

PKI Disclosure Statement of the Certification Authority of the German Federal Chamber of Notaries for qualified electronic time-stamps

Version

2.6

Date

29 January 2024

Document history

| Version | Remarks | Date |
|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| 1.0 | Preparation of the document in the course of the assessment of compliance with the requirements set out in the Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EG (eIDAS Regulation) by an accredited conformity assessment body | 20/06/2017 |
| 1.1 | Editorial changes in preparation of the publication of the English version of this document | 27/07/2017 |
| 2.0 | Update due to the conversion of the PKI-infrastructure of the Certification Authority of the German Federal Chamber of Notaries to a native eIDAS-PKI as well as editorial changes following the entry into force of the Act on Trust Services | 16/02/2018 |
| 2.1 | Editorial changes | 31/05/2018 |
| 2.2 | Editorial changes | 27/05/2019 |
| 2.3 | Editorial changes and updating | 02/06/2021 |
| 2.4 | Editorial changes and updating | 30/05/2022 |
| 2.5 | Editorial changes and updating | 16/03/2023 |
| 2.6 | Editorial changes and adjustment of OID labelling | 29/01/2024 |

Name and identification of the document

Document name: Public Disclosure Statement from the Certification Authority of the German Federal Chamber of Notaries for qualified electronic time-stamps

Qualification (OID): 1.3.6.1.4.1.41460.5.3.1.2.2

Version: 2.6

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

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

Content

| | | |
|------|-----------------------------------------------------|-------------------------------------------|
| 1. | Contact information | 5 |
| 1.1. | General contact information | 5 |
| 1.2. | Revocation of time-stamps | 5 |
| 2. | Qualified trust service | 5 |
| 2.1. | Type of qualified trust service | 5 |
| 2.2. | Restrictions of qualified time-stamps | 6 |
| 2.3. | Retention period | 6 |
| 2.4. | Time accuracy | 6 |
| 2.5. | Verification of the qualified time-stamp | 6 |
| 2.6. | Availability of the time-stamp service | 6 |
| 3. | User obligations of the time-stamping service | 7 |
| 4. | General information | 7 |
| 4.1. | Applicable agreements | 7 |
| 4.2. | Exclusion of liability | 7 |
| 4.3. | Data protection concept | 7 |
| 4.4. | Withdrawal | Fehler! Textmarke nicht definiert. |
| 4.5. | Dispute resolution procedure | 7 |
| 4.6. | Applicable law | 7 |
| 4.7. | Publications and directories | 7 |

1. Contact information

1.1. General contact information

Zertifizierungsstelle der Bundesnotarkammer
 Burgmauer 53
 50667 Köln

Tel.: +49 (2 21) 27 79 35-0

Fax: +49 (2 21) 27 79 35-20

Email: zs@bnotk.de

1.2. Revocation of time-stamps

It is not possible to revoke time-stamps.

2. Qualified trust service

2.1. Type of qualified trust service

| Trust service | Applicable directives | Relevant OID |
|----------------------------------|--------------------------------------------------------------------------------------------------------------|-------------------------------|
| Qualified electronic time-stamps | ▶ Certificate Policy of the Certification Authority of the German Federal Chamber of Notaries | ▶ 1.3.6.1.4.1.41460.5.1.1.1.2 |
| | ▶ TSA Policy and Practice Statement of the Certification Authority of the German Federal Chamber of Notaries | ▶ 1.3.6.1.4.1.41460.5.4.1.1.2 |
| | ▶ ETSI-EN 319 421 | |

The TSP has a conformity assessment for the trust service by a recognized conformity assessment body (TÜV Informationstechnik GmbH), which confirms compliance with the requirements set out in the eIDAS Regulation and the ETSI-EN 319 421 standards.

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

According to current knowledge (as of January 2024), the algorithm used is valid until further notice.

Please note that the TSP does not directly provide qualified electronic time-stamps for end users. In selected individual cases, qualified electronic time-stamps or time-stamping services are made available to third parties who may make these available for end users. In this case, the third party is responsible for giving information to end users and for ensuring that they fulfil their obligations.

2.2. Restrictions of qualified time-stamps

The statutory provisions apply.

2.3. Retention period

The TSP archives documents in accordance with statutory requirements. The following applies specifically to the time-stamping service: all events concerning the life cycle of (i) the TSU key and of (ii) the TSU certificate (if required) are logged.

2.4. Time accuracy

As a reliable time source, time servers with a DFC77 receiver are used to receive the legally valid time from the Physikalisch-Technische Bundesanstalt. In case of temporary signal loss, a high-precision oscillator takes over the task of the timer for the NTP server. Additional NTP servers of the institute are included as an additional reference source. The average maximum deviation of the time is +/- 100 ms and is in no case greater than one second.

2.5. Verification of the qualified time-stamp

The holder of the time-stamp and relying third parties shall only rely on a time-stamp issued by the TSP 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 until the time-stamp's verification date,
- ▶ possible restrictions of the use have been observed,
- ▶ all further agreements and other precautionary measures have been observed,
- ▶ the relying third party has used the relevant trusted list to verify that the time-stamp and the time-stamp unit (**TSU**) are qualified.

2.6. 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 applies.

3. User obligations of the time-stamping service

The statutory provisions apply.

Please note that the TSP in principle doesn't provide qualified electronic time-stamps for end users.

4. General information

4.1. Applicable agreements

The individual contractual agreement concluded with the TSP applies or, if there is no contractual agreement, the statutory provisions apply.

4.2. Exclusion of liability

The statutory provisions apply.

4.3. Data protection concept

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

4.4. Revocation

The declaration of intent to conclude a contract for the purchase of TSP certification services cannot be revoked.

4.5. Dispute resolution procedure

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

4.6. Applicable law

German law shall apply unless foreign law is mandatory.

4.7. Publications and directories

The public certificates based on the keys are published on the website of the TSP at the following link: <https://zertifizierungsstelle.bnotk.de/veroeffentlichungen>.

They are also published on the website of the Federal Network Agency (Bundesnetzagentur, BNetzA) and on the German trusted list.

You can access the BNetzA's trusted list via <https://www.elektronische-vertrauensdienste.de/EVD/DE/Home/start.html> or the EU Commission's new website at <https://eidas.ec.europa.eu/efda/home/#/screen/home>.

<https://zertifizierungsstelle.bnotk.de/>