PKI Disclosure Statement of the certification body BVtrust of Bank-Verlag GmbH for qualified seal certificates (BVseal)

1. Preamble

Bank-Verlag is a qualified trust service provider within the meaning of Art. 21 (2) of Regulation (EU) No. 910/2014.

The service offered includes:

- the issuance of qualified seal certificates for legal persons
- the issuance of qualified electronic seals within the meaning of Regulation (EU) No. 910/2014.

2. Document Name

Document name: PKI Disclosure Statement of the certification body BVtrust of Bank-Verlag GmbH for qualified seal certificates (BVseal)

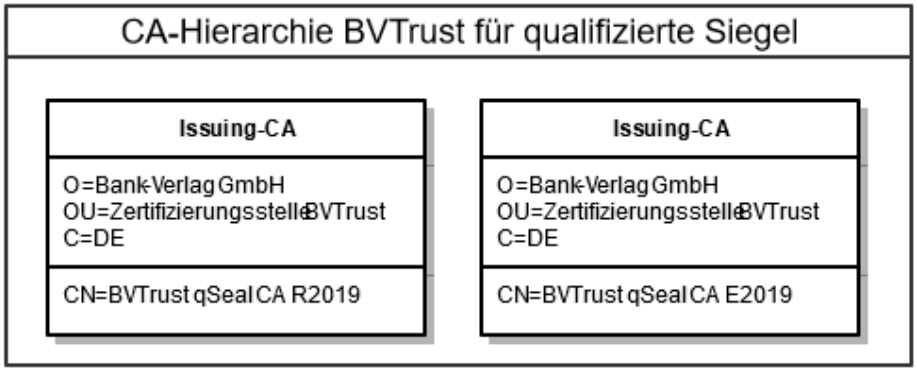
Version: Version 15 am 2020-12-18

3. Contact the TSP

Bank-Verlag GmbH
Wendelinstraße 1
50933 Köln
E-Mail: bvtrust@bank-verlag.de
Phone: +49 221 5490 724

4. Certificate types, validation processes and key types

The PKI service includes the issuance of certificates for qualified seals. The certificates of the issuing CAs are included in the Trusted List of the respective national supervisory body. Two CA certificates are created, each with an RSA and ECDSA key.



The certificate management process, which includes the issuance and revocation of all certificate types, the validation process and key uses are detailed in the Certificate Policy (CP) and Certification Practice Statement (CPS). The currently valid documents as well as all previous versions are available on the Internet: https://www.bank-verlag.de/bvtrust-bvseal.

In the event of termination of the service, the information will also be published at the address named above.

5. Definition of the confidence interval

The confidence interval is defined in the respective CP and CPS. All relevant events from the application, the registration process, the validation process, the issuance, the activation up to the possible revocation of the certificates are recorded by the TSP. A certificate renewal is not offered, instead every application must be processed as a new registration.

6. Obligation of the end user

The obligations of the end user (here also: subject, legal person) or the certificate holder (here also: subscriber, authorized representative of the legal person) are listed in the purchase agreement/ framework agreement and attachments for acquiring a qualified seal. The valid documents are handed over to the end user in the procurement process.

7. Obligation of the trusted third party and certificate validation

Relying third parties must themselves have sufficient information and knowledge to be able to evaluate the handling of certificates and their validation. The relying third party itself is responsible for deciding whether the information provided is reliable and trustworthy. Each reyling third party should therefore

- verify the accuracy of the information contained in the certificate before using it
- verify the validity of the certificate by validating the entire certificate chain up to the trust anchor, which is listed as such in the national trusted list (certification hierarchy), as well as checking the validity period and the status and revocation information of the certificate,
- use the certificate only for authorised and legal purposes in accordance with the corresponding CP/CPS, as Bank-Verlag is not responsible for assessing the suitability of a certificate for a particular purpose,
- check the technical uses defined by the attributes 'key usage' and 'extended key usage' specified in the certificate. Accordingly, relying third parties must use appropriate software and/or hardware to validate certificates and related cryptographic procedures.

8. Disclaimer, limitations of liability

Liability limitations are defined in the respective CP and CPS and are regulated in individual contracts. The TSP is not liable for damages caused by the use of certificates which are not used accordingly and compliantly to legal requirements or to contractually regulated framework conditions.
The TSP is not liable for damages caused by improper or incorrect use of certificates.

9. Applicable and contractual agreements

The following documents can be downloaded at https://www.bank-verlag.de/bvtrust-bvseal

- PKI Disclosure Statement (PDS),
- Certificate Policy (CP) and Certification Practice Statement (CPS)

The current version of the respective documents as well as all previous versions including the validity period of the document can be accessed. The TSP and enduser (subject) shall adhere to the contractually agreed upon framework conditions.

10. Availability of the service

The service infrastructure includes:

- seal infrastructure
- CA infrastructure,
- Status information service via OCSP
- self-service, which enables a certificate retrieval and revocation by the end user or his authorized representative

All components are operated with high availability and redundancy in the data centers of Bank-Verlag GmbH and can be reached 24x7.

11. Privacy policy

The privacy policy of the service is listed in the sales contract / framework agreement and attachments for acquiring a qualified seal. The valid documents are handed over to the certificate holder (here also: authorized representatives of the legal entity) in the procurement process.

12. Reimbursement

A reimbursement is not provided.

13. Applicable law, complaints and dispute resolution

German law shall apply and the place of jurisdiction shall be Cologne. If an end user or relying third party wishes to contact the TSP, the contact data in chapter 3 can be used.

14. Auditing

The trust service provider shall have a valid conformity assessment, which has been carried out by a recognised conformity assessment body, certifying compliance with the requirements. The covered areas of the assessment are available under 8.4. of the respective CP under the link https://www.bank-verlag.de/bvtrust-bvseal.

In addition to the documentation, the implementation of the processes and compliance with the specifications are checked.

The national trusted list is available on the internet at https://tl.bundesnetzagentur.de/TL-DE.xml and the corresponding SHA-companion-file at https://tl.bundesnetzagentur.de/TL-DE.sha2.