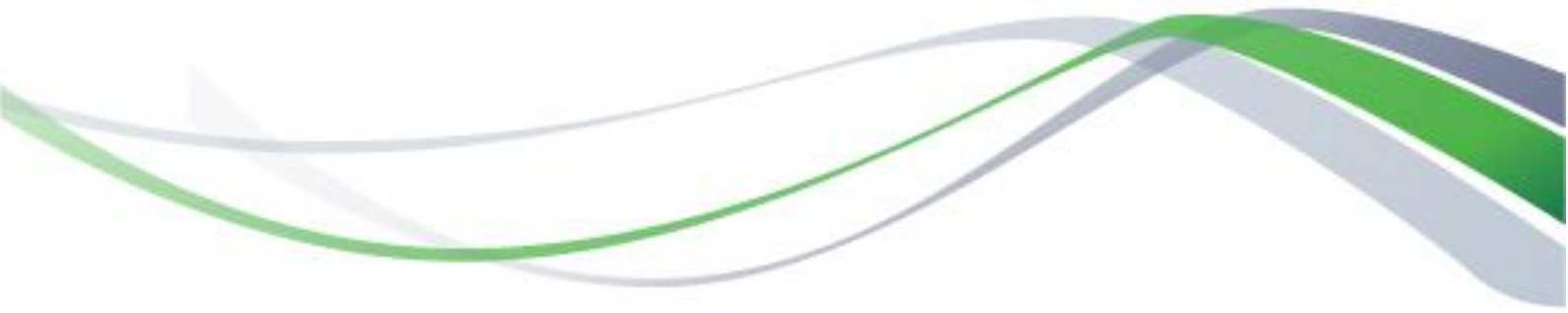
BUNDESNOTARKAMMER
ZERTIFIZIERUNGSSTELLE

Time-Stamp Policy and TSA Practice Statement of the Certification Authority of the German Federal Chamber of Notaries



Version: **2.8**

Date: **29 January 2024**

Document history

Version	Comment	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	Adjustments due to the creation of a new CA hierarchy	28/02/2018
2.1	Editorial changes	31/05/2018
2.2	Editorial changes and updating	07/06/2019
2.3	Extension by certificate profile for 'BNotK TSA Signer 2019'	25/07/2019
2.4	Editorial changes and updating	27/09/2019
2.5	Review and updating	26/02/2021
2.6	Update of certificate profiles, including ECC	12/01/2022
2.7	Annual review	16/03/2023
2.8	Review and adaptation of OID labelling	29/01/2024

Contents

1 Introduction

1.1 About this document

The German Federal Chamber of Notaries is a qualified trust service authority in the sense of Art. 3 lit. 20 of the eIDAS Regulation (EU). Services offered include the issue of qualified certificates and qualified time-stamps.

This document describes the trust service policy of the Certification Authority of the German Federal Chamber of Notaries (Zertifizierungsstelle der Bundesnotarkammer [also Trust Service Provider of the German Federal Chamber of Notaries - hereinafter referred as **TSP**]) for qualified electronic time-stamps. In the form of a Time-stamp Policy and a TSA Practice Statement, it describes how the TSP fulfils the requirements and specifications for the provision of time-stamping services.

This document 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 319 411-2 and EN 319 421.

The structure of the document is based on the ETSI EN 319 421 standard in order to facilitate comparison with corresponding policies from other trust service authorities.

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

This policy is not legally binding. Instead, the relationship between TSP and the user of the time-stamping service 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 policy does not contain any assurances, guarantees or warranties.

1.2 Identification

Document name: Time-Stamp Policy and TSA Practice Statement of the Certification Authority of the German Federal Chamber of Notaries

Identification (OID): 1.3.6.1.4.1.41460.5.4.1.1.2

Version: 2.8

All time-stamps issued by the TSP contain the OID of this policy, which is made available to certificate holders and relying parties by publication on the TSP website. The provision of the TSP time-stamping service is in line with the ETSI Best Practices Timestamp Policy (BTSP) in accordance with ETSI EN 319 421.

2 Definitions and abbreviations

Term	Description
TSA	See time-stamping authority
Time-stamping authority	Trust service authority that offers (qualified) electronic time-stamps

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

3 Overview

3.1 Time-stamping services

The TSP only creates qualified electronic time-stamps.

The time-stamping services offered are divided into two components in this policy:

- ***Provision of time-stamps***

  The creation of time-stamps.

- ***Time-stamping management***

  Monitoring and controlling the operation of the time-stamping services to ensure that the services are provided as specified in this policy. This service is responsible for the implementation as well as for changes or settings of the time-stamping services.

This subdivision is only for the purposes of this policy and does not constitute a restriction on the (internal) organisation of the time-stamping service by the TSP.

3.2 Time-Stamping Authority (TSA)

The TSP (hereinafter also referred to as the time-stamping authority) is responsible in its capacity as a time-stamping authority for the provision of the services specified in this section.

The TSP may delegate tasks to third parties. Even if tasks are transferred to third parties, the TSP retains overall responsibility for the operation of the trust service. Cf. section 1.7 of the Certification Policy of the Certification Authority of the German Federal Chamber of Notaries on the transfer of tasks to third parties.

3.3 User of the time-stamping service (subscriber)

The TSP does not provide qualified electronic time-stamps directly to end-users. In selected individual cases, qualified electronic time-stamps or time-stamping services are made available to third parties,

who may make them available to end-users. In this case, the third party is responsible for informing the end-users and for ensuring that the end-users fulfil their obligations.

4 Policies and procedures

4.1 Risk analysis

The TSP carries out a regular risk analysis in order to identify, analyse and evaluate the risks for the trust services offered. Details are set out in the TSP security concept. See section 8 of the Certification Policy (CP) of the Certification Authority of the German Federal Chamber of Notaries.

4.2 Trust Service Practice Statement

4.2.1 Format of the time-stamp

The time-stamping service used is compliant with RFC 3161 in accordance with ETSI EN 319 422 and only supports RSA encryption with 4096 bit and the SHA256, SHA384 & SHA512 hash algorithms.

4.2.2 Time accuracy

Time servers with a DFC77 receiver are used as a reliable time source to receive the legally valid time from the Physikalisch-Technische Bundesanstalt (Federal Physical Technical Institute). In the event of a temporary loss of signal, a high-precision oscillator takes over the task of the timer for the NTP server. Further NTP servers of the Physikalisch-Technische Bundesanstalt are integrated as an additional reference source. The average maximum deviation of the time is +/- 100 ms and is never greater than one second. Compliance with the exact time as well as changes and attempts to manipulate the time are continuously monitored. If the maximum permitted deviation is exceeded, the time-stamping service is automatically deactivated. Leap seconds are taken into account, processed correctly and logged.

See sections 5.6 to 5.7 on the non-technical and technical security measures against attacks and attempts to manipulate the time.

4.2.3 Restrictions on use of the time-stamping service

The statutory provisions apply, in particular any requirements of the eIDAS Regulation and the Trust Services Act.

4.2.4 Obligations of the users

The statutory provisions apply, in particular any requirements of the eIDAS Regulation and the Trust Services Act.

Please note that the TSP does not provide time-stamping services directly to end-users.

4.2.5 Verification of the time-stamp

Verification of the time-stamp requires the following steps:

- ***1. Verification of the time-stamp issuer***
  The public key of the signing CA is required to verify the issuer. It can be downloaded from the TSL and the website.

- ***2. Verification of the time-stamp status***
  The certificate status of the signing CA is verified via an OCSP responder. The address of the OCSP responder is part of the certificate.

- ***3. Verification of the time-stamp integrity***
  The integrity of the time-stamp can be verified with any RFC 3161-compliant software.

4.2.6 Applicable law

The TSP fulfils the requirements for the provision of a time-stamping service under German law.

4.2.7 Availability of the time-stamping service

The time-stamping service is operated on high-availability IT systems in a high-availability data centre to ensure that the time-stamping service is available at all times. The individual contractual agreement concluded with the TSP on guaranteed availability shall apply.

4.3 General Terms and Conditions

The individual contractual agreement concluded with the TSP shall apply.

4.4 Information security policy

See section 5.1 of the Certification Policy of the Certification Authority of the German Federal Chamber of Notaries.

4.5 Obligations of the time-stamp authority

The individual contractual agreement concluded with the TSP shall apply or, in the absence of a contractual agreement, the statutory provisions shall apply.

This policy does not establish any additional obligations on the part of TSP; in particular, this document does not contain any assurances, guarantees or warranties.

4.6 Information for relying third parties

This document and the certification policy of the Certification Authority of the German Federal Chamber of Notaries will be made available to third parties by publication on the TSP website.

Relying third parties may only rely on a TSP time-stamp if at least the following conditions are met:

- The time-stamp has been properly signed and the private key used to sign the time-stamp has not been compromised by the time the time-stamp is verified

- Any restrictions on use have been taken into account
- All other agreements and other precautionary measures were complied with
- The relying third party has used the authoritative trusted list to determine that the time-stamp and time-stamping unit (**TSU**) are qualified

5 Management and use of the time-stamping service

5.1 Internal organisation

The TSP is a public body under German law.

The TSP has a confidential security concept in which the operational requirements regarding personnel, access control and risk assessment, among other things, are documented.

The TSP has a sufficient number of reliable and qualified staff. The personnel deployed have the necessary expertise, experience and qualifications for their tasks and are trained before taking on a task and during their work.

5.2 Personnel concept

The personnel and role concept of the TSP defines the personnel measures for the operation of certification services on the one hand and the distribution of roles within the TSP on the other. All roles required for certification operations are identified and defined and their tasks are described.

Details are described in section 5.3 of the Certification Practice Statement of the Certification Authority of the German Federal Chamber of Notaries.

5.3 Asset Management

The TSP has introduced an asset management system that fulfils the legal requirements.

Details are described in section 5.2 of the Certification Practice Statement of the Certification Authority of the German Federal Chamber of Notaries.

5.4 Access control

See sections 5.1, 5.4 and 6.5 of the Certification Practice Statement of the Certification Authority of the German Federal Chamber of Notaries.

5.5 Cryptographic control

All keys used for qualified time-stamps and the certificates based on them are stored on certified QSCDs. The QSCDs are operated in a safe environment in accordance with the operating environment of the QSCD certification.

5.5.1 Key generation

Keys for time-stamps are generated in a secure environment according to the manufacturer`s specifications and in compliance with the certified conditions on an approved QSCD, which has been evaluated according to the Common Criteria specifications and is on the EU list of trustworthy certified components. The process and activation of the key is carried out by persons with the corresponding

roles according to the role concept (see section 5.2) in a secure environment in accordance with the four-eyes principle. The public certificates based on the keys are published on the TSP website at the following address: https://zertifizierungsstelle.bnotk.de/veroeffentlichungen. They are also published on the website of the Federal Network Agency and on the German Trusted List. The key generation process is repeated in good time before the keys expire to ensure a smooth transition. To ensure that this is done in a timely manner, the validity of the keys is monitored by a monitoring system.

A time-stamping unit is a group of hardware and software that is managed as a unit and for which a single private signature key is active.

5.5.2 Private key protection

The private key for time-stamps can only be used on the installed QSCDs. The QSCDs are operated in a secure, access-protected environment. Only authorised persons according to the role concept have access to the QSCDs. Access is only possible by using the four-eyes principle.

5.5.3 Public key

The public certificates based on the public keys are published on the TSP website at the following address: https://zertifizierungsstelle.bnotk.de/veroeffentlichungen. Time-stamps are only issued once the corresponding public certificate has been loaded into the TSU or its cryptographic device.

5.5.4 Key lengths

The recommendation of the SOG-IS Crypto Working Group applies to the key length. The keys currently used have a length of 4096 bits.

5.5.5 Key parameters and quality control of the parameters

The key parameters 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.

5.5.6 Key usage

The keys are used exclusively for signing time-stamps. The intended use is stored in the X.509 certificate of the key.

5.5.7 Validity period of keys and certificates

The validity period of the key pairs and the certificates based on them is a maximum of ten years. If the suitability of an algorithm or the QSCD used expires, the keys are revoked before the certificate expires.

Once the validity of the private key has expired, it is no longer possible to issue time-stamps.

5.6 Non-technical security measures

The TSP has introduced non-technical security measures in line with legal requirements.

Details are described in section 5 of the Certification Practice Statement of the Certification Authority of the German Federal Chamber of Notaries.

5.7 Technical security measures

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

Details are described in section 6 of the Certification Practice Statement of the Certification Authority of the German Federal Chamber of Notaries.

5.8 Network security

The TSP has introduced network security measures in line with legal requirements.

Details are described in section 6.7 of the Certification Practice Statement of the Certification Authority of the German Federal Chamber of Notaries.

5.9 Emergency concept

The TSP has an emergency concept.

Details are described in section 5.7 of the Certification Practice Statement of the Certification Authority of the German Federal Chamber of Notaries.

5.10 Archiving of documents

The TSP archives documents in accordance with legal requirements. Details are described in section 5.5 of the Certification Practice Statement of the Certification Authority of the German Federal Chamber of Notaries.

This applies in particular to the time-stamping service:

- TSU key management

All events relating to (i) the life-cycle of the TSU key and (ii) the TSU certificate (if required) are logged.

- Synchronisation of the time

All events concerning (i) the synchronisation of the clock of the TSU and the UTC as well as (ii) the detection of synchronisation losses are logged.

5.11 Business Continuity Management

The TSP has an emergency concept. If the time-stamping service is compromised or if time-stamps are issued with the wrong time, the affected customers are informed and the time-stamping service is deactivated until the cause is rectified. In addition, information on the identification of incorrectly issued time-stamps is made available on the TSP website.

Further details are described in section 5.7 of the Certification Practice Statement of the Certification Authority of the German Federal Chamber of Notaries.

5.12 Termination plan

The TSP has a termination plan in line with legal requirements.

Details are described in section 5.8 of the Certification Practice Statement of the Certification Authority of the German Federal Chamber of Notaries.

5.13 Compliance

The TSP operates the time-stamping service in line with the applicable law.

An accredited conformity assessment body checks at regular intervals that the TSP fulfils the legal requirements.

Details are described in the Certificate Policy.

5.14 Certificate profile

5.14.1 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. [58 ac b6 41 e3 98 90 00]
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	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	e.g. CN = BNotK qSig CA 2017
Validity		
UTCTime (1.3.6.1.4.1.1466.115.121 .1.53)	Start	e.g. 2019-06-27 12:20:24 UTC
	End	e.g. 2029-03-26 12:20:24 UTC
Holder		
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 2019
Extensions		
keyUsage (2.5.29.15)	Purpose	digitalSignature
extKeyUsage (2.5.29.37)	Extended intended use	timeStamping
basicConstraints (2.5.29.19)	Restrictions regarding use of the certificate	Type applicant=End Entity Restriction path length=None
subjectKeyIdentifier (2.5.29.14)	Public key identifier of the holder	[DB 5E EA 40 0B D2 8C F8 76 30 53 B6 52 0F 14 66 85 90 D3 6F]
ValidityModel (1.3.6.1.4.1.8301.3.5)	Certificate extension for validity model during certificate verification	ValidityModelChain (1.3.6.1.4.1.8301.3.5.1)

authorityKeyIdentifier (2.5.29.35)	Issuer public key identifier	[C4 A0 FE 6F E8 D7 E0 84 80 E7 30 35 D7 A6 27 5E EC 5F 1A 02]
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)	Certification Policy TSA of the CA of the BNotK	CPS: https://zertifizierungsstelle.bnotk.de/veroeffentlichungen
qcStatements (1.3.6.1.5.5.7.1.3)	Declaration of eIDAS compliance	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. seal)	0.4.0.1862.1.6.2
QcPDS (0.4.0.1862.1.5)	URL reference to PDS	https://zertifizierungsstelle.bnotk.de/veroeffentlichungen

- 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. [58 ac b6 41 e3 98 90 00]
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	C = DE
organizationName (2.5.4.10)	Name organisation	O = German Federal Chamber of Notaries
organizationIdentifier	Identification organisation	2.5.4.97 = DE122788238

(2.5.4.97)		
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	e.g. 2019-06-27 12:20:24 UTC
	End	e.g. 2029-03-26 12:20:24 UTC
Holder		
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 2019
Extensions		
keyUsage (2.5.29.15)	Purpose	digitalSignature
extKeyUsage (2.5.29.37)	Extended purpose	timeStamping
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	[DB 5E EA 40 0B D2 8C F8 76 30 53 B6 52 0F 14 66 85 90 D3 6F]
ValidityModel (1.3.6.1.4.1.8301.3.5)	Certificate extension for validity model during certificate verification	ValidityModelChain (1.3.6.1.4.1.8301.3.5.1)
authorityKeyIdentifier (2.5.29.35)	Issuer public key identifier	[C4 A0 FE 6F E8 D7 E0 84 80 E7 30 35 D7 A6 27 5E EC 5F 1A 02]
authorityInfoAccess	Reference to issuer and	see following elements

(1.3.6.1.5.5.7.1.1)	service for status inquiry	
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)	Certification Policy TSA of the CA of the BNotK	CPS: https://zertifizierungsstelle.bnotk.de/veroeffentlichungen
qcStatements (1.3.6.1.5.5.7.1.3)	Declaration of eIDAS compliance	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. seal)	0.4.0.1862.1.6.2
QcPDS (0.4.0.1862.1.5)	URL reference to PDS	https://zertifizierungsstelle.bnotk.de/veroeffentlichungen

Time-stamps issued by the TSP comply with RFC 3161

***

https://zertifizierungsstelle.bnotk.de/