1 and EN 319 411-2. It describes the implementation of the resulting requirements.

This Certificate Practice Statement is published on the website of the TSP under the following link: https://zertifizierungsstelle.bnotk.de/veroeffentlichungen.

The structure of the Certificate Practice Statement is based on the RFC 3647 standard to facilitate comparison with the certification practice statements of other trust service providers.

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

This Certificate Practice Statement is not legally binding. Instead, the relationship between the 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. Unless expressly stated otherwise, this Certificate Practice Statement does not contain any assurances, guarantees or warranties.

1.1.2 Properties of the PKI of the Certification Authority of the German Federal Chamber of Notaries

PKI for qualified trust services

The qualified PKI of the German Federal Chamber of Notaries consists of a root CA and sub-/issuing CAs derived from it. End-user certificates are signed by the respective sub-CAs.

RSA algorithm

Active

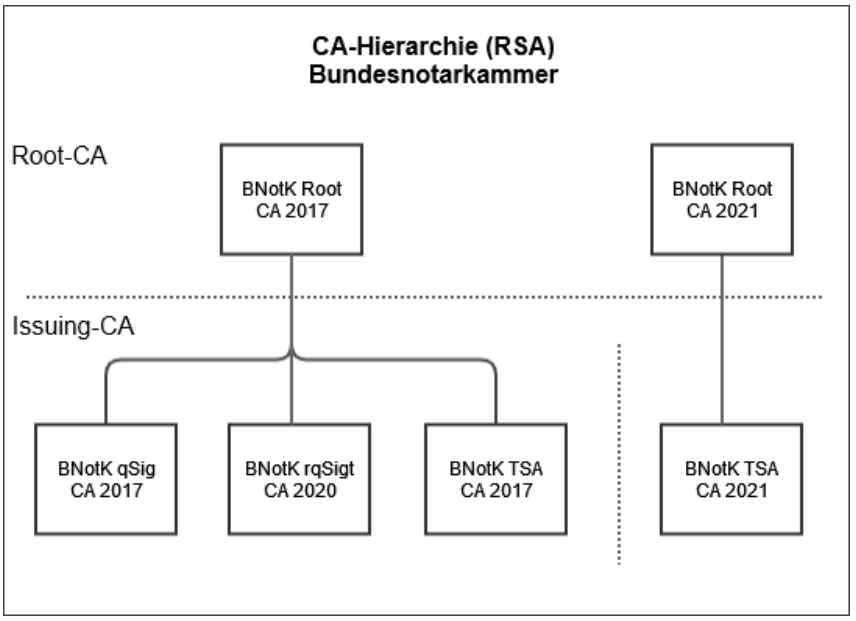


Figure 1: Active PKI hierarchy for qualified signature certificates for natural persons and qualified time-stamps with RSA

Planned

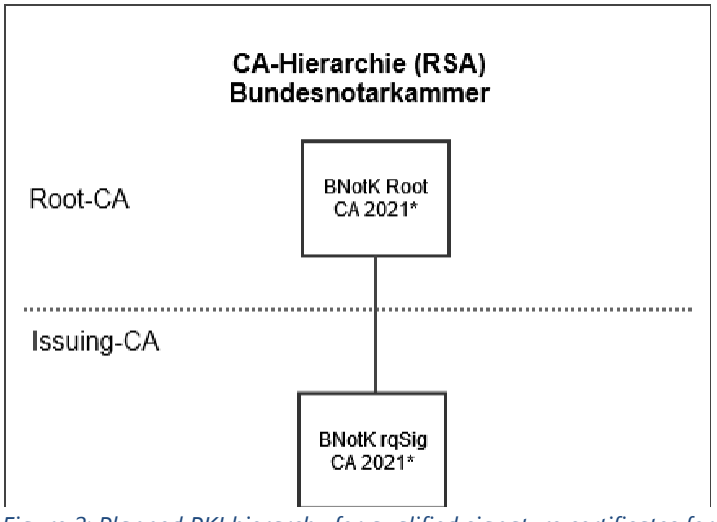


Figure 2: Planned PKI hierarchy for qualified signature certificates for natural persons with RSA

Elliptic Curve

Active

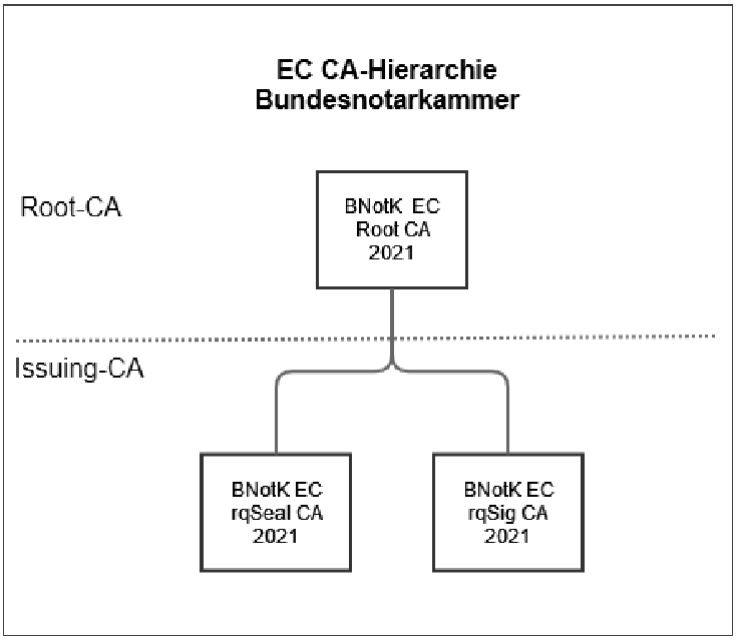


Figure 3: Active PKI hierarchy for qualified signature certificates for natural persons and legal persons with elliptic curve

Planned

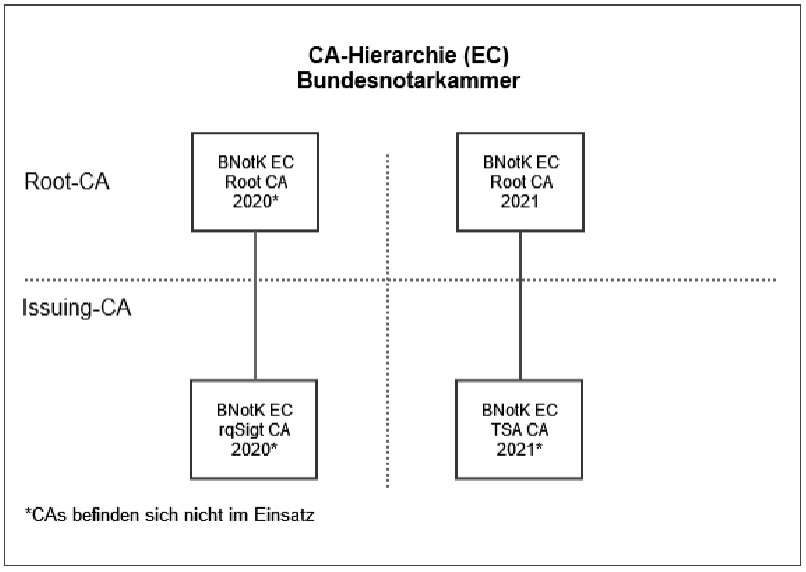


Figure 4: Planned PKI hierarchy for qualified certificates for natural persons and qualified time-stamps with elliptic curve

Qualified certificates

The issued end-user certificates comply with the requirements of the eIDAS regulation (EU 910/2014) as well as the following certification level according to ETSI EN 319 411-2:

QCP-n-qscd - qualified personal certificates on qualified signature creation device. QCP-l-

qscd - qualified seal certificates on qualified signature creation device.

1.2 Name and identification of the document

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

Labelling (OID): 1.3.6.1.4.1.41460.5.2.1.1.2

Version: 3.4

1.3 PKI participant

See section 1.3 of the Certification Policy (*CP*) of the Certification Authority of the German Federal Chamber of Notaries.

1.4 Use of certificates

Certificate holders may only use the qualified certificates issued by the TSP for their own professional purposes for qualified electronic signatures. In this respect, they act on their own responsibility. The assessment of whether this Certificate Practice Statement meets the requirements of an application and whether the use of the qualified certificate in question is suitable for a particular purpose is the responsibility of the certificate holder. The TSP accepts no liability in the event that a certificate holder uses a qualified certificate for other than professional purposes.

A (remote) QSCD is required for the use of the qualified certificates. Furthermore, the certificate holder is subject to the obligations arising from the statutory regulations and, if applicable, to further-reaching or deviating obligations based on individual contractual provisions.

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 in the following cases:

- CA certificates for creating CAs and certificates

- Status information (OCSP) signatures
- Signature of time-stamps

1.5 Management of the Certification Practice Statement

The Certificate Practice Statement is managed by the Certification Authority of the German Federal Chamber of Notaries. It is reviewed regularly, at least every 12 months, and updated if necessary. The Certificate Practice Statement is reviewed in particular in the event of a change in the laws that are essential for the TSP and in the event of a change in operational procedures. The head of the Certification Authority of the German Federal Chamber of Notaries is responsible or, if he is prevented from doing so, his designated deputy. In the event of a change, the amended version is published immediately on the TSP website. If serious changes to the contents of the Certificate Practice Statement are planned, these will be indicated and published in the repository.

Only the head of the Certification Authority of the German Federal Chamber of Notaries may make changes to the Certificate Practice Statement or, if he is prevented from doing so, his designated deputy. In accordance with a corresponding operational instruction, changes are only published with the approval of the Head of the Certification Authority of the German Federal Chamber of Notaries or, if he is prevented from doing so, of his designated deputy. 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
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

See section 1.6 of the Certification Policy (*CP*) of the Certification Authority of the German Federal Chamber of Notaries.

2 Responsibility for directories and publications

2.1 Directories

See section 2.1 of the Certification Policy (*CP*) of the Certification Authority of the German Federal Chamber of Notaries.

2.2 Publication of information on certificates

The TSP publishes the following information on qualified certificates issued by it:

- Status information
- CA certificates
- Instruction booklet for qualified electronic signatures and qualified electronic seals
- Certification Policy
- This Certification Practice Statement
- PKI Disclosure Statement for qualified certificates

2.3 Timing and frequency of publications

CA certificates are published after they are issued. The status of the CA certificates issued the TSP can be retrieved for a period of at least 10 years after the end of the validity of the respective certificate.

Further regulations are described in the Certificate Policy (CP) in section 2.3.

2.4 Access to the information

See section 2.4 of the Certification Policy (*CP*) of the Certification Authority of the German Federal Chamber of Notaries.

3 Identification and authentication

3.1 Naming rules

3.1.1 Types of names

Qualified certificates must contain the name of the certificate holder. Qualified certificates conform to the profile of the standard ITU-T Recommendation X 509.V3 and contain a name composed of several pieces of information.

3.1.2 Meaningfulness of names

The names used are unique (see section 3.1.5).

3.1.3 Pseudonyms

At the request of an applicant, the TSP shall list a pseudonym instead of a name in a qualified certificate. The pseudonym must be unmistakably assigned to the certificate holder and identified as such. Pseudonyms are only assigned once within the user group of the TSP.

Qualified certificates containing a pseudonym comply with the profile of the ITU-T Recommendation X 509.V3 and contain a name composed of several pieces of information. This is at least the following information:

- CN = Common name
- serialNumber = Serial number

Note: Pseudonyms are excluded for qualified certificates for legal persons (seal certificates).

3.1.4 Rules for interpreting different forms of names

See section 7.1 of this document.

3.1.5 Uniqueness of names

- For natural persons (QCP-n-qscd):

The name shall be unique to allow identification of the certificate holder without risk of confusion.

Names shall be composed of at least the following elements:

- First name (G)
- Last name (SN)
- Common name
- Serial number (= certificate number)
- Country name (C)

The serial number is unique for each certificate. A mix-up between several certificates for one person or between several certificates for different people with the same first and last name can be ruled out as the 'serial number' ensures the uniqueness of each certificate.

- For legal persons (QCP-n-qscd):

The name of a legal person shall be unique to allow identification of the certificate holder without the risk of a mix-up.

Names shall be composed of at least the following elements:

- Country name (C)
- Common name (CN)
- Organization name (O)
- Organization Identifier organisation headquarters Germany
- Serial number (= certificate number)

The serial number is unique for each certificate.

Applications for qualified certificates for qualified seals must always be submitted by a legally authorised representative of the legal person.

3.1.6 Recognition, authentication and the role of brand names

The applicant is responsible for the compatibility of the chosen pseudonym or the common name with the rights of third parties, e.g. name, trademark, copyright or other protective rights as well as with general laws.

3.1.7 Test certificates

The TSP reserves the right to issue test certificates in exceptional cases, the use of which is necessary for test purposes (e.g. integration, training). The number of test certificates issued must be kept low. The test certificates for natural persons must be clearly marked and recognisable as such, e.g. by the unique expression "TEST" in any organisational designation. For the inclusion of pseudonyms, the specification of the expression "test card" followed by any character string that uniquely identifies the certificate holder in the context of the PKI is required. Test certificates for natural persons also require the application process, including all documentation, to be completed correctly and in full in accordance with the TSP.

Test certificates for legal persons are provided in the TSP repository.

3.2 Identification of certificate holders

- Qualified certificates for natural persons (for qualified signatures)

The TSP shall uniquely identify persons applying for a qualified certificate. Only the information required to provide the trust services offered by the TSP is recorded.

The minimum required are the full name, the date of birth and the ID details of the applicant. In addition, the applicant must provide his home address and an email address.

Identification shall, in principle, be based on the following documents:

- Identity card of the Federal Republic of Germany
- Identity card or electronic residence permit of the Federal Republic of Germany with an electronic ID function
- Passport issued to a person with citizenship of a member state of the European Union or a state of the European Economic Area
- Documents or suitable technical procedures with equivalent security for identification as the documents referred to in the preceding paragraphs

Identification is necessary if the certificate holder has not yet been identified or if the data on which the identification is based on has changed (for example, if the certificate holder's name has changed).

- Qualified certificates for legal persons (for qualified seals)

When applying for qualified seal certificates, the TSP must clearly identify both the organisation as the certificate holder and the natural person representing the organisation and acting as the applicant. Only the relevant information required to provide the trust services offered by the TSP is recorded.

The procedure for identifying the authorised applicant is the same as for identifying a natural person.

For the identification of the organisation, at least the official organisation's name and the organisation's registered office in Germany are required as well as documents verifying the organisation's legal form and the applicant's right of representation.

The identification of the organisation is based on the following documents, depending on the organisational form:

- Official extract from the commercial register (not older than four weeks)
- Certified resolution
- Notarial certification in accordance with Section 21 in conjunction with Section 24 BnotO (so-called representation and registration certification)
- Official certification of the higher-level authority (technical supervisory or legal supervisory authority)

Identification is necessary if the certificate holder has not yet been identified or if the data on which the identification is based has changed (for example, if the certificate holder's name has changed).

3.2.1 Identification procedures for applicants

- Qualified certificates for natural persons (for qualified signatures)

The identification of the applicant for a qualified signature certificate may in principle be carried out using the following procedures:

- Notaridentident - identification by notaries
- Gerichtident - identification by German courts

- Rechtsanwaltskammerident - identification by employees of bar associations
- eIDent - identification by means of electronic proof of identity
- RA-Ident - identification by employees of the RA of the TSP

The decision on the choice of the concrete identification procedures offered is incumbent on the respective applicant. However, not all identification procedures are offered with all TSP products. Identification using the Rechtsanwaltskammerident procedure is only possible, for example, when ordering a beA product and only if the responsible bar association offers this procedure. The identification procedure Gerichtident is only offered to members of the judiciary. Identification using the RA-Ident procedure is only possible for employees of the German Federal Chamber of Notaries public body.

The applicant must select one of the identification procedures offered to him when applying. Depending on the selection made, the applicant will be informed on how to use the selected procedure after completing the online application. At the same time, depending on the selected identification procedure, the applicant will be provided with the appropriate identification documents for printing.

- Qualified certificates for legal persons (for qualified seals)

The identification of the authorised applicant may in principle be carried out using the following procedures:

- Notarident - identification by notaries
- Gerichtident - identification by German courts
- RA-Ident - identification by employees of the RA of the TSP

The decision on the choice of the concrete identification procedures offered is incumbent on the respective applicant. However, not all identification procedures are offered with all TSP products. Identification using the RA-Ident procedure is only possible for the identification of subsidiaries and institutions of the German Federal Chamber of Notaries, the Gerichtident procedure is only offered for organisations in the field of justice.

The applicant must select one of the identification procedures offered to him when applying. Depending on the selection made, the applicant will be informed on how to use the selected procedure after completing the online application.

At the same time, depending on the selected identification procedure, the applicant will be provided with the appropriate identification documents for printing.

When applying for a qualified seal certificate, proof of the applicant's right of representation must also be provided. This proof shall, in principle, be based on the following documents:

- Official extract from the commercial register (not older than four weeks)
- Certified resolution
- Notarial certification in accordance with Section 21 in conjunction with Section 24 BnotO (so-called representation and registration certification)
- Official certification of the higher-level authority (technical supervisory or legal supervisory authority)

3.2.1.1 Notaridentverfahren

In the Notarident identification procedure, identification is carried out by a notary with an official seat in Germany by means of the notarisation of the applicant's signature. The requirements of the German Notarisation Act [Beurkundungsgesetz - BeurkG], in particular from Section 40 of BeurkG, must be observed.

- Qualified certificates for natural persons (for advanced electronic signature)

For qualified signature certificates, the Notarident procedure includes:

- Receipt of the application documents (signed or still to be signed) and certification of the applicant's signature the data sheet on the application form in accordance with of Section 40 of BeurkG by the notary
- Preparation of a certified copy of the identification documents used for identification and, if applicable, of the proof of the doctor's degree by the notary
- Dispatch of the deed or an electronically certified copy of the deed to the TSP by post or electronically - by post, documents are to be sent directly to the TSP in an envelope
  As an alternative to sending the documents by post, the notary can create electronic certified copies of all documents in accordance with Section 39a of the BeurkG. The files with the notary's qualified electronic signature are then sent securely by electronic means to the certification authority's EGVP mailbox.
  The transfer is encrypted end-to-end.

In the Notarident procedure, neither an examination of the application documents nor a briefing of the applicant by the notary takes place.

- Qualified certificates for legal persons (for qualified seals)

When identifying the certificate holder and the authorised applicant, the requirements of the German Notarisation Act [Beurkundungsgesetz - BeurkG], in particular from Section 40 BeurkG, must be observed.

For qualified seal certificates, the Notarident procedure includes:

- Receipt of the application documents (signed or still to be signed) and certification of the applicant's signature the data sheet on the application form in accordance with Section 40 of BeurkG by the notary
- Preparation of a certified copy of the identification documents used for identification and, if applicable, of the proof of the doctor's degree by the notary
- For partnerships:
  A certificate of representation and registration is prepared in accordance with Section 21 of Federal Code for Notaries (Bundesnotarordnung; BNotO) by the notary. A so-called simple certificate in note form is sufficient for the certification.
  The certificate must state the entry of the legal person in the commercial register and the applicant's right of representation. In addition, the register and the date of inspection of the register or of a certified register extract must be indicated.
- For public authorities and organisations under public law:
  Receipt of a completed official certificate from the superior authority as proof of the existence of the organisation and of the applicant's right of representation.
- Dispatch of the deed or an electronically certified copy of the deed to the TSP by post or electronically.
  By post, documents are to be sent directly to the TSP in an envelope. As an alternative to sending the documents by post, the notary can create electronic certified copies of all documents in accordance with Section 39a of the BeurkG. The files with the notary's qualified electronic signature are then sent securely by electronic means to the certification authority's EGVP mailbox.
  The transfer is encrypted end-to-end.

In the Notarident procedure, neither an examination of the application documents nor a briefing of the applicant or the certificate holder by the notary takes place.

3.2.1.2 Gerichtident procedure

- Qualified certificates for natural persons (for qualified signatures)

For applicants from the judiciary, the identification can also be done by the president or director of a German court. The requirements for the certification of signatures by public authorities (Section 34 of the German Administrative Procedure Act [Verwaltungsverfahrensgesetz - VwVfG] or corresponding state laws) must be observed.

In the case of identification by a court, the same standards apply for the control obligations and the formulation of the certification as for identification by the notary within the framework of the Notaridentprocedure (see section 3.2.1.1). The applicant must present one of the documents mentioned in section 3.2 at the time of identification.

For qualified signature certificates, the Gerichtident procedure includes:

- Receipt of the application documents (signed or still to be signed) and certification of the applicant's signature on the application form in accordance with Section 34 VwVfG BeurkG
- Attachment of a certified copy of the identification documents used for identification and, if applicable, of the proof of the doctor's degree
- Postal delivery of application documents in an envelope directly to the TSP The confirmation of professional details obtained by the applicant is, if necessary, attached, unless it is sent directly by the confirming body

- Qualified certificates for legal persons (for qualified seals)

For members of the judiciary, the identification of the certificate holder and the authorised applicant can also be carried out by the president or director of a German court. In this regard, the requirements for the certification of signatures by public authorities (Section 34 German Administrative Procedure Act [Verwaltungsverfahrensgesetz - VwVfG] or corresponding provisions under Land law) must be complied with.

In the case of identification by a court, the same standards apply for the control obligations and the formulation of the certification as for identification by the notary within the framework of the Notaridentprocedure (see section 3.2.1.1).

The authorised applicant must present the documents listed in section 3.2 as proof of his personal identity, as proof of the legal person's identity as the certificate holder, and as proof of his right of representation for the certificate holder.

For qualified seal certificates, the Gerichtident procedure includes:

- Receipt of the application documents (signed or still to be signed) and certification of the applicant's signature on the application form in accordance with Section 34VwVfG BeurkG
- Attachment of a certified copy of the identification documents used for identification and, if applicable, of the proof of the doctor's degree
- Receipt and attachment of a completed official certificate from the superior authority as proof of the existence of the organisation and of the applicant's right of representation
- Postal delivery of application documents in an envelope directly to the TSP The confirmation of professional details obtained by the applicant is, if necessary, attached, unless it is sent directly by the confirming body

3.2.1.3 Rechtsanwaltskammerident procedure

If necessary, the identification of the applicant can also take place on the basis of the identification by an employee of the German Bar Association - e.g. in the case of swearing-in in accordance with Section 12a of the German Federal Lawyers' Act [Bundesrechtsanwaltsordnung - BRAO].

The Rechtsanwaltskammerident procedure includes:

- Receipt of the signed application documents and verification of correctness of form and content by an employee of the bar association
- Photocopying of identity documents or comparison of photocopies handed over by the applicant with the (original) identity document
- Identification of the applicant and verification of the identification data on the basis of the identity documents
- Scanning of all documents (application documents and identity documents) by an employee of the bar association with the application of at least an advanced electronic signature; the employee shall confirm with the signature that the scans correspond to the paper original in terms of image and content
- Transfer of the electronic files provided with the at least advanced electronic signature via a web application by the bar to the RA; the transfer shall be transport-encrypted

The managing directors of the bar associations are trained by the TSP and ensure that only unobjectionable personnel, who are also used for identification within the framework of the swearing-in, participate in the Rechtsanwaltskammerident procedure.

3.2.1.4 eIDent procedure

In the case of identification by means of electronic proof of identity, the identification takes place while entering the application data online and its transmission to the RA system. Electronic proof of identity is provided by transmitting data from the electronic storage and processing medium of the ID card/ eID-Token via the secure eID infrastructure. Proof of the identification process is documented with the application data.

The certification authority accepts all electronic proofs of identity that have the security level "high" and have been recognized by the European Commission.

3.2.1.5 RA-Ident procedure

- Qualified certificates for natural persons (for qualified signatures)

Applicants who are employees of the Federal Chamber of Notaries can be identified by an RA employee. The application details are entered online and/or the identification is usually carried out directly with the applicant or at the premises of the TSP.

For qualified signature certificates, the RA-Ident procedure includes:

- Receipt of the application documents by the RA employee and verification of correctness of form and content
- Photocopying of identity documents or comparison of photocopies handed over by the applicant with the (original) identity document by the RA employee
- Identification of the applicant and verification of the identification data on the basis of the identity documents by the RA employee
- Signature of the applicant on the last page of the application document
- Verification and comparison of the signature executed in the presence of the RA employee with the signature visible in the identification document
- Signature of the RA employee on the identification form
- Creation and signing of a summary of the identification data by the RA employee

- Transfer of the identification form together with the application data and the identification document by the RA employee into the RA system by applying at least an advanced electronic signature

In order to prevent forged applications from being submitted outside the secure RA environment during the RA-Ident procedure, the RA employee signs each page of the application documents or affixes his/her abbreviation. Afterwards, the application data and identification documents as well as an identification form are scanned by the RA employee with at least an advanced signature and transferred to the RA system. In principle, it can be done from any computer workstation with an internet connection to which a chip card reader and a printer/scanner are connected.

- Qualified certificates for legal persons (for qualified seals)

Authorised applicants of subsidiaries and institutions of the German Federal Chamber of Notaries can be identified by a RA employee. The application details are entered online and/or the identification is usually carried out directly with the applicant or at the premises of the TSP.

- Receipt of the application documents by the RA employee and verification of correctness of form and content
- Photocopying of identity documents or comparison of photocopies handed over by the applicant with the (original) identity document by the RA employee
- Identification of the applicant and verification of the identification data on the basis of the identity documents by the RA employee
- Signature of the applicant on the last page of the application document
- Verification and comparison of the signature executed in the presence of the RA employee with the signature visible in the identification document
- Signature of the RA employee on the identification form
- Receipt and verification of an official extract from the commercial register (not older than four weeks) or a certified resolution on the statutes as proof of the organisation's existence and the applicant's right of representation
- Creation and signing of a summary of the identification data by the RA employee

- Transfer of the identification form together with the application data and the identification document by the RA employee into the RA system by applying at least an advanced electronic signature

In order to prevent forged applications from being submitted outside the secure RA environment during the RA-Ident procedure, the RA employee signs each page of the application documents or affixes his/her abbreviation. Afterwards, the application data and identification documents as well as an identification form are scanned by the RA employee with at least an advanced signature and transferred to the RA system.

3.2.2 Identification in case of extensions and limitations in the certificate

At the request of an applicant, a qualified signature certificate for a natural or legal person may contain information on his power of representation for a third person as well as office- and profession-related or other information on his person (attributes). With regard to the information on the power of representation, the consent of the third person shall be proven; office- and profession-related or other information on the person shall be confirmed by the respective competent body. Qualified certificates containing corresponding attributes shall only be issued if the confirmation of the competent body is available. For this purpose, the applicant shall be provided with a corresponding print-out form following his or her certificate application with the request to forward this form to the competent body.

3.2.2.1 Listing of office- and profession-related or other information

If an applicant has applied for the inclusion of an office- and profession-related or other indication as an attribute, the competent body shall confirm that the applicant is authorised to use the office- and profession-related or other indication and shall send the confirmation by post to the RA of the TSP. The confirming body proves its authorisation by means of appropriate documents (e.g. extract from the commercial register).

The confirmation forms are checked together with the other application documents by the RA employees as part of the application check. In addition, the confirmations are documented.

A special feature applies to obtaining confirmation for the inclusion of notarial attributes. In order to avoid obtaining confirmations for requested notarial attributes in each individual case, the TSP, on the basis of written agreements with the regional chambers of notaries, uses the notarial directory maintained by the German Federal Chamber of Notaries as a trustworthy notarial database when checking requested notarial attributes. In this case, the examination of the admissibility of a requested notarial attribute is carried out in such a way that the application system generally only accepts card applications with a notarial attribute if the

corresponding authorisation to use such a notarial attribute already results from the notarial directory when the application is submitted.

Note: Official-, job-related or other information is not permitted for qualified certificates for legal persons (seal certificates).

3.2.2.2 Listing of an power of representation for a third person

If an applicant has applied for the inclusion of power of representation for a third party, the consent of the third party must be proved to the TSP. In the case of a legal person (under public or private law), the representative of the legal person confirms that the applicant has the power of representation applied for and sends the confirmation by post to the TSP. The representative of the legal person proves his authorisation by means of appropriate documents (e.g. an extract from the commercial register).

This applies accordingly when applying for the inclusion of the power of representation for a natural person.

Note: Applying for a power of representation for a third party for qualified certificates for legal persons (seal certificates) is not possible.

3.2.2.3 Inclusion of a pseudonym

If the applicant applies for a pseudonym and a power of representation is to be included in the qualified certificate, the confirmation must include the consent of the represented person to the inclusion of a pseudonym. The represented person shall be notified of the pseudonym.

If the applicant requests a pseudonym and the inclusion of professional or other information about him in the qualified certificate, consent to the pseudonym must also be obtained from the bodies responsible for such information

Note: The inclusion of a pseudonym is not planned for certificates for legal persons.

3.2.2.4 Restriction of use

The use of the qualified certificate may be restricted generally or financially. The corresponding restriction shall also be made known to the confirming body as part of the confirmation of an attribute.

Note: The inclusion of general or financial restrictions is not planned for certificates for legal persons.

3.3 Identification and authentication for key renewal (re-keying) requests

A key renewal is carried out by producing a new qualified certificate before the old certificate expires. The data and evidence already checked during the initial identification can be referred to. This requires that the identification data and confirmations on attributes available to the TSP are complete and accurate. Before the certificate expires, the certificate holder (for signature certificate for natural persons) or applicant (for seal certificates for legal persons) is automatically informed about the procedure for issuing a follow-up certificate. Here, the identity is ensured via the login, e.g. with an authentication certificate. At the same time, the certificate holder or applicant receives an overview of the relevant data recorded at the TSP and is requested to check the data and notify the TSP of any necessary corrections within a specified period of time (at least four weeks). If the data and evidence available to the TSP are still complete and accurate, a new qualified certificate will be issued. If the identification data have changed in the meantime, a new application and identification is required.

The new qualified certificate is issued on the basis of the existing contractual relationship with the certificate holder. A change in the General Terms and Conditions requires that these have been effectively included in the contract.

A deviating procedure may be agreed in individual cases if this is consistent with the legal and other requirements.

3.4 Identification and authentication when submitting a revocation request

For certificate holders and their authorised representatives, the TSP offers the following options for revoking certificates issued by it:

- By phone
- In written form with a hand-written signature or a qualified electronic signature

The identification and authentication is carried out:

- By phone for a revocation request of qualified signature certificates by providing the revocation password and other personal information
- By phone for a revocation request of qualified seal certificates by providing the revocation password, further personal details and an

authorisation link sent to the known business contact address (email or EGVP)

- In written form for a revocation request of qualified signature certificates by verifying the signature
- In written form for a revocation request of qualified seal certificates by verifying the signature as well as the legally valid power of representation of the person authorised to revoke

4 Operating requirements

4.1 Certificate application

The TSP issues signature certificates exclusively to members of the professional groups named in Section 1.3.3 of the Certificate Policy (***CP***) of the Certification Authority of the German Federal Chamber of Notaries and within the scope of operating the video communication system in accordance with Section 78p BNotO. The TSP also issues seal certificates exclusively to legal persons in the group named in section 1.3.3 of the certification policy (CP) of the Certification Authority of the Federal Chamber of Notaries.

The application data is always entered via the online application page of the TSP. It is not possible to apply in written form only. Applicants themselves have to enter the application data. It is transmitted either via a web form or via a secure API interface after being called up by an authorized application. In the course of submitting the application, the applicant agrees to the General Terms and Conditions of the TSP and confirms that he/she has taken note of the training brochure on qualified certificates. Acceptance of the General Terms and Conditions and confirmation that the applicant has taken note of the brochure is a prerequisite for submitting an application and the conclusion of the contract. The General Terms and Conditions are written in German and will be made available to applicants for download in electronic form together with the training brochure.

For qualified seal certificates, if other authorised signatories are to be added alongside the applicant, these must be noted on the TSP online application page before the official application is submitted.

See section 3.2 on the transmission of documents used for identification to the TSP.

The TSP reserves the right to reject applications for the issue of a certificate.

4.2 Processing of the certificate application

4.2.1 Execution of identification and authentication

After the online application has been submitted, it is verified by RA employees using the four-eyes principle, depending on the identification procedure selected. The verification is only carried out when the identification documents and any required attribute confirmations have been submitted.

The TSP uses various procedures to identify applicants. In some cases (e.g. in the case of the Notarident or Gerichtident procedure), reliable and competent third parties are entrusted with the identification. See explanations in section 3.2.

Under certain conditions, applications for qualified certificates can be verified automatically by the RA system. This applies, among other things, to certificate applications submitted using the identification procedure eIDent. In this case, an automatic system verification of the application data and the electronic proof of identity is carried out.

The identification and authentication of the applicants as well as the verification of further certificate-relevant data (e.g. information on occupation-related attributes) must be completed before the qualified certificate is issued.

After all application data has been cross-verified and confirmed, the second verifying RA employee issues the production release.

4.2.2 Acceptance or rejection of the application

The TSP will reject an application for a certificate if the application documents are incomplete or incorrect, or if identification documents are incomplete, damaged or incorrect. Applications are also rejected if the application data does not match ID documents, attribute confirmations or other necessary evidence (e.g. organisational and representation evidence).

Applications may also be rejected for the following reasons:

- Ineligibility of the applicant because he/she is not a member of one of the professional groups listed in section 1.3.3 of the Certificate Policy of the Certification Authority of the German Federal Chamber of Notaries
- Missing proof of organisation of the legal person
- Missing power of representation of the applicant
- No authorization or permission to transfer application data via API
- Expiration of deadlines (usually three months) for the provision of data and/or documents

The TSP reserves the right to reject applications for other reasons as well.

4.3 Issue of certificates

4.3.1 CA procedure for issuing certificates

The creation of the certificate, the generation of the key and the personalisation of the chip card take place on the premises of the TSP. The actual certificate creation is carried out by the BNotK signing component located in the secure computer centre of the TSP.

After identifying the applicant and cross-verifying the application data with the data available in electronic form, the production process is triggered. This includes the initiation of the key generation, the generation of the certificate as well as the storage of the certificate on the remote QSCD.

The complete documentation for an application and the certificate it contains is stored in an audit-proof manner in accordance with section 5.5. The application documents can be assigned to the created certificate at any time using the unique application number.

4.3.2 Notification of the certificate holder about the creation of the certificate

The certificate holder is notified of the creation of his certificate by email or EGVP.

4.4 Certificate handover

4.4.1 Behaviour during certificate handover

The subscriber is obliged to verify the contents of the certificate for correctness before using it. When certificates are issued, a distinction is made between authentication certificates and qualified certificates.

- Authentication certificates
    - Chip cards

      In principle, the certificate is delivered by post to the applicant's registration or their business address. The functionality of the chip card is checked before dispatch. The applicant must confirm receipt of the chip card online. After the applicant has confirmed receipt of the chip card and the PIN letter has been generated, the card is activated. The PIN letter with the PIN and PUK is then sent to the applicant. They are delivered by post or electronically via EGVP. The applicant can activate the chip card using this PIN, which it is recommended to be changed before first use. The PIN can only be changed successfully if the chip card has not been tampered with. The individual steps are documented.

    - Software authentication certificates

The user generates the authentication certificates himself after registering on a secure, password-protected portal. The (authorised) applicant is the only person who knows the password required for this. After registering on the portal, the software certificate is created locally by the user and downloaded in encrypted form with a specially assigned PIN.

- Qualified certificates for natural and legal persons
    - Remote signature certificate (qualified certificates for natural persons)

    The certificate holder's private key is generated in the secure data centre environment of the TSP and stored there for signature generation. The certificate can only be used after prior registration with authentication data uniquely assigned to the certificate holder (2-factor authentication), using a chip card and PIN.

    - Remote seal certificate (qualified certificates for legal persons)

    The use of seal certificates for legal persons is done exclusively by means of a remote sealing procedure.

    The certificate holder's private key is generated in the secure data centre environment of the TSP and stored there for seal creation. The key for creating the seal can only be used after prior registration with the seal creator's authentication data (2-factor authentication) using a software certificate and PIN, which are uniquely assigned to the authorised applicant or end-users with signing authority.

4.4.2 Publication of the certificate by the TSP

The TSP does not publish certificates in the public directory service. The retrieval is possible at any time via the OSCP extension RetrieveIfAllowed.

The status of a certificate can be checked via OCSP after production.

4.4.3 Notification of third parties about the creation of the certificate

Third parties who have confirmed details in the qualified certificate concerning the power of representation or office- and profession-related or other details shall be informed in written form about the contents of the qualified certificate and shall be informed about the possibility of revoking the qualified certificate (***Third Parties Authorised to Revoke***). A revocation password shall be set for this purpose. There shall be no separate notification of the creation of the qualified certificate.

4.5 Use of the key pair and the certificate

4.5.1 Use of the private key and the certificate by the certificate holder

or the authorised signatory

- Qualified certificates for natural persons (for qualified signatures)

Certificate holders may only use the certificates for professional purposes. The provisions from section 1.4 apply.

For qualified electronic signatures, the TSP issues chip cards that the certificate holder can use to authenticate himself to the TSP in order to release the application of the signature via remote signature. Remote signatures can only be released after logging in with a chip card and PIN. The authentication certificate on the chip card is clearly linked to the key of the signature certificate. The authentication mechanism based on the authentication certificate can be considered as signature creation data in the sense of the eIDAS Regulation (EU 910/2014).

- Qualified certificates for legal persons (for qualified seals)

The use of the certificate is permitted to the authorised representative and end-users with signing authority for exclusively professional purposes.

For sealing processes, the TSP issues software authentication certificates that the authorised applicant and other end-users with signing authority use to authenticate themselves to the TSP in order to release the attachment of the seal via remote sealing. Remote seals can only be released after initial login using a software authentication certificate. The persons authorised to release a seal are thus the authorised applicant as well as all other end-users (such as employees) who, by possessing a software authentication certificate, are authorised to authenticate themselves to the TSP. The authentication certificates are uniquely linked to the seal certificate key. A seal is released when the applicant or an authorised end-user authenticates themselves to the TSP by means of an authentication certificate. The authentication then allows the release of a remote seal by the applicant or end-user. The authentication mechanism based on authentication certificates can be considered as seal creation data in the sense of the eIDAS Regulation (EU 910/2014).

In addition, the TSP enables the authorised applicant to automate sealing processes using the software authentication certificate in the data centre.

The responsibility for protecting the software authentication certificates lies solely with the authorised applicant for the seal certificate. Authentication certificates are to be used exclusively to release seals for professional purposes and are to be protected from access by unauthorised third parties.

4.5.2 Use of the public key and the certificate by certificate holders

The certificates may be used by all certificate holders. However, certificate holders and relying third parties may only rely on the public key and the certificate if the following conditions 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, to check the trust status, the EU Trusted List according to the eIDAS Regulation (EU) No. 910/2014, for example, can be used
- The validity of the certificate has been confirmed via the status request service (OCSP)
- All further agreements and other precautionary measures have been observed

4.6 Certificate renewal

Certificate renewal is not offered.

4.7 Certificate renewal with key renewal

The renewal of a certificate with a new key pair based on the certificate data of the original certificate is possible after prior authentication of the certificate holder or the authorised applicant according to section 3.3 The certificate holder or the authorised applicant must confirm that the data provided during identification (see section 3.2.1) is still valid. The current versions of the CP and CPS at the time of renewal apply to the new certificates.

4.8 Certificate change

A subsequent amendment of the certificate by the TSP is not possible.

4.9 Revocation and suspension of certificates

4.9.1 Conditions for revocation

The TSP revokes qualified certificates for natural and legal persons in the following cases:

- At the request of the certificate holder, a third party authorised to revoke or the BNetzA
- If the qualified certificate was issued on the basis of incorrect information regarding Annexes I, III and IV of the eIDAS Regulation (EU 910/2014)

- In the event of termination of the activity as trust service provider and is not continued by another qualified trust service provider
- If the TSP is informed that the private key has been communicated to an unauthorised person or organisation that does not belong to the certificate holder
- If facts justify the assumption that (i) the certificate is forged or not sufficiently forgery-proof or (ii) the qualified electronic signature creation devices used have security flaws

The TSP also revokes the issued certificate if

- the contractual relationship has been terminated,
- the certificate holder's or the authorised applicant's application was made on the basis of a framework agreement and this framework agreement has been terminated or has been terminated for other reasons,
- the algorithms underlying the procedures used have been broken or if there are reasons to assume that the algorithms underlying the procedures used have been broken,
- a confirmation that the qualified electronic signature or seal creation device used does not meet the legal requirements is not available or is no longer valid,
- a legal obligation to revoke exists,
- the reference authorisation does not exist or has subsequently ceased to exist - this does not entail any obligation to revoke.

The TSP is also authorised to revoke a certificate if it is aware that the underlying root certificate or the certificate itself has been compromised or revoked by the competent authority.

Certificate holders and authorised applicants are also obliged to have issued certificates revoked if

- the chip card or the certificate has been lost, misused or possibly compromised,
- the certificate issued by the TSP, which enables authentication with the TSP, has been lost, misused or possibly compromised,

- there are any changes to the certificate data or if a further use would constitute a violation of professional and/or ethical rules or other legal provisions.

If the TSP learns through a third party that the chip card or certificate of a certificate holder has been lost, misused or possibly compromised, it shall contact the certificate holder or authorised applicant. The certificate is not automatically revoked.

4.9.2 Persons authorised to revoke

The following persons are authorised to revoke the qualified certificate:

- TSP
- Certificate holder
- Authorised applicant
- Third parties authorised to revoke
- BNetzA

4.9.3 Procedure for submitting a revocation request

- Qualified certificates for natural persons (electronic signature)

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

(1) By phone at: (0800) 3550 400 or (0800) 3550 100

Certificate holders who wish to submit a revocation request by telephone must authenticate themselves by naming the agreed revocation password and providing further personal details. If a certificate holder requests a revocation by telephone without knowing the revocation password, he must confirm the request for revocation via an electronically sent one-time link.

(2) In written form

- with a handwritten signature to the following address: Zertifizierungsstelle der BNotK, Burgmauer 53, 50667 Köln.
- with a handwritten signature or a qualified signature via email or EGVP to the TSP.

A written revocation request must either be signed by the person authorised to revoke it or have a qualified electronic signature. The qualified certificate to be revoked must be clearly identifiable by the information on the certificate and the certificate holder.

The revocation of the qualified certificate is documented by means of an automatically generated revocation log. Furthermore, the certificate holder and the confirming body are informed about the revocation in case of additionally requested attributes.

- Qualified certificates for legal persons (for qualified seals)

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

1. By phone at: (0800) 3550 400 or (0800) 3550 100

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

- authenticate themselves by providing the agreed revocation password and other personal information.

  After the correct revocation password and personal data have been provided, a one-time link to confirm the revocation request will also be sent to the business contact address (email or EGVP mailbox) stored with the TSP

2. In written form

(1)

- with a handwritten signature to the following address: Zertifizierungsstelle der BNotK, Burgmauer 53, 50667 Köln.

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

A written revocation request must either be signed by the person authorised to revoke it or have a qualified electronic signature. The qualified certificate to be revoked must be clearly identifiable

by the information on the certificate 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 representation.

The revocation of a certificate cannot be reversed.

4.9.4 Deadlines for a revocation request

Certificate holders shall have certificates revoked without delay if there are grounds for revocation. If the certificate holder is a legal person (in the case of qualified seal certificates), the revocation must be submitted by the authorised representative.

4.9.5 Time period for processing the revocation request

Certificates may be revoked by telephone 24 hours a day, seven days a week via a telephone number set up specifically for this purpose. The certificate will be revoked immediately, but no later than within 24 hours.

Written revocation requests are processed quickly in the RA and certificates are revoked within 24 hours.

If the certificate holder, the authorised applicant or third parties authorised to revoke request so, the revocation will take place on a specific date. Retroactive revocations are not possible.

4.9.6 Methods for checking revocation information

Revocation information can be requested via the OCSP responder. The address of the service is part of the certificate.

4.9.7 Frequency of publication of revocation lists

No revocation lists are provided for certificates.

4.9.8 Maximum latency for revocation lists

No revocation lists are provided for certificates.

4.9.9 Online availability of revocation information

Revocation information can be requested via the OCSP responder. The address of the service is part of the certificate. Revocation information is available immediately, at the latest within 60 minutes after revocation of a certificate. The system time of all IT systems involved in the revocation is continuously synchronised with the legally valid time pursuant to the German Units

and Time Act [Einheiten- und Zeitgesetz].

4.9.10 Necessity for online verification of revocation information

There is no requirement to verify revocation information online.

4.9.11 Other forms of displaying revocation information

None.

4.9.12 Special requirements in the event of the private key being compromised

None.

4.9.13 Suspension of the certificate

Suspension of the certificate is not possible.

4.10 Status request service

Status requests are made via the OCSP responder. The address of the service is part of the certificate and available 24 hours a day, seven days a week. The status query service is highly available to prevent failure. The TSP will eliminate failures of the status query service within the existing technical and operational possibilities within 12 hours at the latest.

The integrity and authenticity of the status information shall be protected.

4.11 Termination of the certification service

The contracts may be terminated by the TSP and the certificate holder in accordance with the contractual agreements concluded between them.

4.12 Deposit and recovery of keys

Deposit of keys is not possible.

5 Non-technical security measures

5.1 Structural security measures

All sensitive data and systems relevant to the operation of the TSP are housed in physically protected security areas. The protection class meets the requirements for the operation for issuing qualified certificates. Access control mechanisms ensure that no unauthorised persons have access to the secure areas. All accesses, including unauthorised access attempts, are logged. Attempts to defeat the security mechanisms, such as break-ins, theft and vandalism, trigger an alarm. Within the security area, there is additional physical protection of the VDA-BNotK's IT systems and keys. Access to the systems is only possible under the dual control principle. This measure and the additional video surveillance provide additional protection against manipulation and theft. The components of the TSP are separate from other services of the BNotK. The security measures and the underlying security concept are regularly checked by a recognised testing and confirmation body.

The computer centre has also been tested and certified according to "Trusted Site Infrastructure Level 3 Extended" by TÜV Informationstechnik GmbH. The audit covers the following assessment aspects:

- Environment
- Building construction
- Fire protection, alarm and extinguishing technology
- Energy supply
- Ventilation and air-conditioning systems
- Organisation
- Documentation

Level 3 Extended certification corresponds to a high protection requirement, i.e. all critical supply systems (in particular the external network connection) are fully redundant. "Extended" means that all requirements of an assessment aspect of the next higher level have been achieved. The assessment is repeated at regular intervals.

5.2 Procedural requirements

5.2.1 Role concept

The role concept implemented and documented in the security concept provides for a division into operational, advisory, administrative and leading roles. The defined roles include the role of IT security officer, who is also responsible for internal auditing, the role as syslog operator, as DB administrator, as CA administrator and as network administrator, as well as the role of RA employee and lockdown officer. The tasks and the necessary qualifications and experience for the corresponding roles are defined in existing job descriptions. Persons appointed to leading roles and those working in the field of certification and revocation services must be free from commercial, financial or other influences likely to significantly affect confidence in the TSP. All employees are given the roles necessary to perform the job through a defined process. A role exclusion principle guarantees that no single person can make security-relevant changes or issue, delete or revoke certificates without authorisation. The revocation of a role also follows a defined process and is documented.

5.2.2 Four-eyes principle

Security-critical processes must always be carried out in accordance with the four-eyes principle. This is implemented through technical and organisational measures. In addition to the verification of certificate requests in the RA, all actions from key activation to key backup are carried out in accordance with the four-eyes principle.

Changes to the security mechanisms and IT systems are made according to a defined process, are documented and can only be carried out using the four-eyes principle. The four-eyes principle is technically enforced and cannot be circumvented. This also applies to the recovery of data.

5.2.3 Other instructions

The TSP employees are not permitted to remove documents, media (with the exception of laptops) and software containing sensitive data from the security area of the TSP.

5.3 Personnel concept

5.3.1 Qualification, experience and reliability of staff

The TSP only employs reliable, qualified personnel. Before taking up work in the security-critical area of the TSP, their specialist knowledge is checked and training is provided. This also applies to all managerial roles at the TSP. Training measures are documented. The TSP ensures that there are no conflicts of interest. Employees of the TSP must refuse to act in the event of a conflict of interest. In this case, they do not face any consequences under labour law.

5.3.2 Security check

All TSP employees deployed for certification services must submit a police clearance certificate at regular intervals, at least every two years. For managerial roles, a certificate of good conduct is also filed with the supervisory authority.

5.3.3 Training and additional learning opportunities

All employees are trained before starting work and as required. Follow-up training for employees is usually held annually. In addition, follow-up training is carried out when changes are made to the processes, the technology and the framework conditions for the operation of the trust service, or if these are necessary to impart or maintain the necessary expertise of an employee.

5.3.4 Appointment, withdrawal and change of roles

Role appointments, role withdrawals and role changes are carried out in accordance with established internal procedures and are documented and the corresponding minutes signed by the appointee and appointee.

The head of the TSP is appointed and dismissed by the president of the German Federal Chamber of Notaries. Other persons who assume managerial or supervisory roles at the TSP, e.g. the deputy head of the TSP as well as the security officer of the TSP, are appointed and dismissed by the head of the TSP. An appointment is only made once the required security review and training have been completed. The implemented role concept and role exclusion criteria ensure that each person working for the TSP only receives the access and access rights necessary to perform his role. The appointment is documented, the appointee declares his/her agreement with the role by countersigning the corresponding protocol.

Part of the appointment and dismissal is also the creation or withdrawal of access and access authorisations to technical systems and protected areas. Access and entry authorisations are only granted to the extent required for the corresponding role.

5.3.5 Requirements for external personnel

External personnel working temporarily in the security area will always be accompanied and supervised by authorised staff. The same regulations apply to permanently deployed personnel from other companies as to internal personnel.

5.3.6 Sanctions for unauthorised actions

The TSP has implemented measures (e.g. the implementation of an internal audit procedure) to control compliance with the established rules and procedures for the proper and secure operation of the certification service. Any violations found are remedied. Unauthorised actions may also have consequences under labour law and criminal law.

5.3.7 Documentation

The following documentation will be made available to staff:

- Security concept (the parts relevant to the performance of the role)
- Role concept
- Certificate Policy and the Certification Practice Statement
- Process documentation for the activity in the RA
- Company's security policy

5.4 Logging of monitoring measures

5.4.1 Monitoring of access

All access to and exit from the security areas of the TSP is logged and stored for an appropriate period of time (see section 5.1). Access by visitors is also logged and must be announced at least 24 hours in advance when visiting the computer centre. Visitors are always accompanied by authorised staff. Video recordings are also stored in the area of the data centre.

5.4.2 Monitoring of organisational measures

The organisational measures are regularly reviewed by the senior roles of the Certification Authority. Changes to organisational measures are appropriately documented in the security concept.

5.5 Archiving of documents

5.5.1 Types of documents

All documents required by law for the complete documentation of the life cycle of the CA and the issued qualified certificates and keys are archived in the form of electronic log data or paper-based. This applies to the life cycle of qualified certificates in particular to the documents arising during registration (see section 3.2) as well as the documents on issuance, acceptance, publication and revocation.

The life cycle of the CA and its systems and keys is fully documented. This concerns, among other things, work on the remote QSCD as well as the issuance, destruction and backup of the keys.

In addition, security concepts, role assignment lists, training documents and procedural instructions as well as other documents relevant to the operation (e.g. the certifications, contracts with service providers, documents on the delivery and storage of the blanks as well as their removal for production, the results of the internal audit, the results of the vulnerability and penetration tests) are archived.

5.5.2 Retention periods

The retention period of the documentation complies with the legal requirements for qualified certificates. The qualified certificates issued by the TSP are also kept beyond the period of their validity together 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 the TSP's operation.

5.5.3 Archive security

The electronic archive is state of the art and guarantees long-term archiving in accordance with TR-ESOR that preserves the value of the evidence. The paper-based documentation is stored in a specially protected area of the TSP. Only authorised employees have access to the documents. The integrity of the electronic archive is guaranteed by affixing signatures. There is also a back-up to prevent data loss. For long-term archiving, the Evidence Record Syntax is also implemented. Qualified time-stamps are used to secure the hash trees created. Only authorised employees of the TSP have access to the data. Requests to view the documentation are processed by the RA. For this purpose, the certificate holder must contact the TSP. The RA employee will provide the certificate holder with copies of his or her documentation for inspection.

5.5.4 Data backup of the archive

Data is backed up using state-of-the-art technology.

5.5.5 Requirements for the time-stamps of the archived records

The system time of the systems responsible for archiving is continuously checked against the legally valid time according to the German Units and Time Act.

5.5.6 Archiving location

Archiving takes place exclusively at the German Federal Chamber of Notaries.

5.6 Key changeover

If required and within a reasonable time before the validity of the existing certificates expires, new keys are generated and the matching certificates are published. This applies to both end-user as well as CA and service certificates.

5.7 Emergency concept

5.7.1 Incident handling

The handling of security-relevant incidents and compromises is documented in the security concept. Responsible for the implementation are the leading roles.

5.7.2 Recovery of IT systems

The IT systems of the TSP are backed up daily and stored remotely at an external location. Restoring the systems is part of the practised and documented IT processes and is carried out by the persons with the corresponding roles according to the role concept.

5.7.3 Recovery after compromise of private CA keys

If private CA keys are compromised, the affected CA and service certificates are revoked and the supervisory authority is informed. Depending on the type of compromise and on the basis of the TSP emergency plan, the end-user certificates generated from the CA may also be revoked in consultation with the supervisory authority. Affected certificate holders and authorised applicants are informed about the incident and its consequences. The revocation information can generally be requested via the OCSP responder or, in the event of a compromise of the OCSP responder's certificate, via the Trusted List issued by the BNetzA.

After implementing appropriate measures to prevent future compromises, new CA keys are created according to the corresponding specifications, published and then the issuing of new end-user certificates is started according to a documented process. The same applies to service certificates. The same process takes place when the algorithms used become invalid or when a QSCD confirmation expires or is revoked and also affects the end-user certificates or their keys.

5.7.4 Continuation of operation after compromise or catastrophe

The responsible persons according to the role concept decide how operation is to be resumed, depending on the type of disaster. Operations should be resumed after 10 working days, provided that the cause of the compromise or disaster has been eliminated. Resumption of operations may be achieved either by reinstallation or restoration according to documented procedures or a combination of both. If required, also at an alternative location. Prior to this, however, it is ensured that appropriate measures are taken to eliminate the causes of the failure or compromise in the future.

5.8 Termination of certification operations

The TSP has a continuously updated termination plan in which details are laid down in the event of cessation of operations. The aim is to ensure continuity of service and an orderly wind-down.

The TSP shall notify certificate holders, applicant and third parties, including relying third parties and the competent supervisory authority, of the discontinuation of the certification service in good time, but at least two months in advance. In addition, all further contractual relationships with third parties concerning the provision of trust services by the TSP shall be terminated upon discontinuation.

The TSP attempts to achieve a takeover of all qualified certificates (including the public keys) by another qualified trust service provider, but cannot guarantee this. The VDA shall also hand over - as far as permissible - its complete documentation to the acquiring trust service provider. At least all records pursuant to Article 24 para. 2 lit. h) of the eIDAS Regulation as well as in particular all information and documentation on the individual certificate holders for registration, logging of all events of the certificate lifecycle and the source data of the OCSP responder as a database extract are handed over. The information on the qualified certificates is provided by the acquiring trust service provider or by the BNetzA on the basis of export and transfer of the certificate status of all certificates regardless of their status.

If a takeover of the qualified certificates by another qualified trust service provider is not possible, the TSP revokes all still valid qualified certificates. In this case, the issued qualified certificates are transferred to the trust infrastructure created by the BNetzA. The public keys of the root and CA certificate are transferred to the qualified VDA or BNetzA taking over the certificates and continue to be held publicly available by the VDA or BNetzA for an appropriate period of time. The private keys of affected CAs and existing backups will be destroyed.

The German Federal Chamber of Notaries has agreed to bear the costs for the takeover of the qualified certificates issued by the Certification Body as qualified trust service provider by another qualified trust service provider or their transfer into the trust infrastructure of the competent supervisory authority as well as the costs for the notification of the certificate holders, the

supervisory authority and other third parties.

6 Technical security measures

6.1 Generation and installation of key pairs

6.1.1 Generation of key pairs

CA keys, OCSP keys and keys for qualified end-user certificates are always generated in a secure environment on an approved remote QSCD that has been evaluated according to the Common Criteria specifications and is on the EU list of trusted certified components (see section 5.1).

The keys of the end-user certificates for remote signatures are generated and stored on a certified remote QSCD, the HSM. This applies both to qualified signature certificates for natural persons and to qualified seal certificates for legal persons.

New key pairs and certificates are generated in good time before the certificate validity expires to ensure a smooth transition. The process for generating CA keys, the key ceremony, takes place according to the corresponding specifications and is documented. The same applies to the creation of service certificates. The role concept of the TSP and the four-eyes principle are applied to key generation. In line with previous TSP practice, the number of TSP employees authorised to generate keys is kept as low as possible. An independent auditor accompanies the key generation.

6.1.2 Delivery of private keys for certificate subscribers

The private keys of qualified certificates for natural persons and legal persons are generated and stored exclusively in an HSM (remote QSCD) and are not delivered to the certificate holders.

6.1.3 Delivery of the public keys to the CA

The public key is transferred to the CA in encrypted form as part of the certificate creation process.

6.1.4 Delivery of the CA public keys

The CA's public keys are available to PKI participants in the Certification Authority's publications. The CA and service certificates can be obtained from the public directory.

6.1.5 Key lengths

The recommendations of the SOG-IS Crypto Working Group apply to the key length. At present, either RSA keys with a length of at least 3072 bits or ECDSA keys with a length of at least 384 bits are used for end-user certificates for natural persons. For legal persons, ECDSA keys with a length of at least 384 bits are used for the end-user certificates.

The CA keys and service certificates have a length of 4096 bits for RSA and 521 bits for ECDSA (secp521r1).

6.1.6 Key parameters and quality control of the parameters

The key parameters and the QSCDs used are based on the recommendations of the SOG-IS Crypto Working Group or the confirmation documents of the QSCD. Compliance with the specifications is continuously checked by a person responsible for this.

6.1.7 Key usage

The CA keys are used exclusively for signing end-user certificates, the OCSP keys (service certificates) for signing OCSP requests. The CA and OCSP keys are used in a secure environment (compare section 5.1).

- Qualified certificates for natural persons (for qualified signatures)

The key usage for end-user certificates is part of the X.509 certificate and may only be used for qualified signatures.

- Qualified certificates for legal persons (for qualified seals)

Keys for end-user certificates may only be used for qualified seals.

6.2 Private key security and cryptographic module

6.2.1 Standards and security measures

The cryptographic modules used comply with the legal requirements and standards and are operated in the environment required according to the certification of the components (see section 5.1). Access to the components is protected by technical and organisational measures.

The QSCD is kept and operated in a secure area of the TSP. This ensures that the QSCD cannot be manipulated by third parties.

The certification of the QSCDs in use is checked throughout the entire life cycle to ensure that it is up to date. If there is a change in the status of the certification, the effects are analysed and appropriate measures are defined.

6.2.2 Multi-eye principle for key activation

CA keys can only be activated in a technically enforced multi-eye principle involving several roles.

6.2.3 Key restoration

Keys cannot be deposited and thus cannot be restored.

6.2.4 Key backup

There are backups of the private CA keys. The backup, restoration and access to the private CA keys encrypted by the HSM is only possible by authorised persons in the four-eyes principle.

6.2.5 Key archiving

Keys are not archived.

6.2.6 Key transfer

The keys secured by the HSM can be transferred in the four-eyes principle for the purpose of exchanging an HSM.

6.2.7 Key storage

The keys are stored on remote QSCDs and are encrypted using an HSM in accordance with ETSI TS 119 431-1 and stored in a TSP database.

6.2.8 Activation of private keys

CA keys and OCSP keys (service certificates) can only be activated in a technically enforced multi-eye principle involving multiple roles. End-user certificate keys, CA keys and OCSP keys must be activated by entering the PIN.

6.2.9 Deactivation of private keys

Private keys for CA, service and end-user certificates are deactivated when the connection between the application, card reader and QSCD is disconnected or when the QSCD is disconnected from the card reader or when the HSM is disconnected or deactivated, as well as when the application accessing it is stopped. Permanent deactivation occurs after the PIN has been entered incorrectly several times. A limited number of reactivation attempts via a PUK are possible.

6.2.10 Destruction of private keys

Keys are destructed by destroying the chip on the QSCD or by deleting the keys secured on the HSM. EE, CA and OCSP keys are destroyed at the end of their validity.

All copies/backups of private keys are destroyed after expiry or revocation, so that any further use or derivation thereof is excluded.

6.2.11 Description of the cryptographic modules

Only modules certified to apply qualified signatures in accordance with the applicable specifications are used.

6.3 Other aspects of key pair management

6.3.1 Archiving the public keys

The public keys of the end-user certificates are archived in accordance with the legal requirements (see section 5.5).

6.3.2 Validity period of keys and certificates

The validity period of the key pairs and certificates based on them corresponds at most to the permitted validity for qualified certificates according to the algorithm catalogue of the BNetzA. When the suitability of a deployed algorithm or the deployed QSCD expires, the keys are revoked before the certificate validity expires (see section 4.9).

6.4 Activation data

6.4.1 Generation and installation of signature and seal creation data Activation data

Signature and seal creation data within the meaning of the eIDAS Regulation (EU 910/2014) are defined as such unique data that are used by the signatory to create an electronic signature or an electronic seal. This unique data can take the form of either a PIN number or a private cryptographic key (with authentication certificate) that is under the control of the signatory.

The signature creation data required to activate the private key (the authentication certificate) is generated for the certificate holder in the case of authentication cards by the subscriber as part of the certificate application and identification process and is permanently linked to the certificate holder by the TSP. Creation and provision for software authentication certificates takes place via a protected portal that is only accessible to the (authorised) applicant. Certificate creation including PIN assignment takes place locally on the client of the (authorised) applicant.

The authentication mechanism based on an authentication certificate can be regarded as the signature creation date within the meaning of the eIDAS Regulation (EU 910/2014).

6.4.2 Protection of signature and seal creation data

For remote signatures, the activation data for participants is stored in encrypted form in a secure computer centre of the TSP, and the certificate holder himself is responsible for protecting his activation data for the authorisation of the private key.

For remote seals, the authorised applicant is responsible for protecting the activation data for the authorisation of the private key. This applies to both authentication certificates and authentication cards.

The activation data for CA keys are only known to the owner of the CA key.

6.4.3 Other aspects of the activation data

In addition to the PIN, a PUK is also part of the activation data for chip cards. The PUK is used to reset the misuse counter if the PIN is entered incorrectly. However, it cannot be used to set a new PIN. The PUK is created, installed and secured in the same way as the PIN.

6.5 Computer security

The TSP uses various technical and organisational measures to ensure that the IT systems can only be used for the designated purpose and are always operated in conformity with the security concept. The mechanisms include monitoring systems, logging systems, multi-level firewall and access systems, strict network segmentation, strict role separation and personalised accounts, integrity protection and monitoring of the cryptographic modules used, virus protection, regular penetration tests and audits. The IT systems are operated in a secure environment (see section 5.1) to protect them from unauthorised access, modification and theft. Unnecessary services, programmes and accounts are removed before the IT components are put into operation.

The system time of all IT systems of the TSP is continuously synchronised with the legally valid time according to the German Units and Time Act.

Access to the systems of the TSP is only granted after appointment to the corresponding role and is immediately withdrawn upon dismissal (see also section 5.3.4). Access is always via multifactor authentication and is logged. Changes to the security mechanisms and IT systems are made according to a defined process, are documented and can only be carried out using the four-eyes principle. The four-eyes principle is technically enforced and cannot be circumvented. This also applies to the recovery of data. The implemented role concept and role exclusion criteria ensure that each person working for the TSP only receives the access and access rights necessary to perform his role. For this purpose, a distinction is made in the technical roles between various administrative, operational and auditing roles.

There are working instructions for the employees of the TSP concerning compliance with the specifications on computer security.

In order to prevent unauthorised persons from gaining access to sensitive data, data carriers are securely deleted before they are reused. Defective data media are destroyed according to a secure procedure.

TSP employees are responsible for their actions in accordance with the applicable legal provisions.

6.6 Technical control during the life cycle

6.6.1 Security measures during the construction, development and expansion of IT systems and software components.

The TSP follows the principles of "Security by Design". Prior to changes, extensions or the construction of new systems, as well as in software development projects, the security requirements are ascertained in order to be able to take them into account in the conception phase. The security requirements are derived, among others, from the certification practice statement, the Certificate Policy, the underlying security concepts and the following sources:

- Legal requirements
- Manufacturer specifications
- Best practices

- Technical guidelines of the BSI, if applicable
- Other applicable standards, if applicable

The commissioning of new components, changes to systems and the implementation of fixes follow defined processes. All changes are appropriately documented.

The life cycle ends with the safe disposal of the systems.

6.6.2 Safety measures during operation

The operation of the components and compliance with the specified operating parameters are continuously monitored with the help of a monitoring system. If safety-relevant events are detected, an alarm is triggered. It is ensured that no sensitive data is leaked via this channel. The monitoring data is also used for capacity planning. Furthermore, all security-relevant processes and malfunctions as well as staff access are logged. Logged in this context - insofar as security-relevant - are in particular the start and termination of the IT systems, start and termination of the logging functionality of the relevant IT systems (in particular firewall, database systems, TOE, RA system), system crashes, hardware failures, activities of the firewall and routers as well as access attempts to the PKI system. The corresponding logs are kept in accordance with legal requirements.

Only software from trustworthy sources is put into operation. The integrity of the software is continuously monitored and changes to the system are reported. Security-critical errors are corrected within a reasonable time and security-relevant patches are applied promptly. Patches are not applied if they result in disadvantages and instabilities that are more serious than the benefits of the patch. The non-application of such updates and the reason for this is documented.

Certified components are always operated in accordance with the required operating environment. In addition, an automatic log analysis takes place to detect errors and attempted attacks at an early stage. This measure is supplemented by regular manual checks. In addition to the logs, the audit logs in particular are also checked. Attack attempts, violations of the security rules and messages from the monitoring system are reported to the administrators, who immediately take care of rectifying the error or narrowing down possible security-relevant events. Security-relevant incidents and open security gaps are immediately reported to the TSP security officer, who evaluates the implementation of all measures necessary to remedy the security incident and then has them implemented if necessary and documents the process. Relevant security incidents are reported to the supervising body within 24 hours. If applicable, persons and companies affected by the security incident are also informed immediately.

Critical vulnerabilities that have not been addressed elsewhere are addressed within 48 hours of their discovery. Based on an assessment of the risk associated with such vulnerabilities, the TSP will fix them or - if this is not possible with economically justifiable effort in relation to the impact -

document why they are not fixed.

All IT systems and software components are always operated in accordance with the manufacturer's specifications.

Data is backed up on hard drives, which are replaced as soon as they become inoperable or may no longer be operated according to the manufacturer's specifications. Data loss due to ageing data media is avoided by storing data redundantly.

The TSP has vulnerability scans and penetration tests carried out regularly, quarterly or annually, by an independent and expert third party or employee of the corresponding specialist department of the German Federal Chamber of Notaries. The results are documented, evaluated by the TSP and any deficiencies identified are remedied, if necessary.

6.7 Network security

The IT systems of the TSP are protected by firewalls. The networks of the security area are segmented into different network zones and physically separated from each other by multi-level firewall systems. The IT systems are distributed across the different network segments according to their protection needs and functions. Systems of the same protection requirement and with the same functionality are located in the same zones. The most important systems for the operation of the TSP, such as the root CA, are located in the zone with the highest protection requirement. A separate network is used for the administration of the IT systems. Separate networks also exist for test environments. The connections and protocols between the segments are limited to the minimum necessary for the functional scope. All other connections are blocked and unauthorised access is logged. The transfer of sensitive data is always encrypted. Communication channels requiring special protection can only be established if the two endpoints authenticate each other. The network environment and the connection of the networks are designed for high availability. To ensure compliance with network and system security, penetration tests are regularly carried out on the externally accessible and internal IP addresses by qualified personnel. The penetration tests are repeated in the event of security-significant changes.

Compliance is monitored on a regular basis.

6.8 Time-stamp

The rules on the qualified time-stamping service are regulated in the document Time-Stamp Policy and TSA Practice Statement of the TSP.

7 Profiles of certificates, revocation lists and OCSP

7.1 Certificate profiles

The serial numbers of the certificates issued by the TSP are generated randomly.

7.1.1 Root CA

Certificate profile RSA

Field (OID)	Description	Value
Version	x.509 version number	V3 (2)
serialNumber (2.5.4.5)	Serial number of the certificate	[6f b8 e3 d6 dc a1 f6 bb]
Signature algorithm	Identifier (OID) Signature algorithm	SHA512withRSAandMGF1 (1.2.840.113549.1.1.10)
Signature hash algorithm	Identifier (OID) Signature hash algorithm	SHA-512 (2.16.840.1.101.3.4.2.3)
algorithmIdentifier	Identifier (OID) key algorithm	RSA (1.2.840.113549.1.1.1)
Key length	Key length	4096 bits
Issuer		
countryName (2.5.4.6)	Name country issuer	C = DE
organizationName (2.5.4.10)	Name organisation	O = German Federal Chamber of Notaries
organizationIdentifier (2.5.4.97)	Identification organisation	2.5.4.97 = DE122788238
organizationalUnitName (2.5.4.11)	Name organisational unit	OU = Certification Authority
commonName (2.5.4.3)	Name holder	CN = BNotK Root CA 2017
Validity		

UTCTime (1.3.6.1.4.1.1466.115.121.1.53)	Start	e.g. 2017-10-09 08:57:57 UTC
	End	e.g. 2037-10-09 08:57:56 UTC
Holder		
countryName (2.5.4.6)	Name country holder	C = DE
organizationName (2.5.4.10)	Name organisation	O = German Federal Chamber of Notaries
organizationIdentifier (2.5.4.97)	Identification organisation	2.5.4.97 = DE122788238
organizationalUnitName (2.5.4.11)	Name organisational unit	OU = Certification Authority
commonName (2.5.4.3)	Name holder	CN = BNotK Root CA 2017
Extensions		
keyUsage (2.5.29.15)	Purpose	keyCertSign, cRLSign
basicConstraints (2.5.29.19)	Restrictions on the use of the certificate	Type applicant=Certification Authority Constraint path length=0
subjectKeyIdentifier (2.5.29.14)	Public key identifier of the holder	[CC53A403E638247DD255 DA0567EE7D78B940B3BA]
authorityKeyIdentifier (2.5.29.35)	Issuer public key identifier	[FDF35084308EEC239AF5 33B2E38107DDE4EF80AE]
authorityInfoAccess (1.3.6.1.5.5.7.1.1)	Reference to issuer and service for status inquiry	see following elements
calssuers (1.3.6.1.5.5.7.48.2)	URL to issuer info	https://zertifizierungsstelle.bnotk.de/veroeffentlichungen
ocsp (1.3.6.1.5.5.7.48.1)	URL to the OCSP service	http://ocsp.zs.bnotk.de/eqsig

Sub-CA Certificate Profile ECC

Field (OID)	Description	Value
Version	x.509 version number	V3 (2)

serialNumber (2.5.4.5)	Serial number of the certificate	[6f b8 e3 d6 dc a1 f6 bb]
Signature algorithm (1.2.840.10045.4.3.4)	Identifier (OID) Signature algorithm	SHA512WITHECDSA
Key length	Key length	521 bits
Issuer		
countryName (2.5.4.6)	Name country issuer	C = DE
organizationName (2.5.4.10)	Name organisation	O = German Federal Chamber of Notaries
organizationIdentifier (2.5.4.97)	Identification organisation	2.5.4.97 = DE122788238
organizationalUnitName (2.5.4.11)	Name organisational unit	OU = Certification Authority
commonName (2.5.4.3)	Name holder	e.g. CN = BNotK Root CA 2017
Validity		
UTCTime	Start	Certificate valid from
	End	Certificate valid until
Holder		
countryName (2.5.4.6)	Name country holder	C = DE
organizationName (2.5.4.10)	Name organisation	O = German Federal Chamber of Notaries
organizationIdentifier (2.5.4.97)	Identification organisation	2.5.4.97 = DE122788238
organizationalUnitName (2.5.4.11)	Name organisational unit	OU = Certification Authority
commonName (2.5.4.3)	Name holder	e.g. CN = BNotK Root CA 2017

Extensions		
keyUsage (2.5.29.15)	Purpose	keyCertSign, cRLSign
basicConstraints (2.5.29.19)	Restrictions on the use of the certificate	Type applicant=Certification Authority Constraint path length=0
subjectKeyIdentifier (2.5.29.14)	Public key identifier of the holder	[CC53A403E638247DD255 DA0567EE7D78B940B3BA]
authorityKeyIdentifier (2.5.29.35)	Issuer public key identifier	[FDF35084308EEC239AF5 33B2E38107DDE4EF80AE]
authorityInfoAccess (1.3.6.1.5.5.7.1.1)	Reference to issuer and service for status inquiry	see following elements
calssuers (1.3.6.1.5.5.7.48.2)	URL to issuer info	https://zertifizierungsstelle.bnotk.de/veroeffentlichungen
ocsp (1.3.6.1.5.5.7.48.1)	URL to the OCSP service	http://ocsp.zs.bnotk.de/eqsig

7.1.2 Sub-CA

Certificate profile RSA

Field (OID)	Description	Value
Version	x.509 version number	V3 (2)
serialNumber (2.5.4.5)	Serial number of the certificate	e.g. [6f b8 e3 d6 dc a1 f6 bb]
Signature algorithm	Identifier (OID) signature algorithm	SHA512withRSAandMGF1 (1.2.840.113549.1.1.10)
Signature hash algorithm	Identifier (OID) signature hash algorithm	SHA-512 (2.16.840.1.101.3.4.2.3)
algorithmIdentifier	Identifier (OID) key algorithm	RSA (1.2.840.113549.1.1.1)
Key length	Key length	4096 bits
Issuer		
countryName	Name country issuer	C = DE

(2.5.4.6)		
organizationName (2.5.4.10)	Name organisation	O = German Federal Chamber of Notaries
organizationIdentifier (2.5.4.97)	Identification organisation	2.5.4.97 = DE122788238
organizationalUnitName (2.5.4.11)	Name organisational unit	OU = Certification Authority
commonName (2.5.4.3)	Name holder	CN = BNotK Root CA 2017
Validity		
UTCTime (1.3.6.1.4.1.1466.115.121.1.53)	Start	Start certificate validity
	End	End of certificate validity
Holder		
countryName (2.5.4.6)	Name country holder	C = DE
organizationName (2.5.4.10)	Name organisation	O = German Federal Chamber of Notaries
organizationIdentifier (2.5.4.97)	Identification organisation	2.5.4.97 = DE122788238
organizationalUnitName (2.5.4.11)	Name organisational unit	OU = Certification Authority
commonName (2.5.4.3)	Name holder	e.g. CN = BNotK qSig CA 2017
Extensions		
keyUsage (2.5.29.15)	Purpose	keyCertSign, cRLSign
basicConstraints (2.5.29.19)	Restrictions on the use of the certificate	Type applicant=Certification Authority Constraint path length=0
subjectKeyIdentifier (2.5.29.14)	Public key identifier of the holder	e.g. [CC53A403E638247DD255 DA0567EE7D78B940B3BA]
authorityKeyIdentifier	Identification of public	[FDF35084308EEC239AF5

(2.5.29.35)	keys of the issuer	33B2E38107DDE4EF80AE]
authorityInfoAccess (1.3.6.1.5.5.7.1.1)	Reference to issuer and service for status inquiry	see following elements
calssuers (1.3.6.1.5.5.7.48.2)	URL to issuer info	https://zertifizierungsstelle.bnotk.de/veroeffentlichungen
ocsp (1.3.6.1.5.5.7.48.1)	URL to the OCSP service	http://ocsp.zs.bnotk.de/eqsig

Sub-CA Certificate Profile ECC

Field (OID)	Description	Value
Version	x.509 version number	V3 (2)
serialNumber (2.5.4.5)	Serial number of the certificate	e.g. [6f b8 e3 d6 dc a1 f6 bb]
Signature algorithm (1.2.840.10045.4.3.4)	Identifier (OID) Signature algorithm	SHA512WITHECDS
Key length	Key length	521 bits
Issuer		
countryName (2.5.4.6)	Name country issuer	C = DE
organizationName (2.5.4.10)	Name organisation	O = German Federal Chamber of Notaries
organizationIdentifier (2.5.4.97)	Identification organisation	2.5.4.97 = DE122788238
organizationalUnitName (2.5.4.11)	Name organisational unit	OU = Certification Authority
commonName (2.5.4.3)	Name holder	e.g. CN = BNotK Root CA 2017
Validity		
UTCTime (1.3.6.1.4.1.1466.115.121.1.53)	Start	Start certificate validity
	End	End of certificate validity

Holder		
countryName (2.5.4.6)	Name country holder	C = DE
organizationName (2.5.4.10)	Name organisation	O = German Federal Chamber of Notaries
organizationIdentifier (2.5.4.97)	Identification organisation	2.5.4.97 = DE122788238
organizationalUnitName (2.5.4.11)	Name organisational unit	OU = Certification Authority
commonName (2.5.4.3)	Name holder	e.g. CN = BNotK qSig CA 2017
Extensions		
keyUsage (2.5.29.15)	Purpose	keyCertSign, cRLSign
basicConstraints (2.5.29.19)	Restrictions on the use of the certificate	Type applicant=Certification Authority Constraint path length=0
subjectKeyIdentifier (2.5.29.14)	Public key identifier of the holder	e.g. [CC53A403E638247DD255 DA0567EE7D78B940B3BA]
authorityKeyIdentifier (2.5.29.35)	Issuer public key identifier	[FDF35084308EEC239AF5 33B2E38107DDE4EF80AE]
authorityInfoAccess (1.3.6.1.5.5.7.1.1)	Reference to issuer and service for status inquiry	see following elements
calssuers (1.3.6.1.5.5.7.48.2)	URL to issuer info	https://zertifizierungsstelle.bnotk.de/veroeffentlichungen
ocsp (1.3.6.1.5.5.7.48.1)	URL to the OCSP service	http://ocsp.zs.bnotk.de/eqsig

7.1.3 End-user certificate profile

QCP-n-qscd RSA - qualified signature certificates on qualified signature creation devices based on an RSA crypto algorithm.

Field (OID)	Description	Value
Version	x.509 version number	V3 (2)
serialNumber	Serial number of the certificate	e.g. [6f b8 e3 d6 dc a1 f6 bb]

(2.5.4.5)		
Signature algorithm	Identifier (OID) signature algorithm	SHA512withRSAandMGF1 (1.2.840.113549.1.1.10)
Signature hash algorithm	Identifier (OID) signature hash algorithm	SHA-512 (2.16.840.1.101.3.4.2.3)
algorithmIdentifier	Identifier (OID) key algorithm	RSA (1.2.840.113549.1.1.1)
Key length	Key length	2048 bits
Issuer		
countryName (2.5.4.6)	Name country issuer	C = DE
organizationName (2.5.4.10)	Name organisation	O = German Federal Chamber of Notaries
organizationIdentifier (2.5.4.97)	Identification organisation	2.5.4.97 = DE122788238
organizationalUnitName (2.5.4.11)	Name organisational unit	OU = Certification Authority
commonName (2.5.4.3)	Name holder	e.g. CN = BNotK qSig CA 2017
Validity		
UTCTime (1.3.6.1.4.1.1466.115.121.1.53)	Start	Start certificate validity
	End	End of certificate validity
Holder		
countryName (2.5.4.6)	Name country holder	e.g. C = DE Country in which the certificate holder resides or in which the presented identification document of the certificate holder was issued.
organizationName (2.5.4.10)	Name organisation	O = [Organisation]
organizationIdentifier (2.5.4.97)	Identification organisation	2.5.4.97 = [Identifier Organisation]

organizationalUnitName (2.5.4.11)	Name organisational unit	OU = [Department]
commonName (2.5.4.3)	Name holder	CN = First name(s) Last name
serialNumber (2.5.4.5)	Identifier holder	2.5.4.5 = Identification number (locally defined, if applicable)
givenName (2.5.4.42)	First name holder	2.5.4.42 = First name(s)
surname (2.5.4.4)	Surname holder	2.5.4.4 = Surname
title (2.5.4.12)	Title holder	2.5.4.12 = Title
emailAdress (1.2.840.113549.1.9.1)	Email address holder	emailAdress = [name@domain.tld]
(0.9.2342.19200300.100.1.1)	Unique user ID for linking means of authentication and remote signature	restrictedID of the eID, unique user ID of card owner
Extensions		
keyUsage (2.5.29.15)	Purpose	nonRepudiation
basicConstraints (2.5.29.19)	Restrictions on the use of the certificate	Type applicant=End Entity Restriction path length=None
subjectKeyIdentifier (2.5.29.14)	Public key identifier of the holder	[CC53A403E638247DD255 DA0567EE7D78B940B3BA]
authorityKeyIdentifier (2.5.29.35)	Issuer public key identifier	[FDF35084308EEC239AF5 33B2E38107DDE4EF80AE]
authorityInfoAccess (1.3.6.1.5.5.7.1.1)	Reference to issuer and service for status inquiry	see following elements
calssuers (1.3.6.1.5.5.7.48.2)	URL to issue info	https://zertifizierungsstelle.bnotk.de/veroeffentlichungen
ocsp (1.3.6.1.5.5.7.48.1)	URL to the OCSP service	http://ocsp.zs.bnotk.de/eqsig

CertificatePolicies (2.5.29.32)		Reference to applicable certification policy	see following elements
Policy information	policyIdentifier	Identifier (OID) and URL reference to CPS	1.3.6.1.4.1.41460.5.2.1.1.2
	policyQualifier		https://zertifizierungsstelle.bnotk.de/veroeffentlichungen
qcStatements (1.3.6.1.5.5.7.1.3)		Identifier (OID) eIDAS compliance qSig	see following elements
QcCompliance (0.4.0.1862.1.1)		Qualified certificate	0.4.0.1862.1.1
QcSSCD (0.4.0.1862.1.4)		Generation on SSCD	0.4.0.1862.1.4
QcType (0.4.0.1862.1.6)		Type (Electr. signature)	0.4.0.1862.1.6.1
QcPDS (0.4.0.1862.1.5)		URL reference to PDS	https://zertifizierungsstelle.bnotk.de/veroeffentlichungen
subjectAltName (2.5.29.17)		Email address holder	[name@domain.tld] According to IETF RFC 5280 [7]
Subject Directory Attributes (2.5.29.9)		Additional features describing the holder or certificate	see following elements
dateOfCertGen (1.3.36.8.3.1)		Date of certificate creation	e.g. 2017-10-09 08:57:57 UTC
admission (1.3.36.8.3.3)		Occupational attributes holder	[admissionAuthorithy, namingAuthorithy, professionInfo]
procuration (1.3.36.8.3.2)		Information on procuration	[StringType]
restriction (1.3.36.8.3.1)		Other restrictions related to the use of the certificate	[StringType]

QCP-n-qscd (ECDSA) - qualified signature certificates on qualified signature creation devices based on an ECDSA crypto algorithm.

Field (OID)	Description	Value
Version	x.509 version number	V3 (2)

serialNumber (2.5.4.5)	Serial number of the certificate	e.g. [6f b8 e3 d6 dc a1 f6 bb]
Signature algorithm (1.2.840.10045.4.3.4)	Identifier (OID) signature algorithm	SHA512WITHECDSA (1.2.840.10045.4.3.4)
Signature hash algorithm	Identifier (OID) signature hash algorithm	SHA-512 (2.16.840.1.101.3.4.2.3)
algorithmIdentifier	Identifier (OID) key algorithm	ECDSA (1.2.840.10045.4.3.4)
Key length	Key length	521 bits
Issuer		
countryName (2.5.4.6)	Name country	C = DE
organizationName (2.5.4.10)	Name organisation	O = German Federal Chamber of Notaries
organizationIdentifier (2.5.4.97)	Identification organisation	2.5.4.97 = DE122788238
organizationalUnitName (2.5.4.11)	Name organisational unit	OU = Certification Authority
commonName (2.5.4.3)	Name holder	e.g. CN = BNotK qSig CA 2017

Validity		
UTCTime (1.3.6.1.4.1.1466.115.121.1.53)	Start	Start certificate validity
	End	End of certificate validity
Holder		
countryName (2.5.4.6)	Name country	C = DE
organizationName (2.5.4.10)	Name organisation	O = [Organisation]
organizationIdentifier (2.5.4.97)	Identification organisation	2.5.4.97 = [Identifier Organisation]
organizationalUnitName (2.5.4.11)	Name organisational unit	OU = [Department]

commonName (2.5.4.3)	Name holder	CN = First name(s) Last name
serialNumber (2.5.4.5)	Identifier holder	2.5.4.5 = Identification number (locally defined, if applicable)
givenName (2.5.4.42)	First name holder	2.5.4.42 = First name(s)
surname (2.5.4.4)	Surname holder	2.5.4.4 = Surname
title (2.5.4.12)	Title holder	2.5.4.12 = Title
emailAdress (1.2.840.113549.1.9.1)	Email address holder	emailAdress = [name@domain.tld]
userID (0.9.2342.19200300.100.1.1)	Unique user ID for linking means of authentication and remote signature	restrictedID of the eID, unique user ID of certificate holder
Extensions		
keyUsage (2.5.29.15)	Purpose	nonRepudiation
basicConstraints (2.5.29.19)	Restrictions on the use of the certificate	Type applicant=End Entity Restriction path length=None

subjectKeyIdentifier (2.5.29.14)	Public key identifier of the holder	[CC53A403E638247DD255 DA0567EE7D78B940B3BA]
authorityKeyIdentifier (2.5.29.35)	Issuer public key identifier	[FDF35084308EEC239AF5 33B2E38107DDE4EF80AE]
authorityInfoAccess (1.3.6.1.5.5.7.1.1)	Reference to issuer and service for status inquiry	see following elements
calssuers (1.3.6.1.5.5.7.48.2)	URL to issuer info	https://zertifizierungsstelle.bnotk.de/veroeffentlichungen
ocsp (1.3.6.1.5.5.7.48.1)	URL to the OCSP service	http://ocsp.zs.bnotk.de/eqsig
CertificatePolicies (2.5.29.32)	Reference to applicable certification policy	see following elements

Policy information	policyIdentifier	Identifier (OID) and URL reference to CPS	1.3.6.1.4.1.41460.5.2.1.1.2
	policyQualifier		https://zertifizierungsstelle.bnotk.de/veroeffentlichungen
qcStatements (1.3.6.1.5.5.7.1.3)		Identifier (OID) eIDAS compliance qSig	see following elements
QcCompliance (0.4.0.1862.1.1)		Qualified certificate	0.4.0.1862.1.1
QcSSCD (0.4.0.1862.1.4)		Generation on SSCD	0.4.0.1862.1.4
QcType (0.4.0.1862.1.6)		Type (electr. signature)	0.4.0.1862.1.6.1

QcPDS (0.4.0.1862.1.5)	URL reference to PDS	https://zertifizierungsstelle.bnotk.de/veroeffentlichungen
subjectAltName (2.5.29.17)	Email address holder	[name@domain.tld]
Subject Directory Attributes (2.5.29.9)	Additional features describing the holder or certificate	see following elements
dateOfCertGen (1.3.36.8.3.1)	Date of certificate creation	e.g. 2017-10-09 08:57:57 UTC
admission (1.3.36.8.3.3)	Occupational attributes holder	[admissionAuthorithy, namingAuthorithy, professionInfo]
procuration (1.3.36.8.3.2)	Information on procuration	[StringType]
restriction (1.3.36.8.3.1)	Other restrictions related to the use of the certificate	[StringType]

QCP-l-qscd (ECDSA) - qualified seal certificates on qualified seal creation devices based on an ECDSA crypto algorithm.

Field (OID)	Description	Value
Version	x.509 version number	V3 (2)

serialNumber (2.5.4.5)	Serial number of the certificate	e.g. [6f b8 e3 d6 dc a1 f6 bb]
Signature algorithm	Identifier (OID) signature algorithm	SHA512withECDSA (1.2.840.113549.1.1.10)
Signature hash algorithm	Identifier (OID) signature hash algorithm	SHA-512 (2.16.840.1.101.3.4.2.3)
algorithmIdentifier	Identifier (OID) key algorithm	ECDSA_P384 (1.2.840.113549.1.1.1)
Key length	Key length	384 bits

Issuer		
countryName (2.5.4.6)	Name country	C = DE
organizationName (2.5.4.10)	Name organisation	O = German Federal Chamber of Notaries
organizationIdentifier (2.5.4.97)	Identification organisation	2.5.4.97 = DE122788238
organizationalUnitName (2.5.4.11)	Name organisational unit	OU = Certification Authority
commonName (2.5.4.3)	Name holder	e.g. CN = BNotK qSig CA 2021
Validity		
UTCTime (1.3.6.1.4.1.1466.115.121.1.53)	Start	Start certificate validity
	End	End of certificate validity
Holder		
countryName (2.5.4.6)	Name country	C = DE
organizationName (2.5.4.10)	Name organisation	O = [Organisation]
organizationalUnitName (2.5.4.11)	Name organisational unit	OU = [Department]
commonName (2.5.4.3)	Name holder	CN = organisation name or other designation belonging to the organisation.

userID (0.9.2342.19200300.100.1.1)	Unique user ID for linking means of authentication and remote signature	Unique UUID of the certificate holder
Extensions		

keyUsage (2.5.29.15)		Purpose	nonRepudiation
basicConstraints (2.5.29.19)		Restrictions on the use of the certificate	Type applicant=End Entity Restriction path length=None
subjectKeyIdentifier (2.5.29.14)		Public key identifier of the holder	[CC53A403E638247DD255 DA0567EE7D78B940B3BA]
authorityKeyIdentifier (2.5.29.35)		Issuer public key identifier	[FDF35084308EEC239AF5 33B2E38107DDE4EF80AE]
authorityInfoAccess (1.3.6.1.5.5.7.1.1)		Reference to issuer and service for status inquiry	see following elements
calssuers (1.3.6.1.5.5.7.48.2)		URL to issuer info	https://zertifizierungsstelle.bnotk.de/veroeffentlichungen
ocsp (1.3.6.1.5.5.7.48.1)		URL to the OCSP service	http://ocsp.zs.bnotk.de/eqsig
CertificatePolicies (2.5.29.32)		Reference to applicable certification policy	see following elements
Policy information	policyIdentifier	Identifier (OID) and URL reference to CPS	1.3.6.1.4.1.41460.5.2.1.1.2
	policyQualifier		https://zertifizierungsstelle.bnotk.de/veroeffentlichungen
qcStatements (1.3.6.1.5.5.7.1.3)		Identifier (OID) eIDAS compliance qSig	see following elements
QcCompliance (0.4.0.1862.1.1)		Qualified certificate	0.4.0.1862.1.1

QcSSCD (0.4.0.1862.1.4)	Generation on SSCD	0.4.0.1862.1.4
QcType (0.4.0.1862.1.6)	Type (Electr. signature)	0.4.0.1862.1.6.2
QcPDS (0.4.0.1862.1.5)	URL reference to PDS	https://zertifizierungsstelle.bnotk.de/veroeffentlichungen

7.2 Revocation list profiles

Revocation lists are not provided for qualified certificates.

7.3 Status query service profiles

An OCSP responder according to RFC 6960 is operated to query the status of the certificates, which also supports positive information (certHash extension). The responses of the OCSP responder are signed in a qualified manner.

The BNotK OCSP responder provides information on the validity of a certificate at a specific time for a requesting third party. The following statuses are returned:

- Good – the certificate exists in the directory service and is not revoked,
- Unknown – the certificate does not exist in the directory service,
- Revoked – the certificate was revoked at the specified time.

7.3.1 Version number

OCSP v1 in accordance with RFC 6960 is used.

7.3.2 OCSP extensions

- Requests:

Extensions	**Value**
RetrieveIfAllowed	A requested certificate is supplied in the response if set (optional)

- Requests:

Extension	**Value**
RequestedCertificate	Contains the requested certificate if RetrieveIfAllowed is set.
archiveCutOff	Defines the period in which the OCSP responder provides the status information from certificate creation.

8 Conformity Audit

See section 8 of the Certificate Policy (*CP*) of the TSP.

9 Other business and legal regulations

See section 9 of the Certificate Policy (*CP*) of the TSP.

***