

PKI Disclosure Statement der Zertifizierungsstelle BVtrust der Bank-Verlag GmbH für fortgeschrittene Zertifikate (BVsign AdES)

1. Einleitung

Der Bank-Verlag ist qualifizierter Vertrauensdiensteanbieter i.S.d Art. 21 Abs. 2 der VO (EU) Nr. 910/2014.

Angebotene Dienste, die dem Dienst unterliegen, sind:

- die Ausgabe von fortgeschrittenen Zertifikaten für elektronische Signaturen für natürliche Personen sowie
- das Ausstellen von Fernsignaturen i.S.d. der VO (EU) Nr. 910/2014.

2. Name des Dokuments

Dokumentenname: PKI Disclosure Statement der Zertifizierungsstelle BVtrust der Bank-Verlag GmbH für fortgeschrittene Zertifikate (BVsign AdES)

Version: Version 1 am 2022-08-17

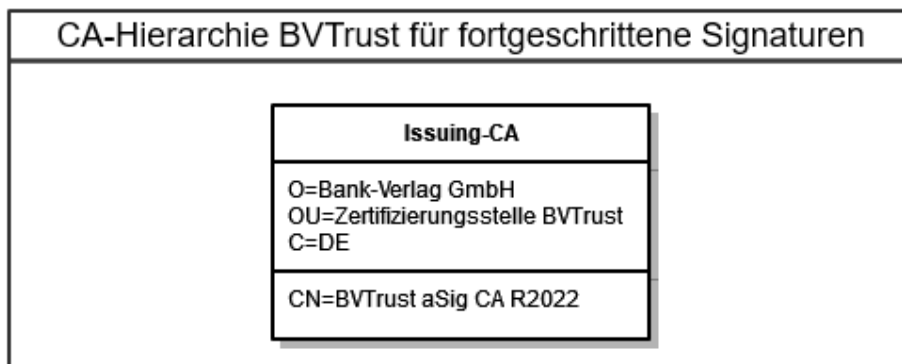
3. Kontakte des TSP

Bank-Verlag GmbH
Wendelinstraße 1
50933 Köln

E-Mail: bvtrust@bank-verlag.de
Telefonnummer: +49 221 5490 724

4. Zertifikatstypen, Validierungsprozesse und Schlüsseltypen

Die PKI-Dienstleistung umfasst die Ausstellung von Zertifikaten für fortgeschrittene Signaturen. Diese ist in einer 1-Tier Hierarchie aufgebaut. Es wird nicht zwischen Root-CA und Issuing-CA unterschieden.



Der Zertifikatsverwaltungsprozess, der die Ausstellung und Widerruf aller Zertifikatstypen umfasst, der Validierungsprozess sowie Schlüsselverwendungen sind ausführlich in den Zertifizierungsrichtlinien (Certificate Policy, CP) und Erklärungen zum Zertifizierungsbetrieb (CertificationPractice Statement, CPS) dargestellt.

Die aktuell gültigen Dokumente sowie alle bisherigen Versionen sind im Internet unter:

<https://www.bank-verlag.de/bvtrust-bvsign>

auffindbar. Im Falle einer Beendigung des Dienstes werden die Informationen diesbezüglich ebenfalls unter o.g. Adresse veröffentlicht.

5. Abgrenzung des Vertrauensbereichs

Der Vertrauensbereich ist in der jeweiligen CP und CPS abgegrenzt. Es werden alle relevanten Ereignisse von der Antragstellung, über den Registrierungsprozess, die Prüfungen des TSPs, die Produktion, die Aktivierung bis hin zum etwaigen Widerruf der Zertifikate vom TSP erfasst. Eine Zertifikaterneuerung ist nicht vorgesehen, sondern muss als erneute Registrierung durchgeführt werden.

6. Verpflichtung des Endanwenders

Die Verpflichtungen der Endanwender sind im Dokument „Nutzungsbedingungen *BVsign AdES – fortgeschrittene Signaturen*“ aufgeführt. Das aktuell gültige Dokument als auch alle bisherigen Versionen sind im Internet unter <https://www.bank-verlag.de/bvtrust-bvsign> abrufbar.

7. Verpflichtung der vertrauenden Drittpartei und Zertifikatsvalidierung

Vertrauende Dritte müssen selbst über hinreichende Informationen und Kenntnisse verfügen, um den Umgang mit Zertifikaten und dessen Validierung bewerten zu können. Der Vertrauende Dritte ist selbst für seine Entscheidungsfindung verantwortlich, ob die zur Verfügung gestellten Informationen zuverlässig und vertrauensvoll sind. Jeder Vertrauende Dritte sollte daher

- vor der Nutzung des Zertifikats die darin angegebenen Informationen auf Richtigkeit überprüfen,
- die Gültigkeit des Zertifikats überprüfen, in dem er unter anderem die gesamte Zertifikatskette bis zum Wurzelzertifikat, welches in der nationalen Trusted-List als solches aufgeführt ist, validiert (Zertifizierungshierarchie) sowie den Gültigkeitszeitraum und die Statusinformationen des Zertifikats überprüft,
- das Zertifikat ausschließlich für autorisierte und legale Zwecke in Übereinstimmung mit der vorliegenden CP/CPS einsetzen. Der Bank-Verlag ist nicht für die Bewertung der Eignung eines Zertifikats für einen bestimmten Zweck verantwortlich,
- die technischen Verwendungszwecke prüfen, die durch die im Zertifikat angegebenen Attribute „Schlüsselverwendung“ und „erweiterte Schlüsselverwendung“ festgelegt sind. Vertrauende Dritte müssen geeignete Software und/oder Hardware zur Überprüfung von Zertifikaten (Validierung) und den damit verbundenen kryptografischen Verfahren verwenden.

8. Haftungsausschluss, Haftungsbeschränkungen

Haftungsbeschränkungen werden in der jeweiligen CP und CPS definiert und werden einzelvertraglich geregelt. Sollte sich die Nutzung von Zertifikaten nicht innerhalb der gesetzlichen Vorgaben bewegen oder gegen die vertraglich geregelten Rahmenbedingungen verstoßen, so haftet der TSP nicht für die daraus resultierenden Schäden. Der TSP haftet nicht für Schäden, die durch unsachgemäße oder fehlerhafte Nutzung von Zertifikaten entstehen.

9. Anwendbare und vertragliche Vereinbarungen

Im Internet sind unter dem Link <https://www.bank-verlag.de/bvtrust-bvsign> folgende Dokumente abrufbar:

- PKI-Offenlegungspflichten (PKI Disclosure Statement (PDS)),
- Nutzungsbedingungen
- Datenschutzerklärung
- Certificate Policy (CP) und Certification Practice Statement (CPS)

Dabei ist die aktuelle Fassung der jeweiligen Dokumente sowie alle Vorläuferversionen inklusive des Gültigkeitszeitraums des Dokumentes abrufbar. Für den TSP, Endanwender (Zertifikatnehmer) gelten die vertraglich vereinbarten Bedingungen.

10. Verfügbarkeit des Dienstes

Die Infrastruktur des Dienstes umfasst:

- Signaturinfrastruktur
- CA-Infrastruktur
- Verzeichnisdienst für Statusinformationen über OCSP
- Self-Service, der einen Zertifikatsabruf und Widerruf durch den Endanwender ermöglicht.

Alle Komponenten werden in den Rechenzentren der Bank-Verlag GmbH hochverfügbar betrieben und sind 24/7 erreichbar.

11. Datenschutzrichtlinie

Die Datenschutzerklärung des Dienstes ist einsehbar unter www.bank-verlag.de/bvtrust-bvsign

12. Kostenerstattung

Eine Kostenerstattung ist nicht vorgesehen.

13. Anwendbares Recht, Beschwerden und Streitbeilegung

Es gilt deutsches Recht und der Gerichtsstand ist Köln. Möchte ein Endanwender (Zertifikatnehmer) oder Vertrauender Dritter mit dem TSP Kontakt aufnehmen, so kann er dafür die Kontaktinformationen aus Kapitel 2 verwenden.

14. Auditierung

Der Vertrauensdiensteanbieter verfügt über die Konformitätsbewertung durch eine anerkannte Konformitätsbewertungsstelle, die die Einhaltung der Anforderungen bestätigt. Die abgedeckten Bereiche der Prüfung sind unter 8.4. der jeweiligen CP unter dem Link <https://www.bank-verlag.de/bvtrust-bvsign> abrufbar.

Neben der Dokumentation werden die Umsetzung der Prozesse sowie die Einhaltung der Vorgaben überprüft.