

# PKI Disclosure Statement of the certification body BVtrust of Bank-Verlag GmbH for qualified website certificates as part of the second Payment Services Directive (PSD2)

## 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 website certificates under the second Payment Services Directive (PSD2 regulation).

## 2. Contact the TSP

Bank-Verlag GmbH  
Wendelinstraße 1  
50933 Köln

E-Mail: [bvtrust@bank-verlag.de](mailto:bvtrust@bank-verlag.de)  
Phone: +49 221 5490 724

## 3. Certificate types, validation processes and key types

The PKI service includes the issuance of website certificates within the framework of the PSD2 regulation. The certificates of the issuing CAs are included in the Trusted List of the respective national supervisory authority. A CA certificate with an RSA key pair is available.

CA Hierarchy BVtrust for qualified website certificates within the framework of the PSD2 regulation
Issuing-CA
O=Bank-Verlag GmbH OU=BVtrust C=DE
CN=BVtrust PSD2 QWAC CA R2019

The certificate management process, which includes the issuance, renewal 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-psd2-qwac>

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

## 4. 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 production, 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.

## 5. Obligation of the end user

The obligations of the end users and subscribers are contractually regulated and have to be fulfilled taking into account the respective CP and CPS.

## 6. Obligation of the trusted third party and certificate validation

Confiding third parties must themselves have sufficient information and knowledge to be able to evaluate the handling of certificates and their validation. The trusted third party itself is responsible for deciding whether the information provided is reliable and trustworthy. Each trusted 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 (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, trusted third parties must use appropriate software and/or hardware to validate certificates and related cryptographic procedures.

## 7. 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.

## 8. Applicable and contractual agreements

The following documents can be downloaded at <https://www.bank-verlag.de/bvtrust-psd2-qwac>

- 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, end user and subscriber shall adhere to the contractually agreed upon framework conditions.

## 9. Availability of the service

The infrastructure of the service includes:

- CA infrastructure,
- Status information service via OCSP

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

## 10. Privacy policy

A service-specific privacy policy is not available. The privacy policy of the Bank-Verlag applies, which is available at <https://www.bank-verlag.de/index.php?id=25>

## 11. Reimbursement

A reimbursement is not provided.

## 12. Applicable law, complaints and dispute resolution

German law shall apply and the place of jurisdiction shall be Cologne.

If an end user, subscriber or trusted third party wishes to contact the TSP, the contact data in chapter 2 can be used.

## 13. 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-psd2-qwac> .

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