bank-verlag Das Service-Unternehmen der privaten Banken

Bank-Verlag GmbH

Terms of use

BVsign – qualified electronic signatures

Version: 1.30

Date: 07.04.2022

Status: Final

Table of contents

1. General

1.1 Scope of application

Bank-Verlag GmbH is a trust service provider ("TSP") qualified by the Federal Network Agency as the competent supervisory body in accordance with 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 ("eIDAS Regulation"). The basis of the approval is a conformity assessment by a conformity assessment body in accordance with Article 3 number 18 of the eIDAS Regulation.As part of the conformity assessment, the trust service to be provided as a service and the Bank-Verlag as provider are audited in advance and at regular intervals.

The following terms of use apply to the registration for the creation of a qualified electronic certificate and for the creation of remote signatures (BVsign trust services).

1.2 Legal basis

The TSP provides the trust services for the user based on the

- eIDAS Regulation of 23 July 2014 ("eIDAS Regulation") and
- Trust Services Act ("VDG") of 18 July 2017 and
- Trust Services Ordinance ("VDV") of 15 February 2019.

1.3 Definitions

Term	Abbreviation	Definition
BVSign		Name of product from TSP Bank-Verlag which summarized all trust center activities for issuing qualified signatures under eIDAS Regulation
BVtrust		Name of service from TSP Bank-Verlag which summarized all qualified trust center activities (under the eIDAS Regulation). Designation is here also displayed as a certification authority
Certificate authority	CA	The certification authority generates and issues the public key certificates, The TSP (remote signatures) generates and stores the cryptographic keys (here: based on a remote signature) and provides the signature generation on behalf of the signatory.
Certificate Subscriber		Holder of the qualified certificate
Certificate Policy	CP	Certificate policy of the trust services operated by the TSP. Represents, among other things, the requirements and specifications for the public key infrastructure operated by the certification authority

Certification Practice Statement	CPS	(Technical) Certificate concept describing the solutions by the TSP to fulfil the requirements defined in the CP
Conformity assessment		Auditing of a TSP and its offered trust service by an accredited Conformity Assessment Body according Regulation (EU) No 910/2014.
Conformity Assessment Body		Private organization ("accredited body "), as defined in eIDAS Article 3 (18) who performs the audits / conformity assessments required in eIDAS Art. 20 (1) (and Art. 21 (1)).
eIDAS Regulation		Regulation of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. As a regulation, it has a direct effect on the national legislation of the European member states
End User		User who has a certificate and has sole control to issue his signature
End provider		Third party (e.g., bank) that offers its business transaction via its own IT application
Federal Network Agency		Competent national supervisory body for qualified trust service providers (“TSP”) in Germany in accordance with eIDAS Regulation
Hash Value		A hash value is the cryptographic checksum for ensuring the integrity of data that is created when a qualified electronic signature is generated and signed with the end user's private key
Identification		The establishment of identity is the prerequisite for the creation of a qualified certificate by the TSP. According to Article 24, Clause 1 of the eIDAS Regulation, this can be done: • by personal presence (e.g. on site at the TSP or by PostIdent), • remotely by means of electronic identification (e.g. with the eID function of the personal identity card), • by a certificate of a qualified electronic signature or

		• by other identification procedures recognised at national level (e.g. VideoIdent). In addition, according to §11 (4) VDG, the TSP can also use data that has already been collected at an earlier point in time as part of a proper identification process (e.g. when opening an account at a bank).
Online Certificate Status Protocol	OCSP	Describes a technical protocol for retrieving status information on a qualified electronic certificate. The URL of the service is specified in the certificates. The TSP provides a status query service via the OCSP protocol
Personal identification number	PIN	Sequence of digits known only to the certificate subscriber and with which the person can authenticate himself to a machine.
PKI Disclosure Statement	PDS	PKI Disclosure Statement of the certification authority, in particular on the infrastructure, for the issuance of qualified certificates and signatures
Public Key Infrastructure		Technical infrastructure of the TSP for generating and managing cryptographic public and private keys
Qualified Electronic Signature Creation Device	QSCD	A qualified and approved Device according to eIDAS Regulation. A QSCD is used to securely generate, store and use cryptographic keys as defined in eIDAS Regulation.
Qualified electonic signature	QES	Signature generated using a qualified certificate and a QSCD
Qualified electronic certificate		Data record according eIDAS, Annex I that describes a natural person (e.g., first name, surname, e-mail address), which is based on an identification that was carried out in a legally prescribed procedure. This data record is inextricably linked to a key pair (public & private key) during registration. Each certificate has a validity period specified by the TSP
Registration		Registration refers to the assignment of a key pair to an end user after successful authentication by the TSP. The TSP confirms the affiliation of the private key to the end user with a certificate. Each certificate has a validity period determined by the TSP

Remote Signature		A remote signature refers to the use of the end user's private key from the secure operating environment of the TSP. The end user can initiate a remote signature by using a 2-factor authentication procedure ("2FA procedure")
Revoke		Once a certificate has been revoked, it can no longer be used for signing
Signature		Data in electronic form (e.g., certificate) that is attached to or logically associated with other electronic data (document hash value) and that the end user uses to electronically sign a digital content (e.g., electronic documents). The signature is linked to the signed data in this way, so that even a subsequent change to the data can be detected
Terms of Use	TOS	Conditions for using the BVSign service, including registration and identification of end users in connection with the issuance of qualified certificates and remote signature creation
Transaction number	TAN	One-time password or string of digits tied to a specific process (transaction) and (usually) to a person. By entering the TAN, the person can confirm a release
Trust Service Provider	TSP	Provider with technical infrastructure offering (qualified) trust services according to the eIDAS Regulation (here: Bank Verlag GmbH)
Trust Services Act	VDG	This law regulates the effective national implementation of the regulations on trust services and is a national addition to the eIDAS Regulation.
Trust Services Ordinance	VDV	This ordinance regulates qualified trust service providers and is a national addition to the eIDAS Regulation.
Two-Factor-Authentification	2FA	Proof of user authentication using a combination of two different and in particular, independent components (factors): As a rule, these are possession (e.g., mobile phone number),knowledge (e.g., TAN or PIN) and inherence (e.g. facial biometrics)

1.4 Changes to the terms of use

In the event of changes to the terms of use, the TSP is entitled to revoke certificates that refer to the previously applicable terms of use. A new registration is then required for renewed use, in the context of which the end user gives his consent to the amended terms of use.

2. Trust services

2.1 Creation of an End User Certificate

The end user confirms the correctness of the data collected during registration. The TSP generates a key pair for the end user and confirms that the keys belong to the end user by issuing a qualified certificate.

The TSP stores the private key of the end user certificate in a secure environment and ensures that it can only be used under the sole control of the end user.

2.2 Creation of remote signatures

The end user can sign a provided document by means of a remote signature via an online portal (web-based and/or mobile) or another suitable IT application of a third party ("end provider"). For this purpose, the end user authenticates the use of his private key by the TSP by means of a 2-factor procedure (e.g., by entering a TAN). After checking the TAN, the end provider transmits the hash value of the document to be signed to the TSP. After verifying the transmitted data, the TSP signs the hash value with the user's private key and transfers the signature of the hash value to the end provider.

The end user observes the security requirements/duties of care agreed in connection with the use of the authentication procedure with regard to the handling of the means of authentication. The end user must ensure that the authentication features used (e.g., password, TAN) and the associated authentication media, such as a mobile phone, are stored securely, not passed on to third parties and only used as intended for the process of authenticating the end user.

2.3 Provision of the End User Certificate

The TSP reserves the right to publish end user certificates. Furthermore, the end user has the possibility to obtain his personal certificate via the website

https://www.bank-verlag.de/bvsign

by providing their e-mail address.

2.4 Revocation of the End User Certificate

The end user is obliged to revoke his certificate if

- the details do not or no longer correspond to the facts, or
- there is a reasonable suspicion of unauthorised third-party access to the identification or authentication data (e.g., PIN/TAN).

If an end user wishes to submit a revocation request, this must be

- via the end provider or
- via a one-time link on the TSP revocation page.

If the revocation request is submitted via the end provider, the end user informs the end provider of the certificate to be revoked, which triggers the revocation process via BVsign. If this is not possible or desired, an end user can contact the TSP directly. For this purpose, the TSP offers an electronic revocation request on its website at

https://www.bank-verlag.de/bvsign

By entering the e-mail address provided during registration, the end user can initiate the revocation process using a one-time link. If an authenticated revocation request is submitted, the TSP is obliged to revoke the End User certificate.

2.5 Publication of the End User Certificate

By agreeing to these Terms of Use, the end user consents to the publication of the Certificate.

2.6 Provision of content

Provision of content (e.g., for signature visualisation) is carried out by the end user or the end provider used.

2.7 Further information

Details on the type and scope of the BVsign trust service (e.g., Certificate Policy or “CP”), PKI Disclosure Statement or “PDS”, TSP Certification Practice Statement or “CPS”) of the CA services offered under the name BVtrust can be found at

https://www.bank-verlag.de/bvtrust

and are integral part of these Terms of Use.

3. Obligations of the TSP

3.1 End User identification

The TSP issues the end user certificate exclusively based on the data collected in conformity with the eIDAS Regulation.

3.2 Status request service

The TSP provides a status query service via the OCSP protocol. The URL of the service is specified in the certificates. The status request service is operated 24/7.

Further details on the design of the status query service can be found in the certificate concept (CPS).

The TSP ensures that the end user or authorised third parties can revoke a certificate issued by the TSP. A revoked certificate cannot be reactivated.

A certificate can be revoked if

- the certificate holder / end user orders this,
- the end provider or an authorised third party (e.g., the Federal Network Agency as the responsible supervisory authority) initiates this,
- the TSP becomes aware of fraud in the use of the certificate,
- the TSP discontinues the operation of the trust service,
- procedures used in connection with the provision of the trust services are no longer considered sufficiently secure, and
- legal requirements make this necessary.

If a revocation is not initiated by the end user, the end user must be informed of the revocation process by the TSP or the bank. Further details on the design of the revocation service can be found in the certificate concept (“CPS”).

4. Terms of contract

These terms of use shall be deemed to be agreed for the period of validity of the end user certificate. Any revocation of the end user certificate shall lead to termination of the contractual relationship.

5. Data protection

In order to provide the trust services, the TSP processes personal data of the end user. Details on the handling of personal data can be found at

https://www.bank-verlag.de/bvsign

The data protection declaration also contains information on the rights and complaint options of the end user.

6. Contact

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

7. Final provisions

7.1 Applicable law

German law shall apply to the exclusion of the UN Convention on Contracts for the International Sale of Goods.

7.2 Place of jurisdiction

The place of jurisdiction for all legal disputes is the general place of jurisdiction of the end user. Any exclusive place of jurisdiction shall remain unaffected by this provision.

7.3 Place of fulfillment

Place of fulfilment for TSP and end user is Cologne.