

Certificate



The certification body of TÜV Informationstechnik GmbH hereby awards this certificate to the company

**Bundesnotarkammer
Mohrenstraße 34
10117 Berlin, Germany**

Certificate validity:
2023-06-23 – 2025-06-23

to confirm that its trust service

BNotK qualifizierte Zertifikate für elektronische Signaturen

fulfils all relevant requirements defined in regulation

Reg. (EU) No. 910/2014 (eIDAS) for creation of qualified certificates for electronic signatures.

The appendix to the certificate is part of the certificate with the ID 97215.23 and consists of 3 pages.

Essen, 2023-06-23

Dr. Christoph Sutter, Head of Certification Body



Certification Scheme

The certification body of TÜV Informationstechnik GmbH is accredited by “DAkkS Deutsche Akkreditierungsstelle GmbH” according to EN ISO/IEC 17065 for the scopes IT security and security technology product certification and according to eIDAS. The certification body performs its certification on the basis of the following accredited certification scheme:

- “Certification Scheme eIDAS (accredited scope) of the certification body of TÜV Informationstechnik GmbH”, version 2.1 as of 2023-01-30, TÜV Informationstechnik GmbH

Conformity Assessment Report

- German document: “Konformitätsbewertungsbericht TUVIT.97215.TSP.06.2023, BNotK qualifizierte Zertifikate für elektronische Signaturen” as of 2023-06-23, TÜV Informationstechnik GmbH

Conformity Assessment Requirements

The conformity assessment requirements are defined in eIDAS:

- Regulation (EU) No. 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

for the following trust service:

- creation of qualified certificates for electronic signatures

Conformity Assessment Target

The target of conformity assessment is characterized by the certificate information of the inspected trust service:

BNotK qualifizierte Zertifikate für elektronische Signaturen

**Issuer of CA certificate (Root CA or Intermediate CA): CN = BNotK EC Root CA 2020
Certificate Serial Number: 78A38912C9704C46**

Name of CA (as in certificate)	serial number of certificate
CN = BNotK EC qSig CA 2020	268A5832C0773226
CN = BNotK EC rqSig CA 2020	1AE778AE2245FC0D

**Issuer of CA certificate (Root CA or Intermediate CA): CN = BNotK EC Root CA 2021
Certificate Serial Number: 14F6C08492B782E3279A672D7437165DE0173BDF**

Name of CA (as in certificate)	serial number of certificate
CN = BNotK EC qSig CA 2021	6279FA1CBE2DCA251DB23C7EBC69B7978A919C4F
CN = BNotK EC rqSig CA 2021	765F29FC6FB388D716E36F55FBFCC84325AC5ECE

**Issuer of CA certificate (Root CA or Intermediate CA): CN = BNotK Root CA 2017
Certificate Serial Number: 1451C65D97BAFDFD**

Name of CA (as in certificate)	serial number of certificate
CN = BNotK qSig CA 2017	5C30476DF7A5753C
CN = BNotK rqSig CA 2020	2274FB49ADE0EAF0

**Issuer of CA certificate (Root CA or Intermediate CA): CN = BNotK Root CA 2021
Certificate Serial Number: OCD284126A21E8A1301CD925C89A33D0EBAD3082**

Name of CA (as in certificate)	serial number of certificate
CN = BNotK qSig CA 2021	2874C5550ED7767556EB3704BF3C2BE1111BC2C7
CN = BNotK rqSig CA 2021	72CFA7FADA7EFC4FAC585EB17151D4BDCF1B79BF

together with the documentation of the operator:

- Zertifikatsrichtlinie der Zertifizierungsstelle der Bundesnotarkammer, version 1.6, valid from 2023-03-16, Bundesnotarkammer
- Zertifizierungskonzept der Zertifizierungsstelle der Bundesnotarkammer für qualifizierte Zertifikate, version 3.2 as of 2023-06-06, Bundesnotarkammer
- PKI Disclosure Statement der Zertifizierungsstelle der Bundesnotarkammer für qualifizierte Zertifikate, version 2.6, valid from 2023-02-02, Bundesnotarkammer
- ALLGEMEINE GESCHÄFTSBEDINGUNGEN DER ZERTIFIZIERUNGSSTELLE DER BUNDESNOTARKAMMER, version , valid from 2022-04-25, Bundesnotarkammer

Conformity Assessment Result

- The target of conformity assessment fulfills all applicable conformity assessment requirements.
- The certification requirements defined in the certification scheme are fulfilled.

Summary of the Conformity Assessment Requirements

The eIDAS contains the following general requirements for the trust service:

- 1 Data processing and protection**
Requirements from eIDAS, Article 5
- 2 Liability and burden of proof**
Requirements from eIDAS, Article 13 para. 2, 3
- 3 Accessibility for persons with disabilities**
Requirements from eIDAS, Article 15
- 4 Security requirements applicable to trust service providers**
Requirements from eIDAS, Article 19, para. 1, 2
- 5 Supervision of qualified trust service providers**
Requirements from eIDAS, Article 20 para. 1
- 6 Requirements for qualified trust service providers**
Requirements from eIDAS, Article 24, Para. 1 a), b), para. 2 a), b), c), d), e), f), g), h), i), j), k), para 3, para.4
- 7 Requirements for creation of qualified certificates for electronic signatures**
Requirements from eIDAS, Article 28, para. 1, 2, 3, 4, Article 29, para. 1, 2