Zertifikatsrichtlinie (Certificate Policy) der Zertifizierungsstelle BVtrust der Bank-Verlag GmbH für qualifizierte Siegelzertifikate im Rahmen der zweiten Zahlungsdiensterichtlinie (PSD2-VO)

1. Einleitung (Introduction)

Dieses Dokument beschreibt die Zertifikatsrichtlinie der von der Bank-Verlag GmbH betriebenen Vertrauensdienste, welche unter dem Namen BVtrust angeboten werden, in Form einer Certificate Policy (im Folgenden CP genannt) und stellt die Anforderungen und Vorgaben für die von der Zertifizierungsstelle BVtrust betriebenen Public-Key-Infrastruktur (PKI) dar.

Die Gliederung des Dokuments basiert auf dem Standard RFC 3647, um einen Vergleich mit den CPs anderer Vertrauensanbieter zu erleichtern.

Maßgeblich ist allein die deutsche Fassung der CP. Bei Abweichung zwischen der deutschen und der englischen Fassung dieses Dokuments gilt daher ausschließlich die deutsche Fassung.

Das zu dieser Zertifikatsrichtlinie zugehörige Zertifkatskonzept ist unter der OID mit der Kennzeichnung: 1.3.6.1.4.1.50833.1.3.1 aufgeführt.

1.1. Überblick (Overview)

Der Vertrauensdiensteanbieter (Trust Service Provider, im Folgenden TSP genannt) ist die

Bank-Verlag GmbH
Wendelinstr. 1
50933 Köln.

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

Der TSP verfügt über die Konformitätsbewertung durch eine anerkannte Konformitätsbewertungsstelle, die die Einhaltung der in der VO (EU) Nr. 910 /2014, VDG und VDV sowie den Normen ETSI EN 319 401, ETSI EN 319 411-1 und ETSI EN 319 411-2 festgelegten Anforderungen bestätigt.

Die Regelungen der PKI sind in dem zum Zertifikat gehörenden Zertifikatskonzept (Certification Practice Statement, im Folgenden CPS genannt) beschrieben. Der TSP bietet unter dieser Policy diverse Produkte an, die die Anforderungen aus dieser CP in ihren speziellen Produkteigenschaften erfüllen. Die Erfüllung dieser Anforderungen wird in einem CPS beschrieben, welches zu einem Produkt oder einer Produktgruppe zugeordnet werden kann. Diese Zuordnung erfolgt über einen eindeutigen policyIdentifier in Form einer eindeutigen OID, die in jedem Zertifikat die Zugehörigkeit zu einer spezifischen CP enthält. Weiterhin befindet sich in jedem Zertifikat ein policyQualifier in Form einer URI, unter welchem die zum Zertifikat zugehörigen CP und CPS abgerufen werden können. Die URL, unter denen die jeweiligen CP bzw. CPS zu finden sind, lautet https://www.bank-verlag.de/bvtrust.

Zertifikate, die im Rahmen dieses Dienstes vom TSP ausgegeben werden, unterliegen immer der Zertifizierung im Sinne der eIDAS-VO, PSD2-VO, VDG, VDV, ETSI EN 319 401, ETSI EN 319 411-1, ETSI EN 319 411-2 und ETSI TS 119 495.

Das TSP-Management stellt sicher, dass die Anforderungen und Vorgaben innerhalb des TSP umgesetzt werden.

Der TSP kann Teilaufgaben an Partner oder externe Anbieter auslagern.

1.2. Name und Kennung des Dokuments (Document name and identification)

Dokumentenname: Zertifikatsrichtlinie (Certificate Policy) der Zertifizierungsstelle BVtrust der Bank-Verlag GmbH für qualifizierte Siegelzertifikate im Rahmen der zweiten Zahlungsdiensterichtlinie (PSD2-VO)

Kennzeichnung (OID): 1.3.6.1.4.1.50833.1.3.2

Stand: Version 32 am 2019-08-02

1.3. PKI-Beteiligte (PKI participants)

1.3.1. Zertifizierungsstellen (Certification authorities)

Die Zertifizierungsstelle (auch Certificate Authority – kurz CA) stellt Zertifikate aus und erteilt Auskünfte zu deren Status.

1.3.2. Registrierungsstellen (Registration authorities)

Die Registrierungsstelle (auch Registration Authority, kurz RA) identifiziert und authentifiziert die Zertifikatnehmer und Endanwender, durch Mitarbeiter in der Rolle Validation Specialist, die Teil der Registrierungsstelle sind, und erfasst und prüft Anträge, die von einem vertretungsberechtigten Zertifikatnehmer für den Endanwender gestellt werden, auf Erbringung von Vertrauensdienstleistungen durch die CA. Die Identifizierung von Zertifikatnehmern wird von der identity Trust Management AG durchgeführt. Anträge auf Widerrufung der von der CA ausgegebenen Zertifikate werden ebenfalls von der Registrierungsstelle erfasst, geprüft und an die CA weitergeleitet.

Die Regelungen sind in dem jeweils zum Zertifikat zugehörigen Zertifizierungskonzept bzw. CPS beschrieben.

1.3.3. Zertifikatnehmer und Endanwender (Subscribers/End Entity)

Zertifikatnehmer (auch Antragsteller oder Subscriber nach ETSI EN 319 411-1) sind vertretungsberechtigte, natürliche Personen, die den Antrag für den Endanwender stellen, der die von der Zertifizierungsstelle ausgegebenen Zertifikate innehat.

Endanwender (auch Subject oder End Entity, kurz EE) sind Zertifikatinhaber und verwenden die ausgegebenen Zertifikate. Endanwender sind hierbei die Eigentümer des privaten Schlüssels des jeweils zugehörigen Zertifikats. Ferner kann der TSP Einschränkungen in der Nutzung und Ausstellung von Zertifikaten an Endanwender stellen. Der Endanwender ist immer eine juristische Person.

Die Regelungen sind in dem jeweils zum Zertifikat zugehörigen Zertifizierungskonzept bzw. CPS beschrieben.

1.3.4. Vertrauende Dritte (Relying parties)

Vertrauende Dritte (auch Relying Party) sind natürliche oder juristische Personen oder sonstige Dritte (z.B. Systeme), die sich auf die Vertrauenswürdigkeit der von dem TSP ausgegebenen Zertifikate verlassen.

1.3.5. Andere Teilnehmer (Other participants)

Andere Teilnehmer sind Dritte, auf die die Zertifizierungsstelle Funktionen und/oder Aufgaben übertragen hat.

Die Regelungen der Funktionen und/oder Aufgaben sind, sofern vorhanden, in dem zum Zertifikat gehörenden CPS beschrieben.

1.4. Zertifikatsverwendung (Certificate usage)

1.4.1. Zulässige Verwendung von Zertifikaten (Appropriate certificate uses)

Zertifikate, die dieser CP unterliegen, können im Allgemeinen für alle Zwecke verwendet werden. Der Zertifikatnehmer ist dafür verantwortlich, Zertifikate so zu verwenden, dass die Verwendung den anwendbaren gesetzlichen Bestimmungen entspricht.

Weitere Regelungen sind in dem jeweils zum Zertifikat zugehörigen Zertifizierungskonzept bzw. CPS beschrieben.

1.4.2. Unzulässige Verwendung von Zertifikaten (Prohibited certificate uses)

Die Verwendung von Zertifikaten für Dienste und Systeme, die bei Störungen oder Ausfällen zu großen materiellen oder immateriellen Schäden führen sowie Schäden an Leib oder Leben verursachen können, ist nicht gestattet.

Hierzu zählen Atomkraftwerke, Chemieproduktionsanlagen oder Luftfahrtsysteme.

Hiervon abweichende Regelungen können im Einzelnen mit dem TSP schriftlich vereinbart werden.

Weitere Regelungen sind in dem jeweils zum Zertifikat zugehörigen Zertifizierungskonzept bzw. CPS beschrieben.

1.5. Verwaltung der Zertifikatsrichtlinie (Policy administration)

1.5.1. Zuständigkeit für dieses Dokument (Organization administering the document)

Diese CP wird durch das TSP-Management der Bank-Verlag GmbH verwaltet.

1.5.2. Kontaktinformationen (Contact person)

Eine Kontaktaufnahme kann über folgende Adressen erfolgen:

Bank-Verlag GmbH
Security and Trusted Services
Wendelinstr. 1
50933 Köln

Tel: +49 221 5490 724

E-Mail: bvtrust@bank-verlag.de

Certificate Problem Reports können über folgende E-Mail-Adresse eingereicht werden: psd2-problems@bank-verlag.de

1.5.3. Pflege der Richtlinie

Diese CP behält Gültigkeit, solange sie nicht von der zuständigen Instanz widerrufen wird. Sie wird bei Bedarf fortgeschrieben und erhält dann jeweils eine neue aufsteigende Versionsnummer.

1.5.4. Genehmigungsverfahren dieses Dokuments

Der in Kapitel 1.5.1 benannte Herausgeber ist für dieses Dokument (CP) verantwortlich. Die Freigabe erfolgt durch das TSP-Management und das Dokument wird unmittelbar nach der Freigabe auf der Webseite des TSP als aktuelle Version veröffentlicht. Alle vorangegangenen Versionen werden in ein Archiv verschoben und sind weiterhin verfügbar. Vergangene Versionen werden nicht gelöscht.

Relevante Änderungsanforderungen oder Änderungen des laufenden PKI-Betriebs werden rechtzeitig fachlich bewertet, überprüft und eingearbeitet.

1.6. Akronyme und Definitionen(Definitions and acronyms)

Begriff	Beschreibung
CA	Certificate Authority
CP	Certificate Policy
CPS	Certification Practice Statement
DSGVO	Datenschutz-Grundverordnung
EE	End Entity - Endanwender oder Subject
LDAP	Lightweight Directory Access Protocol
MaRisk	Mindestanforderungen an das Risikomanagement
PKI	Public-Key-Infrastruktur
RA	Registration Authority
TSP	Trust Service Provider
VA	Validation Authority

2. Veröffentlichungen und Verzeichnisdienste (PUBLICATION AND REPOSITORY RESPONSIBILITIES)

2.1. Verzeichnisdienste (Repositories)

Alle CA-Zertifikate des TSP sind auf den Webseiten der Bank-Verlag GmbH veröffentlicht und können dort abgefragt werden.

Weitere Details sind ggf. in dem jeweils zum Zertifikat zugehörigen Zertifizierungskonzept bzw. CPS beschrieben.

2.2. Veröffentlichung von Zertifikatsinformationen (Publication of certification information)

Die Regelungen sind in dem jeweils zum Zertifikat zugehörigen Zertifizierungskonzept bzw. CPS beschrieben.

2.3. Zeitpunkt und Häufigkeit von Veröffentlichungen (Time or frequency of publication)

Diese CP, die jeweiligen Zertifikatskonzepte bzw. CPS und PDS sowie die Zertifikate der Konformitätsbewertungen werden stets in der aktuell gültigen Version veröffentlicht und sind auf der Website des TSP unter folgenden Link veröffentlicht: https://www.bank-verlag.de/bvtrust

Im Falle der Aktualisierung werden die neuen Fassungen unverzüglich durch die TSP-Leitung veröffentlicht. Alte Fassungen aller dort veröffentlichten Dokumente bleiben ebenfalls in einem separaten Archivbereich abrufbar. Die Gültigkeit von CP und CPS bezieht sich auf den Erstellungszeitpunkt des jeweiligen ausgestellten Zertifikats und wird im Normalfall nicht durch neue Versionen von CP und CPS beeinträchtigt. Der TSP hält sich das Recht vor, bei Änderungen von CP und CPS diese auch für existierende Zertifikatnehmer und Endanwender zu erzwingen. In dem Fall werden alle betroffenen Zertifikate widerrufen und alle Endanwender, unter Zuhilfenahme der Registrierungsdaten, über diese Änderung informiert. Die Endanwender müssen sich erneut registrieren.

Statusinformationen zu ausgegebenen Zertifikaten sind via OCSP unverzüglich, spätestens jedoch nach einer Stunde, verfügbar.

2.4. Zugang auf Verzeichnisdienste (Access controls on repositories)

CA-Zertifikate, CP, CPS und PDS können öffentlich und unentgeltlich abgerufen werden. Es gibt keine Zugriffsbeschränkungen für lesenden Zugriff. Es wird kein Verzeichnisdienst für Endteilnehmerzertifikate angeboten. Änderungen der Webinhalte werden ausschließlich vom TSP vorgenommen. Der TSP stellt sicher, dass der Zugriff jederzeit möglich ist. Störungen des Zugriffs werden unverzüglich behoben.

Weitere, nicht öffentliche Dokumente, können bei begründetem Interesse auf Nachfrage in den relevanten Teilen ausgegeben werden.

3. Identifizierung und Authentifizierung (IDENTIFICATION AND AUTHENTICATION)

Die Identifizierung und Authentifizierung der Zertifikatnehmer und Endanwender entsprechen den gesetzlichen Vorgaben und richtet sich nach produkt- und kundenspezifischen Anforderungen sowie den Anforderungen der entsprechenden Zertifizierung (eIDAS-VO, PSD2-VO, VDG, VDV, ETSI EN 319 401, ETSI EN 319 411-1, ETSI EN 319 411-2 und ETSI TS 119 495).

Einzelheiten zu den Vorgängen sind in dem jeweils zum Zertifikat zugehörigen Zertifizierungskonzept bzw. CPS in Abschnitt 3 beschrieben.

4. Betriebsanforderungen (CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS)

Die Betriebsanforderungen für Zertifikate des TSP entsprechen den gesetzlichen Vorgaben und richtet sich nach produkt- und kundenspezifischen Anforderungen sowie den Anforderungen der entsprechenden Zertifizierung (eIDAS-VO, PSD2-VO, VDG, VDV, ETSI EN 319 401, ETSI EN 319 411-1, ETSI EN 319 411-2 und ETSI TS 119 495).

Die Funktionalität aller Systeme, die sich auf diese CP beziehen, muss Barrierefreiheit gewährleisten, soweit dies möglich ist. Um Menschen mit Behinderungen zu unterstützen, müssen folgende Umsetzungskriterien bei Kontaktaufnahme, vorrangig im Rahmen der Internet-Präsenz, unterstützt werden:

- Verwendung von maschinenlesbaren Texten
- Skalierbare Darstellung
- Verwendung von „leichter Sprache", sofern dies möglich ist
- Gliederung weniger Ebenen sowie ein klar abgegrenzter Navigationsbereich
- Verwendung von klaren Kontrasten

Weitere Einzelheiten zu den Betriebsanforderungen sind in dem jeweils zum Zertifikat zugehörigen Zertifizierungskonzept bzw. CPS in Abschnitt 4 beschrieben.

5. Nicht-technische Sicherheitsmaßnahmen (FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS)

Der TSP hat gemäß den gesetzlichen Anforderungen sowie gemäß den Anforderungen aus eIDAS-VO, PSD2-VO, VDG, VDV, ETSI EN 319 401, ETSI EN 319 411-1, ETSI EN 319 411-2 und ETSI TS 119 495 entsprechende nicht-technische Sicherheitsmaßnahmen eingeführt.

Einzelheiten sind in dem jeweils zum Zertifikat zugehörigen Zertifizierungskonzept bzw. CPS beschrieben.

6. Technische Sicherheitsmaßnahmen (TECHNICAL SECURITY CONTROLS)

Der TSP hat gemäß den gesetzlichen Anforderungen sowie gemäß den Anforderungen aus eIDAS-VO, PSD2-VO, VDG, VDV, ETSI EN 319 401, ETSI EN 319 411-1, ETSI EN 319 411-2 und ETSI TS 119 495 entsprechende technische Sicherheitsmaßnahmen eingeführt.

Einzelheiten sind in dem jeweils zum Zertifikat zugehörigen Zertifizierungskonzept bzw. CPS beschrieben.

7. Zertifikats-, Widerruflisten- und OCSP-Profile (CERTIFICATE, CRL, AND OCSP PROFILES)

7.1. Zertifikatsprofil (Certificate profile)

Die von den CAs des TSP ausgestellten Zertifikate erfüllen die Anforderungen der Standards ITU X.509, IETF RFC 5280, IETF RFC 6818 sowie der ETSI EN 319 412 des SOG-IS Kataloges.

Die Details sind in dem jeweils zum Zertifikat zugehörigen Zertifizierungskonzept bzw. CPS beschrieben.

Der TSP veröffentlicht auf der Website des TSP Testzertifikate aller Arten von Zertifikaten, die der TSP ausstellt, um Dritten die Möglichkeit zu bieten, die ausgestellten Zertifikate zu prüfen und zu testen.

7.2. Widerruflistenprofil (CRL profile)

Es werden keine öffentlichen Widerrufslisten angeboten.

7.3. OCSP-Profil (OCSP profile)

Der Statusabfragedienst ist konform zum Standard IETF RFC 6960.

Die Profile werden in dem jeweils zum Zertifikat zugehörigen Zertifizierungskonzept bzw. CPS beschrieben.

8. Konformitätsprüfung (COMPLIANCE AUDIT AND OTHER ASSESSMENTS)

Der TSP betreibt den Vertrauensdienst im Einklang mit dem geltenden Recht. Einzelheiten sind in den folgenden Abschnitten beschrieben.

8.1. Intervall oder Gründe von Prüfungen (Frequency or circumstances of assessment)

Eine akkreditierte Konformitätsbewertungsstelle überprüft in regelmäßigen Abständen, dass der TSP die gesetzlichen Anforderungen erfüllt. Es finden regelmäßige Wiederholungsprüfungen statt. Außerdem erfolgen anlassbezogene Prüfungen, so z.B. bei der Durchführung von sicherheitsrelevanten Änderungen an den Arbeitsprozessen des TSP.

8.2. Identität/Qualifikation des Prüfers (Identity/qualifications of assessor)

Die TSP-spezifischen Konformitätsprüfungen werden von qualifizierten Dritten (z.B. von qualifizierten Unternehmen wie SRC Security Research & Consulting GmbH) durchgeführt, die Erfahrung in den Bereichen PKI-Technologie, Sicherheits-Auditing und Verfahren sowie Hilfsmittel der Informationssicherheit vorweisen können.

8.3. Beziehung des Prüfers zur prüfenden Stelle (Assessor's relationship to assessed entity)

Beim Prüfer für die Konformitätsprüfung handelt es sich um einen unabhängigen und qualifizierten Auditor.

Selbstaufsichtsmaßnahmen (Quality Assessments) werden von dafür qualifizierten Bank-Verlag-Mitarbeitern durchgeführt.

8.4. Abgedeckte Bereiche der Prüfung (Topics covered by assessment)

Zielsetzung der Überprüfung ist die Umsetzung der gesamten zum Vertrauensdienst gehörenden Dokumentation sowie die Umsetzung der beschriebenen Prozesse. Es sind alle Prozesse zu prüfen, die mit der Lebenszyklusverwaltung von Zertifikaten in Verbindung stehen:

- Identitätsprüfungen der Zertifikatnehmer und Endanwender
- Zertifikatsbeantragungsverfahren
- Bearbeitung von Zertifikatsanträgen
- Re-Zertifizierungen
- Zertifikatswiderrufungen
- Zutrittsschutz
- Berechtigungs- und Rollenkonzept
- Einbruchshemmende Maßnahmen
- Personal

In jedem Fall wird nach den jeweils gültigen Versionen der Audit-Kriterien nach PSD2-VO, eIDAS-VO, MaRisk (Mindestanforderungen an das Risikomanagement), VDG, VDV, DSGVO, ETSI TS 119 495, ETSI EN 319 401, ETSI EN 319 411-1 und ETSI EN 319 411-2 geprüft.

8.5. Maßnahmen zur Mängelbeseitigung (Actions taken as a result of deficiency)

Werden bei einer Konformitätsprüfung von einem Prüfer schwerwiegende Mängel oder Fehler bei dem Betreiber der Zertifizierungsstelle festgestellt, wird darüber entschieden, welche Korrekturmaßnahmen zu treffen sind. Der Leiter des Trust Centers entscheidet zusammen mit dem Prüfer über geeignete Maßnahmen, deren Umsetzung in einem wirtschaftlich angemessenen Zeitraum durchzuführen sind. Bei schweren sicherheitskritischen Mängeln muss innerhalb von 48 Stunden ein Korrekturplan erstellt und die Abweichung behoben werden. Bei weniger schwerwiegenden Defiziten entscheidet der Leiter des Trust Centers über den Zeitrahmen der Behebung.

8.6. Mitteilung der Ergebnisse (Communication of results)

Die Ergebnisse der Konformitätsprüfung werden in einem vom Prüfer erstellten Bericht dokumentiert und der Bank-Verlag GmbH übergeben. Die Bank-Verlag GmbH behält es sich vor, Ergebnisse bzw. Teilergebnisse zu veröffentlichen, wenn Missbrauch stattfand oder bei Schädigung des Ansehens der Bank-Verlag GmbH.

Das Zertifikat der Konformitätsbestätigung wird auf der Internetseite der Bank-Verlag GmbH unter https://www.bank-verlag.de/bvtrust veröffentlicht.

9. Sonstige geschäftliche und rechtliche Bestimmungen (OTHER BUSINESS AND LEGAL MATTERS)

9.1. Gebühren (Fees)

9.1.1. Gebühren für die Ausstellung oder Erneuerung von Zertifikaten (Certificate issuance or renewal fees)

Die Gebühren für die Ausgabe und den Erhalt eines Zertifikats richten sich nach der mit dem Endanwender, der durch den Zertifikatnehmer vertreten wird, geschlossenen Vereinbarung.

9.1.2. Gebühren für den Zugriff auf Zertifikate (Certificate access fees)

Es werden keine Gebühren für den Zugriff auf Zertifikate erhoben.

9.1.3. Gebühren für den Zugriff auf Widerrufs- oder Statusinformationen (Revocation or status information access fees)

Für die Abfrage von Widerrufs- und Statusinformationen werden keine Gebühren erhoben.

9.1.4. Gebühren für andere Leistungen (Fees for other services)

Soweit andere Dienstleistungen angeboten werden, richten sich die Gebühren nach den vertraglichen Vereinbarungen mit dem Endanwender, der durch den Zertifikatnehmer vertreten wird.

9.1.5. Gebührenerstattung (Refund policy)

Es gelten die Vereinbarungen mit dem Endanwender, der durch den Zertifikatnehmer vertreten wird.

9.2. Finanzielle Verantwortlichkeit (Financial responsibility)

9.2.1. Versicherungsdeckung (Insurance coverage)

Der TSP verfügt über die notwendigen Mittel, um den Betrieb von Vertrauensdiensten ordnungsgemäß durchzuführen. Die notwendigen Mittel werden unter anderem durch die Erhebung der Gebühren für die Bereitstellung und Nutzung der Vertrauensdienste des TSP erzielt.

9.2.2. Andere Ressourcen für Betriebserhaltung und Schadensdeckung (Other assets)

Keine Angaben.

9.2.3. Versicherungs- oder Gewährleistungsschutz für Endnutzer (Insurance or warranty coverage for end-entities)

Der TSP verfügt über eine angemessene Deckungssumme bzw. Haftpflichtversicherung gemäß Vertrauensdienstegesetz und Vertrauensdiensteverordnung.

9.3. Vertraulichkeit von Geschäftsinformationen (Confidentiality of business information)

9.3.1. Definition von vertraulichen Informationen (Scope of confidential information)

Die Vertraulichkeit von Informationen kann vereinbart werden, sofern sie nicht bereits durch geltendes Recht definiert ist.

9.3.2. Definition von nicht vertraulichen Informationen (Information not within the scope of confidential information)

Als öffentlich gelten alle Informationen in ausgestellten und veröffentlichten Zertifikaten sowie die unter Abschnitt 2.2 genannten Daten.

9.3.3. Verantwortung zum Schutz vertraulicher Informationen (Responsibility to protect confidential information)

Der TSP kann im Einzelfall verpflichtet werden, die ihm als vertrauliche Geschäftsdaten benannten Daten durch entsprechende technische und organisatorische Maßnahmen gegen Preisgabe und Ausspähung zu schützen, und hat zu unterlassen, dass diese Daten zweckentfremdet genutzt werden oder diese Daten Drittpersonen offengelegt werden, soweit eine solche Verpflichtung nicht gegen das Gesetz verstößt. Im Rahmen der organisatorischen Maßnahmen werden die vom TSP eingesetzten Mitarbeiter in dem gesetzlich zulässigen Rahmen zur Geheimhaltung der vertraulichen Daten verpflichtet.

9.4. Schutz von personenbezogenen Daten (Datenschutz) (Privacy of personal information)

9.4.1. Datenschutzkonzept (Privacy plan)

Der TSP verarbeitet personenbezogene Daten im Einklang mit den gesetzlichen Bestimmungen. Die Datenschutzerklärung kann unter www.bank-verlag.de/bvtrust eingesehen werden.

9.4.2. Definition von personenbezogenen Daten (Information treated as private)

Personenbezogene Daten sind gemäß Art. 4 Abs. 1 Nr. 1 DSGVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.

9.4.3. Nicht vertrauliche Daten (Information not deemed private)

Alle Informationen und Daten, die in den von dem TSP ausgegebenen Zertifikaten und in den in Abschnitt 2 genannten Dokumenten und Diensten enthalten sind oder daraus abgeleitet werden können, werden als nicht vertrauliche Daten behandelt.

9.4.4. Verantwortung für den Schutz personenbezogener Daten (Responsibility to protect private information)

Die Verantwortung für den Schutz der personenbezogenen Daten trägt der TSP.

Der Datenschutzbeauftragte des TSP achtet auf die Einhaltung der gesetzlichen Bestimmungen zum Datenschutz. Er erarbeitet Datenschutzrichtlinien, steht als Ansprechpartner in Datenschutzfragen zur Verfügung und verpflichtet Mitarbeiter des TSP oder mit dem TSP in vertraglicher Verbindung stehende Dritte mit Zugriff auf personenbezogene Daten zur Beachtung der Datenschutzrichtlinien.

9.4.5. Hinweis und Einwilligung zur Nutzung personenbezogener Daten (Notice and consent to use private information)

Bei der Antragstellung werden personenbezogene Daten des Zertifikatnehmers im Rahmen des Identifikationsverfahrens erhoben und verarbeitet. Der Zertifikatnehmer stimmt im Rahmen der Antragstellung der Nutzung seiner personenbezogenen Daten zwecks Identifizierung und Authentifizierung zu. Eine Datenerhebung bei Dritten erfolgt nur bei Vorliegen einer Einwilligung des Zertifikatnehmers.

9.4.6. Erteilung von Auskünften im Rahmen von Gerichts- oder Verwaltungsverfahren (Disclosure pursuant to judicial or administrative process)

Der TSP unterliegt dem Recht der Bundesrepublik Deutschland sowie den Bestimmungen des BDSG und der DSGVO. Auskünfte über vertrauliche oder personenbezogene Daten werden den ermittelnden Behörden herausgegeben, sofern ein Gerichtsbeschluss vorliegt oder sonstige gesetzlichen Bestimmungen eine Herausgabe erfordern.

9.4.7. Andere Bedingungen zur Offenlegung von Daten (Other information disclosure circumstances)

Auskünfte anderer Art als unter Abschnitt 9.4.6 beschrieben werden nicht erteilt.

9.5. Urheberrecht (Intellectual property rights)

Keine Angaben.

9.6. Zusicherungen, Garantien und Gewährleistungen (Representations and warranties)

Der TSP gewährleistet, sichert zu und garantiert, dass der in der CP und CPS beschriebene Dienst in Übereinstimmung mit der Dokumentation betrieben wird.

Zusätzlich zu den Angaben in CP und CPS sind für Zertifikatnehmer, Endanwender, Vertrauende Dritte sowie alle anderen Personen die gesetzlichen Bestimmungen bzw. die jeweiligen einzelvertraglichen Vereinbarungen maßgeblich.

9.7. Haftungsausschluss (Disclaimers of warranties)

Ein Haftungsausschluss ist einzelvertraglich geregelt.

Der TSP haftet nicht für Schäden, die durch Nutzung von Zertifikaten entstehen, die nicht im Rahmen der gesetzlichen Vorgaben oder der vertraglich geregelten Rahmenbedingungen verwendet werden.

Der TSP haftet nicht für Schäden, die durch unsachgemäße oder fehlerhafte Nutzung von Zertifikaten entstehen.

9.8. Haftungsbeschränkungen (Limitations of liability)

Die Haftungsbeschränkungen richten sich nach den gesetzlichen Vorgaben und werden einzelvertraglich geregelt.

9.9. Schadenersatz (Indemnities)

Es gelten die gesetzlichen Bestimmungen und die jeweiligen einzelvertraglichen Vereinbarungen.

9.10. Laufzeit und Beendigung (Term and termination)

9.10.1. Gültigkeitsdauer der Zertifikatsrichtlinie (Term)

Diese CP gilt ab dem Zeitpunkt der Veröffentlichung und bleibt wirksam bis zum Ablauf des letzten unter dieser CP ausgestellten Zertifikats. Es gilt jeweils die Version der CP, die zum Zeitpunkt der Antragstellung veröffentlicht ist.

9.10.2. Beendigung des Betriebs (Termination)

Für den Fall, dass der TSP den Betrieb einstellt, liegt ein Beendigungsplan vor, der regelmäßig auf Aktualität überprüft wird.

9.10.3. Auswirkung der Beendigung (Effect of termination and survival)

Ist absehbar, dass der komplette Betrieb des TSP oder Teile davon eingestellt werden, so wird diese Beendigung gemäß dem Beendigungplan des TSP durchgeführt. Der TSP hat zu prüfen, ob eine Übernahme des jeweiligen Dienstes durch einen anderen qualifizierten Vertrauensdiensteanbieter möglich ist. In dem Fall werden alle vom TSP ausgegebenen Zertifikate für den zu beendenden Dienst an den neuen Vertrauensdiensteanbieter übergeben.

Ist eine Übernahme des Dienstes durch einen TSP ausgeschlossen, so werden alle vom TSP ausgegebenen Zertifikate und Widerrufsinformationen für den zu beendenden Dienst in elektronischer Form an die Bundesnetzagentur zur Übernahme in die Vertrauensinfrastruktur übergeben. Alle zu diesem Dienst zugehörigen Endanwenderzertifikate werden vor der Übergabe an die Bundesnetzagentur oder einen anderen VDA widerrufen und der dienstspezifische private CA-Schlüssel wird vernichtet, sodass keine neuen Zertifikate ausgestellt werden können. Gegebenenfalls sind weitere Schritte mit der jeweiligen Aufsichtsbehörde abzustimmen.

In jedem Fall werden Endanwender mithilfe der aus der Registrierung hinterlegten Kontaktdaten per E-Mail über diese Beendigung informiert. Der TSP stellt Informationen zur Beendigung auf seiner Website frei zugänglich zur Verfügung. Auch wird der Endanwender über mögliche Folgen, Konsequenzen und Widerrufsmöglichkeiten unterrichtet.

Weitere Details zu dieser Beschreibung können in dem jeweils zum Zertifikat zugehörigen Zertifizierungskonzept bzw. CPS in Kapitel 4.11 beschrieben sein.

Weitere Einzelheiten zum Beendigungsplan können bei begründetem Interesse auf Nachfrage in den relevanten Teilen ausgegeben werden.

9.11. Individuelle Mitteilungen und Kommunikation mit Teilnehmern (Individual notices and communications with participants)

Mitteilungen des TSP an Zertifikatnehmer werden an die letzte in den Unterlagen vom TSP verzeichnete Anschrift oder der entsprechenden hinterlegten E-Mail-Adresse (elektronisch signiert) versendet.

Möchte ein Zertifikatnehmer oder eine andere vertretungsberechtigte Person des Endanwenders Kontakt zum TSP aufnehmen oder eine Beschwerde einreichen, so kann er die Kontaktinformationen aus 1.5.2 zur Kontaktaufnahme verwenden.

9.12. Änderung der Zertifikatsrichtlinie (Amendments)

9.12.1. Verfahren für Änderungen (Procedure for amendment)

Veränderungen und Nachträge zu dieser CP werden in diesem Dokument eingearbeitet und unter demselben OID veröffentlicht.

9.12.2. Benachrichtigungsverfahren und -fristen (Notification mechanism and period)

Keine Angaben.

9.12.3. Bedingungen für OID-Änderungen (Circumstances under which OID must be changed)

Keine Angaben.

9.13. Streitschlichtungsverfahren (Dispute resolution provisions)

Beschwerden können schriftlich (Bank-Verlag GmbH, Wendelinstr. 1, 50933 Köln) oder via E-Mail (service-desk@bank-verlag.de) bei dem TSP eingereicht werden.

9.14. Anwendbares Recht (Governing law)

Es gilt deutsches Recht und der Gerichtsstand ist Köln.

9.15. Einhaltung geltenden Rechts (Compliance with applicable law)

Der jeweilige Zertifikatnehmer ist dafür verantwortlich, dass die von dem TSP ausgegebenen Zertifikate im Einklang mit den gesetzlichen Bestimmungen verwendet werden.

9.16. Sonstige Bestimmungen (Miscellaneous provisions)

9.16.1. Vollständigkeitserklärung (Entire agreement)

Folgende Dokumente sind Gegenstand der geltenden Vereinbarungen, an denen PKI-Teilnehmer beteiligt sind:

- Vertrags- und Antragsunterlagen,
- die zum Zeitpunkt der Antragstellung gültige CP, CPS und PDS.

9.16.2. Abgrenzungen (Assignment)

Keine Angaben.

9.16.3. Salvatorische Klausel (Severability)

Durch etwaige Unwirksamkeit einer oder mehrerer Bestimmungen dieser CP wird die Wirksamkeit der übrigen Bestimmungen nicht berührt.

9.16.4. Vollstreckung (Rechtsanwaltsgebühren und Rechtsverzicht) (Enforcement (attorneys' fees and waiver of rights))

Es gelten die etwaigen jeweiligen Vereinbarungen.

9.16.5. Höhere Gewalt (Force Majeure)

Es gelten die etwaigen jeweiligen Vereinbarungen.

9.17. Andere Bestimmungen (Other provisions)

Keine Angaben.