PKI Disclosure Statement der Zertifizierungsstelle BVtrust der Bank-Verlag GmbH für qualifizierte Websitezertifikate im Rahmen der zweiten Zahlungsdiensterichtlinie (PSD2-VO)

1. Einleitung

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

Der angebotene Dienst umfasst:

- die Ausgabe von qualifizierten Website-Zertifikaten im Rahmen der zweiten Zahlungsdiensterichtlinie (PSD2-VO).

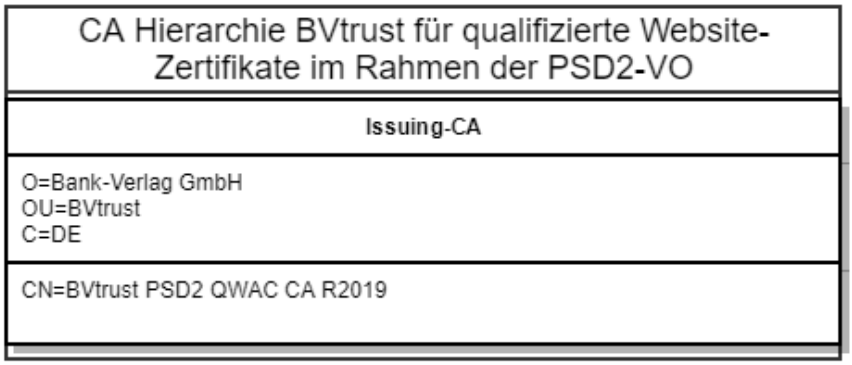
2. Kontakte des TSP

Bank-Verlag GmbH
Wendelinstraße 1
50933 Köln

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

3. Zertifikatstypen, Validierungsprozesse und Schlüsseltypen

Die PKI-Dienstleistung umfasst die Ausstellung von Website-Zertifikaten im Rahmen der PSD2-VO. Die Zertifikate der ausstellenden CAs werden in die Trusted List der entsprechenden nationalen Aufsichtsbehörde aufgenommen. Es ist ein CA-Zertifikat mit einem RSA Schlüsselpaar verfügbar.



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

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

https://www.bank-verlag.de/bvtrust-psd2-qwac

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

4. 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 Zertifikatserneuerung ist nicht vorgesehen, sondern muss als erneute Registrierung durchgeführt werden.

5. Verpflichtung des Endanwenders

Die Verpflichtungen der Endanwender und Zertifikatnehmer sind vertraglich geregelt und unter Berücksichtigung der jeweiligen CP und CPS zu erfüllen.

6. 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, indem er unter anderem die gesamte Zertifikatskette bis zum Vertrauensanker 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, da der Bank-Verlag nicht für die Bewertung der Eignung eines Zertifikats für einen bestimmten Zweck verantwortlich ist,
- die technischen Verwendungszwecke prüfen, die durch die im Zertifikat angegebenen Attribute „Schlüsselverwendung“ und „erweiterte Schlüsselverwendung“ festgelegt sind. Es muss dementsprechend geeignete Software und/oder Hardware zur Überprüfung von Zertifikaten (Validierung) und den damit verbundenen kryptografischen Verfahren verwendet werden.

7. 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.

8. Anwendbare und vertragliche Vereinbarungen

Im Internet sind unter dem Link https://www.bank-verlag.de/bvtrust-psd2-qwac folgende Dokumente abrufbar:

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

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

9. Verfügbarkeit des Dienstes

Die Infrastruktur des Dienstes umfasst:

- CA-Infrastruktur,
- Statusinformationsdienst über OCSP

Alle Komponenten werden in den Rechenzentren der Bank-Verlag GmbH hochverfügbar und redundant betrieben und sind 24x7 erreichbar.

10. Datenschutzrichtlinie

Eine dienstspezifische Datenschutzerklärung ist nicht verfügbar. Es gilt die Datenschutzerklärung des Bank-Verlags, welche unter https://www.bank-verlag.de/index.php?id=25 einsehbar ist.

11. Kostenerstattung

Eine Kostenerstattung ist nicht vorgesehen.

12. 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.

13. 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-psd2-qwac abrufbar.

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