Zertifikatskonzept (Certification Practice Statement) der Zertifizierungsstelle BVtrust der Bank-Verlag GmbH für qualifizierte Websitezertifikate im Rahmen der zweiten Zahlungsdiensterichtlinie (PSD2-VO)

1. Einleitung (Introduction)

Dieses Dokument beschreibt das Zertifikatskonzept, in Form eines Certification Practice Statement (im Folgenden CPS genannt), der von der Bank-Verlag GmbH betriebenen Vertrauensdienste, die für die Ausstellung PSD2-konformer qualifizierter Website-Zertifikate angeboten werden.

Das CPS nimmt Bezug aufdie Zertifikatsrichtlinie der Zertifizierungsstelle der Bank-Verlag GmbH (im Folgenden CP genannt) mit der Kennung 1.3.6.1.4.1. 50833.1.2.2 sowie die gesetzlichen Bestimmungen und Normen eIDAS-VO, VDG, VDV, ETSI EN 319 401, ETSI EN 319 411-1, ETSI EN 319 411-2, ETSI TS 119 495. Es beschreibt die Umsetzung der daraus resultierenden Anforderungen.

Die Gliederung des Dokuments basiert auf dem Standard RFC 3647, um einen Vergleich mit dem CPS anderer Vertrauensdiensteanbieter zu erleichtern.

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

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 angebotene Dienst, der diesem CPS unterliegt, ist

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

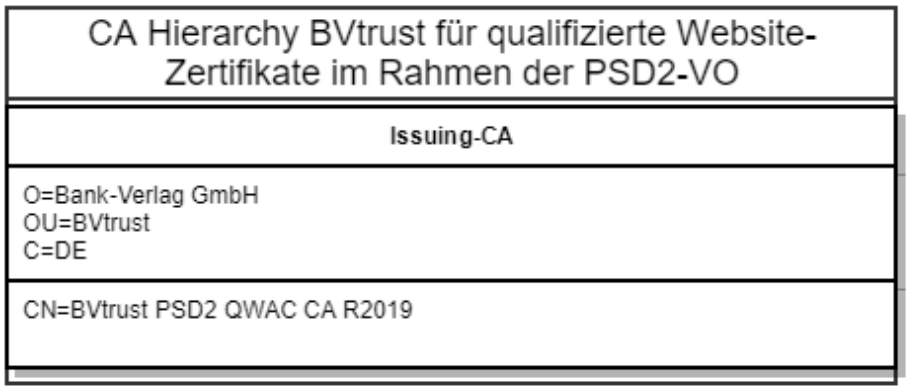
Der Dienst der Zertifikatsausstellung für qualifizierte Website-Zertifikate und alle damit verbundenen Themen werden, wie alle CA-Dienste, unter dem Namen BVtrust angeboten.

Dieses Dokument beschreibt das Zertifizierungskonzept (CPS) der oben genannten Vertrauensdienste. Es enthält Anforderungen und Vorgaben für die Erb ringung der Vertrauensdienste. Die Policy QCP-w aus ETSI EN 319 411-2 wird erfüllt. Diese enthält Referenzen auf Anforderungen in den Dokumenten ETSI EN 319 411-1, ETSI EN 319 412-4, ETSI EN 319 412-5, ETSI TS 119 495, welche ebenfalls umgesetzt werden.

Der TSP erbringt den Vertrauensdienst zur Ausstellung qualifizierter Website-Zertifikate unter Erfüllung aller durch die Policy QCP-w von ETSI EN 319 411-2 referenzierten Anforderungen.

Dieses CPS betrachtet die PKI für die Ausstellung von Zertifikaten für qualifizierte Website-Zertifikate im Rahmen der zweiten Zahlungsdiensterichtlinie (PSD2-VO). Diese ist in einer 1-Tier-Hierarchie aufgebaut. Es wird nicht zwischen Root- und Issuing-CA unterschieden. Die Zertifikate der ausstellenden CAs werden in die *EU Trusted List* aufgenommen. Es wird ein CA-Zertifikat mit einem RSA-Schlüssel für qualifizierte Website-Zertifikate erstellt.

Die Ausgabe von Wildcard-Zertifikaten ist im Rahmen dieses Dienstes nicht möglich.



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

Dokumentenname: Zertifikatskonzept (Certification Practice Statement) der Zertifizierungsstelle BVtrust der Bank-Verlag GmbH für qualifizierte Websitezertifikate im Rahmen der zweiten Zahlungsdiensterichtlinie (PSD2-VO)

Kennzeichnung (OID): 1.3.6.1.4.1.50833.1.2.1

Stand: Version 145 am 2019-08-20

1.3. PKI-Beteiligte (PKI participants)

1.3.1. Zertifizierungsstellen (Certification authorities)

Dieser Abschnitt wird in der zugehörigen Zertifikatsrichtlinie (CP) der Zertifizierungsstelle der Bank-Verlag GmbH beschrieben.

1.3.2. Registrierungsstellen (Registration authorities)

Dieser Abschnitt wird in der zugehörigen Zertifikatsrichtlinie (CP) der Zertifizierungsstelle der Bank-Verlag GmbH beschrieben.

Innerhalb der Registration Authority (RA) existiert die Rolle des Validation Specialist (VS). Die Rolle VS übernimmt die Validierung eines an die RA gestellten Zertifikatsrequests. Innerhalb der Rolle des VS existiert ein Vieraugenprinzip, sodass der Rolle VS, für einen funktionierenden Prozessablauf, mindestens zwei Elemente innerhalb der Rolle VS zugeordnet werden müssen.

Der erste VS prüft

- die Angaben über den Endanwender aus dem Antrag gegen einen Handelsregisterauszug,
- die PSD2-Angaben gegen die Quellen der EBA und
- die Identifizierungsdaten, die von identityTM übermittelt werden.

Der zweite VS prüft,

- ob der Validierungsprozess ordnungsgemäß durchgeführt wurde und
- bestätigt die erhobenen Daten.

Die Rolle VS erfüllt alle zusätzlichen sektorspezifischen Anforderungen zur Herausgabe von qualifizierten Zertifikaten, die unter der Payment services (PSD 2) - Directive (EU) 2015/2366 von einem TSP gefordert werden. Elemente der Rolle VS werden regelmäßig geschult.

1.3.3. Zertifikatnehmer und Endanwender (Subscribers/End Entity)

Dieser Abschnitt wird in der zugehörigen Zertifikatsrichtlinie (CP) der Zertifizierungsstelle der Bank-Verlag GmbH beschrieben.

Die Ausgabe von qualifizierten Website-Zertifikaten zur Website-Authentifizierung wird auf juristische Personen als Endanwender beschränkt. Natürliche Personen sind als Endanwender von der Nutzung der qualifizierten Website-Zertifikate für PSD2 ausgeschlossen.

1.3.4. Vertrauender Dritter (Relying parties)

Dieser Abschnitt wird in der zugehörigen Zertifikatsrichtlinie (CP) der Zertifizierungsstelle der Bank-Verlag GmbH beschrieben.

1.3.5. Andere Teilnehmer (Other participants)

Der TSP bietet den Endanwendern ein qualifiziertes Website-Zertifikat an. Der Endanwender oder ein Vertretungsberechtigter des Endanwenders ist dazu berechtigt, beim TSP einen Antrag für ein qualifiziertes Website-Zertifikat zu stellen.

Der TSP identifiziert den für den Endanwender vertretungsberechtigten Zertifikatnehmer über einen nach VO (EU) Nr. 910/2014 eIDAS-konformen Identifizierungsdiensteanbieter. Es wird identityTM mit dem Verfahren „identity Kurier" genutzt.

1.4. Zertifikatsverwendung (Certificate usage)

1.4.1. Zulässige Verwendung von Zertifikaten (Appropriate certificate uses)

Zertifikate, die diesem CPS unterliegen, sind ausschließlich für Endanwender (auch Subjects oder End Entities, kurz EE) ausgestellt; CA-Zertifikate werden nicht ausgestellt. Die Endanwenderzertifikate können im Sinne der der zweiten Zahlungsdiensterichtlinie (EU) 2015/2366 verwendet werden.

1.4.2. Unzulässige Verwendung von Zertifikaten (Prohibited certificate uses)

Alle Verwendungen, die nicht dem Punkt 1.4.1 oder Punkt 1.4.2 der CP entsprechen, sind unzulässig.

1.5. Verwaltung der Richtlinie (Policy administration)

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

Dieses CPS wird durch das TSP-Management der Bank-Verlag GmbH verwaltet.

1.5.2. Kontaktinformationen (Contact person)

Dieser Abschnitt wird in der zugehörigen Zertifikatsrichtlinie (CP) der Zertifizierungsstelle der Bank-Verlag GmbH beschrieben.

1.5.3. Pflege der Richtlinie

Dieses CPS behält Gültigkeit, solange es nicht von der zuständigen Instanz widerrufen wird. Es 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 (CPS) 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, auf die Einhaltung dieser sowie übergeordneter CP/CPS hin 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
NCA	National competent authority
PKI	Public-Key-Infrastruktur
PSD2	Payment services (PSD 2) - Directive (EU) 2015/2366
RA	Registration Authority
TSP	Trust Service Provider
VA	Validation Authority
VS	Validation Specialist

2. Veröffentlichungen und Verzeichnisdienste (PUBLICATION AND REPOSITORY RESPONSIBILITIES)

2.1. Verzeichnisdienste (Repositories)

Dieser Abschnitt wird in der zugehörigen Zertifikatsrichtlinie (CP) der Zertifizierungsstelle der Bank-Verlag GmbH beschrieben.

2.2. Veröffentlichung von Zertifikatsinformationen (Publication of certification information)

Der TSP veröffentlicht zu den von ihm ausgegebenen Zertifikaten

- die CP,
- dieses CPS,
- das PDS,
- CA-Zertifikate und

- Statusinformationen über OCSP.

Alle Informationen können auf der Webseite des TSP abgerufen werden, ausgenommen der Statusinformationen, die direkt via OCSP abgefragt werden können. Webseite und Statusinformationsdienst werden hochverfügbar in den redundant ausgelegten Rechenzentren des TSP betrieben und sind 24/7 erreichbar. Sie werden im Falle eines Ausfalls schnellstmöglich wieder zur Verfügung gestellt. Die zugesicherte maximale Wiederanlaufzeit gem. BCM Notfallplan beträgt 4 Stunden.

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

Dieser Abschnitt wird in der zugehörigen Zertifikatsrichtlinie (CP) der Zertifizierungsstelle der Bank-Verlag GmbH beschrieben.

2.4. Zugang auf Verzeichnisdienste (Access controls on repositories)

Dieser Abschnitt wird in der zugehörigen Zertifikatsrichtlinie (CP) der Zertifizierungsstelle der Bank-Verlag GmbH beschrieben.

3. Identifizierung und Authentifizierung (IDENTIFICATION AND AUTHENTICATION)

3.1. Namensregeln (Naming)

3.1.1. Namensformen (Types of names)

Qualifizierte elektronische Zertifikate müssen den Namen des Endanwenders enthalten. Die Identität des Zertifikatsnehmers und die Angaben über den Endanwender werden überprüft. Die Zertifikate entsprechen dem Profil des Standards ITU-T Recommendation X.509v3. Qualifizierte Zertifikate für juristische Personen enthalten die offizielle Bezeichnung der Organisation.

3.1.2. Aussagekraft von Namen (Need for names to be meaningful)

Die verwendeten Namen sind eindeutig. Um dies sicherzustellen, enthält der DistinguishedName (DN) das Feld description mit einer UUID, um eine eindeutige Zuordnung des Zertifikats zu gewährleisten.

3.1.3. Pseudonymisierung bzw. Anonymisierung der Zertifikatnehmer (Anonymity or pseudonymity of subscribers)

Zertifikate mit Pseudonymen oder anonyme Zertifikate werden nicht ausgestellt.

3.1.4. Regeln zur Interpretation verschiedener Namensformen (Rules for interpreting various name forms)

Attribute von EE-Zertifikaten für juristische Personen werden wie folgt interpretiert:

DN-Bestandteile	Interpretation
commonName	Als CN wird die Hauptdomain des Endanwenders (SAN1) im Format: *firma-gmbh.de* verwendet. | Es gilt eine Zeichenbegrenzung von 64 Zeichen. Zertifikate für reservierte IP-Adressen oder interne Namen werden nicht ausgestellt.
organizationName	Offizielle Bezeichnung der juristischen Person oder Bezeichnung der Organisation, der der Endanwender angehört oder damit verbunden ist (Firma, Behörde, Verein etc.) entsprechend Existenznachweis, ggf. sinnvolle Abkürzung bei Überschreiten der Zeichenbegrenzung von 64 Zeichen.
organizationIdentifier	Eindeutige PSD2-Autorisierungsnummer der Organisation. Der TSP akzeptiert die von einer National Competent Authority für PSD2 (z.B. BaFin) vergebenen IDs. Wurde die PSD2-Autorisierungsnummer nicht durch eine NCA ausgestellt, muss eine andere, von der NCA anerkannte Registrierungsnummer gemäß ETSI EN 319 412-1, Klausel 5.1.4 verwendet werden.
countryName	Das aufzuführende Land entspricht dem im Register genannten Sitz der Organisation und ist gemäß ISO 3166 zu notieren.
localityName	Die aufzuführende Stadt entspricht dem im Register genannten Sitz der Organisation.
serialNumber	Seriennummer in Form einer Registrierungsnummer (Handelsregisternummer), oder, wenn kein Handelsregisterauszug vorliegt, das Gründungsdatum der juristischen Person, als Namenszusatznummer.

jurisdiction (jurisdictionCountryName; jurisdictionStateorProvinceName; jurisdictionLocalityName)	Diese Felder geben den Ort des Gerichtsstands an, in welchem die Gründungs- oder Registrierungsbehörde sitzt, die die Gründung der subject-Organisation bestätigt. Es dürfen nur die relevanten Felder angegeben werden. Arbeitet die Behörde auf Länderebene, muss und wird nur jurisdictionCountryName angegeben. Arbeitet die Behörde auf Ebene eines Bundesstaates oder einer Provinz, werden und müssen jurisdictionCountryName und jurisdictionStateOrProvinceName angegeben werden. Arbeitet die Behörde auf Orts- oder Stadtebene, dann müssen alle drei Attribute angegeben werden. Das Feld jurisdictionCountryName muss immer angegeben werden. Dieses Feld muss den ISO-3166-1-Ländercode enthalten.
businessCategory	Enthält einen der vier Werte „Private Organization" (dt. „Privatorganisation"), „Government Entity" (dt. „Regierungseinrichtung"), „Business Entity" (dt. „Unternehmen") and „Non-Commercial Entity" (dt. „Nichtkommerzielle Organisation").
description	Enthält eine UUID, um die eindeutige Zuordenbarkeit des Zertifikats zu gewährleisten. Beinhaltet den Text "test certificate - UUID" im Falle von für Testzwecke ausgestellten Zertifikaten.
Nicht-DN-Bestandteile	**Interpretation**
SAN1 (subjectAltName)	Es muss immer mindestens eine FQDN in diesem Feld stehen. Als SAN1 wird die Hauptdomain des Endanwenders im Format: *firma-gmbh.de* verwendet | Weitere SANs, die optional sind, werden als FQDNs werden in entsprechend benannten Feldern gelistet. Es gilt eine Zeichenbegrenzung von 64 Zeichen. Zertifikate für reservierte IP-Adressen oder interne Namen werden nicht ausgestellt. Genaue Spezifikationen befinden sich in 7.1.2.3 dieser CPS.

Es müssen alle DN-Bestandteile verwendet werden. Weitere können ergänzt werden. Alle DN-Bestandteile müssen RFC 5280, RFC 6818 und ETSI EN 319 412 entsprechen. Das Feld description enthält in produktiven Zertifikaten eine UUID, um die Eindeutigkeit des Distinguished Name zu gewährleisten. In Testzertifikaten enthält das Feld den Wert "test certificate".

3.1.5. Eindeutigkeit von Namen (Uniqueness of names)

Die Namen setzen sich aus mindestens den Bestandteilen aus 3.1.4 zusammen. Um eine Eindeutigkeit des DN zu erzwingen, muss eine eindeutige Seriennummer in Form einer UUID vergeben werden. Ein bereits vergebener DN wird niemals an einen anderen Endanwender vergeben. Die Gefahr einer möglichen Verwechslung durch zwei Personen mit identischem Namen ist somit ausgeschlossen.

3.1.6. Anerkennung, Authentifizierung und die Rolle von Markennamen (Recognition, authentication, and role of trademarks)

Der Endanwender trägt die Verantwortung für die Vereinbarkeit der Namenswahl mit den Rechten Dritter, z.B. Namens-, Marken-, Urheber- oder sonstigen Schutzrechten sowie mit den allgemeinen Gesetzen. Der TSP ist nicht verpflichtet, solche Rechte zu überprüfen. Daraus resultierende Schadenersatzansprüche gehen zu Lasten des Endanwenders.

3.2. Identitätsprüfung bei Neuantrag (Initial identity validation)

Der TSP hat Personen, die ein qualifiziertes Zertifikat beantragen, eindeutig zu identifizieren. Dabei werden nur Informationen erfasst, die zur Nutzung des Dienstes und zur Erstellung der Zertifikate notwendig sind.

3.2.1. Methode zum Besitznachweis einer Domain (Method of verification of domain control)

Der TSP muss überprüfen, dass der Endanwender über die Kontrolle der zu zertifizierenden Domains verfügt. Der TSP versendet per E-Mail an jede zu zertifizierende Top-Level-Domain einen Zufallswert, der vom Endanwender zurückgesendet wird, um die Kontrolle zu bestätigen. Der Prozess verläuft konform zu den Anforderungsdokumenten des CA/Browser Forums.

3.2.2. Methode zum Besitznachweis eines privaten Schlüssels (Method to prove possession of private key)

Das Schlüsselpaar wird im Verantwortungsbereich des Endanwenders generiert. Der Endanwender muss glaubhaft und sicher nachweisen, dass dieser im Besitz des Schlüsselpaars ist.

Nach der Übersendung eines Certificate Signing Requests (CSR) an den TSP prüft ein Validation Specialist, ob er auf dem Antragsformular angegebene Hashwert mit dem Hashwert des CSR übereinstimmt, welcher durch den VS selbst, unter Verwendung des öffentlichen Schlüssels des gelieferten CSR, generiert wird.

Zudem wird die Signatur des CSR mithilfe des öffentlichen Schlüssels geprüft, um sicherzustellen, dass der Endanwender im Besitz des privaten Schlüssels ist.

3.2.3. Authentifizierung der Identität von Organisationen (Authentication of organization identity)

Um die juristische Person, die im DN des Zertifikats unter Organization (O) genannt wird, zu authentifizieren, wird entsprechend der Art der juristischen Person bei der Erstbeauftragung folgendes Dokument benötigt:

- Behörde: Das von einem Bevollmächtigten der Behörde unterschriebene und mit dem Dienstsiegel versehene Auftragsformular.
- Verein: Die beglaubigte Kopie (nicht älter als 30 Tage) des Vereinsregisterauszuges sowie das unterzeichnete Antragsformular.
- Gewerbetreibende(r): Die beglaubigte Kopie (nicht älter als 30 Tage) eines aktuellen Gewerbescheins und des Personalausweises des Gewerbetreibenden sowie das unterzeichnete Antragsformular.
- Alle anderen Geschäftsformen: Das von einem Zeichnungsberechtigten Vertreter der Organisation unterschriebene Auftragsformular.

Alle Personen, unabhängig von der Art der Organisation, die eine Organisation vertreten, müssen gemäß Art. 24 Abs. 1 der VO (EU) Nr. 910/2014 identifiziert werden.

Für alle Geschäftsformen werden folgende Daten erhoben:

1. Firma, Name oder Bezeichnung,
2. Rechtsform,
3. Umsatzsteuer- und Handelsregisternummer (falls vorhanden),
4. Anschrift des Sitzes oder der Hauptniederlassung oder der im Handelsregister angegebenen Geschäftsanschrift,
5. die Namen der Mitglieder des Vertretungsorgans oder die Namen der gesetzlichen Vertreter und
6. E-Mail-Adresse des technischen Ansprechpartners zur direkten Kontaktaufnahme durch den TSP.

Darüber hinaus können zusätzlich weitere freiwillige Angaben erhoben werden wie bspw. E-Mail-Adresse oder Branche. Diese freiwilligen Angaben können als Anhang zum Antrag mitgeliefert werden.

Für alle Gesellschaftsformen wird in jedem Fall überprüft:

- die im Zertifikatsantrag angegebene Adresse der Organisation wird anhand des elektronischen Handelsregisters oder vergleichbarer Verzeichnisse überprüft. Der Auftraggeber muss an dem angegebenen Standort eine Filiale, Geschäftsstelle oder Ähnliches betreiben.
- die Zeichnungsberechtigung des im Antrag aufgeführten Zertifikatnehmers für den Endanwender.

Für die Überprüfung der Existenz oder der Adresse der Organisation können alternativ oder zusätzlich zum Handelsregister bzw. der vergleichbaren Verzeichnisse weitere Methoden herangezogen werden.

Mindestens ein juristischer Vertreter wird durch die identity Trust Management AG mit dem „identity Kurier"-Verfahren, welches nach VO (EU) Nr. 910 /2014 zugelassen ist, identifiziert.

Ferner sind gemäß ETSI TS 119 495 zwingend folgende Angaben einzureichen:

- Rolle(n) des Payment Service Providers (PSP) laut PSD2-VO,
- NCAName (auf Englisch) und
- NCAId.

Dabei überprüft der TSP, ob der Endanwender durch die NCA die Berechtigung innehat, in der oder den beantragten Rolle(n) als PSP zu agieren.

Zusätzliche Prüfungen werden nach Bedarf durchgeführt.

3.2.4. Authentifizierung der Identität von natürlichen Personen (Authentication of individual identity)

Die Identität einer natürlichen Person muss gemäß Art. 24 Abs. 1 der VO (EU) Nr. 910/2014 korrekt identifiziert sein. Dies umfasst den Vertretungsberechtigten des Endanwenders. Der TSP identifiziert den für den Endanwender vertretungsberechtigten Zertifikatnehmer über einen nach VO (EU) Nr. 910/2014 eIDAS-konformen Identifizierungsdiensteanbieter. Es wird die identity Trust Management AG als Identifizierungsdiensteanbieter verwendet. Die Identifizierung erfolgt mit dem Verfahren „identityKurier“ vor Ort. Es werden keine existierenden Daten, die auf Basis anderer Richtlinien erhoben wurden, verwendet.

Folgende Daten werden erhoben:

- Vor- und Zuname,
- vollständige Adresse laut eingetragenem Wohnsitz,
- Geburtsdatum,
- Geburtsort,
- Telefonnummer,
- E-Mail-Adresse,
- Organisationszugehörigkeit,
- Staatsangehörigkeit.

Darüber hinaus können optional folgende Daten erhoben werden:

- Telefaxnummer,
- Geburtsname.

Diese freiwilligen Angaben können als Anhang zum Antrag mitgeliefert werden.

Zertifikate werden nur für juristische Personen ausgestellt. Der Endanwender (bzw. dessen autorisierter Vertreter) stellt beim TSP einen Antrag für das qualifizierte Websitezertifikat.

Zusätzliche Prüfungen werden nach Bedarf durchgeführt.

3.2.5. Ungeprüfte Angaben zum Zertifikatnehmer (Non-verified subscriber information)

Alle Informationen, welche in ein Zertifikat übernommen werden und im Rahmen der Authentifizierung nach 3.2.3 und 3.2.4 erhoben werden, müssen verifiziert werden.

3.2.6. Prüfung der Berechtigung zur Antragstellung (Validation of authority)

Qualifizierte Website-Zertifikate werden ausschließlich für juristische Personen (Endanwender) ausgestellt. Der Endanwender muss dem TSP gegenüber seinen Existenznachweis nach 3.2.3 erbringen, die Vertretungsberechtigung des Zertifikatsnehmers nachweisen, sowie den Identitätsnachweis ggf. mit Organisationszugehörigkeit des Zertifikatnehmers nach 3.2.3 und 3.2.4 erbringen. Nach der Prüfung der Antragsdokumente entscheidet der TSP, ob er den Antrag annimmt oder ablehnt.

3.3. Identifizierung und Authentifizierung bei Anträgen auf Schlüsselerneuerungen (Identification and authentication for re-key requests)

Eine Schlüsselerneuerung ist nicht vorgesehen.

3.3.1. Identifzierung und Authentifizierung für routinemäßige Schlüsselerneuerungen (Identification and authentication for routine re-key)

Eine Schlüsselerneuerung ist nicht vorgesehen.

3.3.2. Identitätsprüfung und Authentifizierung bei Schlüsselerneuerungen nach Zertifikatswiderruf (Identification and authentication for re-key after revocation)

Eine Schlüsselerneuerung ist nicht vorgesehen.

3.4. Identifizierung und Authentifizierung bei Widerrufsanträgen (Identification and authentication for revocation requests)

Widerrufsberechtigte nach 4.9.2 können, unter Angabe eines Widerrufsgrundes, beim TSP einen Antrag auf Widerruf eines Zertifikats einreichen. Abhängig davon, wer diesen Widerrufsantrag einreicht, sind unterschiedliche Prozesse vorgesehen.

NCAs erhalten die Möglichkeit, Widerrufsanträge über einen durch ein qualifiziertes Zertifikat authentifizierten Kommunikationweg an den TSP zu stellen.

Zuständige Behörden wie das Bundesamt für Sicherheit in der Informationstechnik stellen einen Widerrufsantrag über die unten angegebene E-Mail-Adresse. Der TSP kontaktiert die Behörde daraufhin telefonisch und verifiziert die Authentizität des Antrags.

Der Endanwender wendet sich zum Widerruf eines Zertifikats direkt über die veröffentlichten Kontaktinformationen an den TSP. Die Authentifizierung der Anfrage geschieht dabei durch eine Kontaktaufnahme des des TSP mit dem Endanwender und der Abfrage des Widerrufpassworts, welches der Endanwender bzw. der Zertifikatnehmer dem TSP mit dem Antrag auf Ausstellung eines Zertifikats übergeben hat.

Der Widerruf sowie die vom Widerrufsantragsteller angegebenen Widerrufsgründe werden mittels eines automatisch erzeugten Widerrufsprotokolls dokumentiert. Der Widerruf wird protokolliert und kann nur durch autorisiertes Personal durchgeführt werden. Ferner werden der Zertifikatnehmer und Endanwender über den Widerruf per E-Mail informiert.

Für Endanwender sowie Widerrufsberechtigte Dritte können weitere Möglichkeiten explizit vereinbart werden. Der Widerruf eines Zertifikats kann nicht rückgängig gemacht werden.

Certificate Problem Reports können an psd2-problems@bank-verlag eingereicht werden.

Der 24x7-Bereitschaftsdienst reagiert innerhalb der festgelegten Reaktionszeiten auf einen Certificate Problem Report, widerruft nach Prüfung entsprechende Zertifikate und informiert, wenn nötig, die zuständigen Strafverfolgungsbehörden über den Inhalt eines Certificate Problem Reports mit hoher Priorität.

4. Betriebsanforderungen (CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS)

4.1. Zertifikatsantrag (Certificate Application)

4.1.1. Berechtigung zur Antragstellung (Who can submit a certificate application)

Anträge für ein qualifiziertes Website-Zertifikat dürfen im Rahmen von BVtrust nur von juristischen Personen und deren autorisierten Vertretern gestellt werden, die im Rahmen der PSD2-VO von ihrer jeweiligen National Competent Authority (NCA) für eine oder mehrere Rollen als Payment Service Provider (PSP) autorisiert worden sind.

Juristische Personen oder deren autorisierte Vertreter beantragen das Zertifikat direkt bei der RA des TSPs.

Der TSP ist dazu berechtigt, Anträge abzulehnen.

4.1.2. Registrierungsprozess und Verantwortlichkeiten (Enrollment process and responsibilities)

Die Einhaltung des Registrierungsprozesses gewährleistet der TSP.

Dem Endanwender liegen vor Abschluss des Registrierungsprozesses alle Dokumente wie CP, CPS und PDS vor, zu deren Einhaltung sich der Endanwen der verpflichtet. Die Dokumente sind öffentlich. Weiterhin verpflichtet sich der Endanwender zu der Einhaltung der mit dem TSP gesondert geschlossenenen vertraglichen Rahmenbedingungen, zu dem die Einstimmung des Endanwenders zur Einhaltung der oben genannten Dokumente gehört. Der Antrag beinhaltet weiterhin die Einverständniserklärung des Endanwenders zur Veröffentlichung oder Nicht-Veröffentlichung der Zertifikate. Alle Vereinbarungen werden vertraglich getroffen und in Papierform festgehalten. Alle Nachweise und Vertragsdokumente werden für die Dauer, die vertraglich vereinbart wurde, elektronisch oder papierbasiert hinterlegt.

Nutzungsbedingungen bzw. AGBs werden im Rahmen der Vertragsdokumente an den Antragsteller übermittelt, dies geschieht in physischer Form.

4.2. Verarbeitung des Zertifikatsantrags (Certificate application processing)

4.2.1. Durchführung der Identifikation und Authentifizierung (Performing identification and authentication functions)

Der beschriebene Identifizierungs- und Authentifizierungsprozess muss vollständig durchlaufen werden und alle nötigen Nachweise und Dokumente müssen erbracht werden.

Der TSP ist für die ordentliche Prüfung der zu zertifizierenden Domains auf Vorhandensein des korrekten CAA-Eintrags verantwortlich. Der TSP prüft bei Antragsannahme die Domains auf einen entsprechenden CAA-Eintrag. Ist der Eintrag leer, wird mindestens ein Eintrag gesetzt, der bank-verlag.de enthält, oder ist jede CA autorisiert, Zertifikate für eine Domain auszustellen, ist die Prüfung erfolgreich.

Der TSP ist für die ordentliche Identifizierung und Authentifizierung des Endanwenders bzw. des Zertifikatnehmers nach Art. 24 Abs. 1 der VO (EU) Nr. 910 /2014 verantwortlich.

Der TSP identifiziert den für den Endanwender vertretungsberechtigten Zertifikatnehmer über den nach VO (EU) Nr. 910/2014 zugelassenen Identifizierungsdiensteanbieter identity Trust Mangement AG über das „identityKurier“-Verfahren vor Ort.

Der Endanwender wird in Übereinstimmung mit Abschnitt 3.2.3 authentifiziert.

Die Identifizierung und Authentifizierung der Zertifikatnehmer und Endanwender muss vor der Ausstellung des Zertifikats abgeschlossen sein. Der VS führt die Identifizierung und Authentifizierung des Endanwenders durch und überprüft die durch identity TM durchgeführte Identifikation des Zertifikatnehmers.

4.2.2. Genehmigung oder Ablehnung des Zertifikatsantrags (Approval or rejection of certificate applications)

Treten bei der Prüfung der Identität oder im Rahmen der Identifizierung und Authentifizierung oder der Prüfung auf Korrektheit der Daten im Zertifikatsantrag oder den Ausweis- und Nachweisdokumenten Unstimmigkeiten auf, die nicht restlos ausgeräumt werden können, wird der Antrag abgelehnt. Weitere Gründe für die Antragsablehnung können folgende Punkte sein:

- Verdacht auf die Verletzung der Namensrechte Dritter,
- Nichteinhalten von Fristen für den Nachweis der Daten,
- Zahlungsrückstände des Antragstellers gegenüber dem TSP oder
- Umstände, die den Verdacht begründen, dass eine Zertifikatsausstellung den Betreiber der CA in Misskredit bringt.

Der TSP ist berechtigt, Zertifikatsanträge auch ohne die Angabe von Gründen abzulehnen. Erhält der TSP PKCS#10- oder andere Zertifikats-Requests, werden deren Inhalte durch den TSP auf Korrektheit überprüft. Erfüllt der Public Key des Zertfikats nicht die Anforderungen bezüglich der verwendeten Verschlüsselungsalgorithmen und -stärken oder liegt dem CSR ein schwacher Private Key zugrunde, wird der CSR abgelehnt. Die Überprüfung des Requests wird von den Mitarbeitern des TSP in der Rolle VS geprüft. Diese VS-Mitarbeiter müssen alle Vorgaben zur Überprüfung von Zertifikatsrequests einhalten.

Zu einer Annahme des Zertifikats sind zwingend folgende Angaben einzureichen:

- eine oder mehrere Rollen des Payment Service Providers (PSP) laut PSD2-VO z.B.:
  - PSP_AS,
  - PSP_PI,
  - PSP_AI,
  - PSP_IC
- sowie den Namen und die eindeutige Kennung der zuständigen Behörde (NCA), bei dem der PSP registriert ist:
  - NCAName (auf Englisch) und
  - NCAId
- alle in 3.1.4 beschriebenen Punkte.

4.2.3. Bearbeitungsdauer von Zertifikatsanträgen (Time to process certificate applications)

Entfällt.

4.3. Ausstellung von Zertifikaten (Certificate issuance)

4.3.1. Vorgehen der CA bei der Ausstellung des Zertifikats (CA actions during certificate issuance)

Der Endanwender generiert ein Schlüsselpaar und befindet sich im alleinigen Besitz des dazugehörigen privaten Schlüssels. Mithilfe dieses Schlüsselpaars wird ein CSR erstellt, mit welchem sich der Endanwender gegenüber dem TSP authentifiziert.

Die Erstellung des Zertifikats erfolgt in den Liegenschaften bzw. Räumlichkeiten des TSP. Die eigentliche Zertifikatserstellung erfolgt durch die im gesicherten Rechenzentrum des TSP befindliche CA. Dabei wird sichergestellt, dass bei der Zertifikatserstellung die korrekte Zeit verwendet wird.

Die RA des TSP initiiert im Vier-Augen-Prinzip den eigentlichen Zertifikatserstellungsprozess, sobald der Registrierungsantrag korrekt bearbeitet wurde.

Das Zertifikat wird an den Endanwender übermittelt.

4.3.2. Benachrichtigung von Endteilnehmern über die Ausstellung von Zertifikaten (Notification to subscriber by the CA of issuance of certificate)

Es erfolgt keine weitere gesonderte Benachrichtigung des Zertifikatnehmers.

4.4. Zertifikatsübergabe (Certificate acceptance)

4.4.1. Verhalten bei der Zertifikatsübergabe (Conduct constituting certificate acceptance)

Der TSP vereinbart mit dem Zertifikatnehmer ein geeignetes Verfahren zur Bereitstellung des Zertifikats.

4.4.2. Veröffentlichung des Zertifikats durch den TSP (Publication of the certificate by the CA)

Der TSP bietet einen intern wie extern erreichbaren Statusabfragedienst über OCSP an. Eine gesonderte Veröffentlichung der ausgestellten Zertifikate der Endanwender erfolgt nicht.

4.4.3. Benachrichtigung Dritter über die Erstellung des Zertifikats (Notification of certificate issuance by the CA to other entities)

Eine gesonderte Benachrichtigung über die Erstellung des Zertifikats erfolgt nicht.

4.5. Verwendung des Schlüsselpaars und des Zertifikats (Key pair and certificate usage)

4.5.1. Verwendung des privaten Schlüssels und des Zertifikats durch den Zertifikatnehmer (Subscriber private key and certificate usage)

Endanwender sowie Vertretungsberechtigte des Endanwenders dürfen ihre privaten Schlüssel ausschließlich für die Anwendungen nutzen, die in Übereinstimmung mit den im Zertifikat angegebenen Nutzungsarten stehen. Für Endanwender und Vertretungsberechtigte des Endanwenders gelten die Bestimmungen aus Abschnitt 1.4.

4.5.2. Verwendung des öffentlichen Schlüssels und des Zertifikats durch Zertifikatsinhaber (Relying party public key and certificate usage)

Das Zertifikat kann von allen durch den Endanwender autorisierten Personen genutzt werden. Die Endanwender, Zertifikatsnehmer und Dritte dürfen jedoch nur dann auf den öffentlichen Schlüssel und das Zertifikat vertrauen, wenn folgende Voraussetzungen vorliegen:

- vor der Nutzung des Zertifikats werden die darin angegebenen Informationen auf Richtigkeit überprüft,
- das Zertifikat wird gemäß den zulässigen Nutzungsarten benutzt und eventuelle Einschränkungen im Zertifikat wurden beachtet,
- dabei sollen insbesondere die technischen Verwendungszwecke geprüft werden, 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.
- die Zertifikatskette kann erfolgreich bis zu einem vertrauenswürdigen Root-Zertifikat verifiziert werden, welches in der EUTL (European Trusted List) aufgeführt ist,
- die Gültigkeit des Zertifikats wurde über den Statusabfragedienst (OCSP) bestätigt,
- alle weiteren Vereinbarungen und sonstigen Vorsichtsmaßnahmen wurden eingehalten.

4.6. Zertifikatserneuerung (Certificate renewal)

Eine Zertifikatserneuerung wird nicht angeboten.

4.7. Zertifikatserneuerung mit Schlüsselerneuerung (Certificate re-key)

Eine Zertifikatserneuerung mit Schlüsselerneuerung wird nicht angeboten. In diesem Fall ist eine erneute Registrierung erforderlich.

4.8. Änderung von Zertifikatsdaten (Certificate modification)

Eine nachträgliche Änderung des Zertifikats durch den TSP ist nicht möglich.

4.9. Zertifikatswiderrufe und Suspendierung (Certificate revocation and suspension)

4.9.1. Bedingungen für einen Widerruf (Circumstances for revocation)

Endanwender und Zertifikatnehmer oder auch betroffene Dritte sind aufgefordert, den Widerruf unverzüglich zu beantragen, wenn der Verdacht besteht, dass private Schlüssel kompromittiert wurden, die Kontrolle und der Zugriff (z.B. Authentifizierungsdaten) über den privaten Schlüssel kompromittiert wurde oder Daten des Zertifikats nicht mehr korrekt sind.

Der TSP muss ein Zertifikat widerrufen

- auf Verlangen des Endanwenders, eines autorisierten Vertreters des Endanwenders, eines Widerrufsberechtigten Dritten oder der entsprechenden Aufsichtsbehörde,
- wenn der Endanwender den TSP darüber informiert, dass der ursprüngliche Zertifikatsantrag nicht autorisiert wurde und auch nicht rückwirkend autorisiert wird,
- bei fehlerhaften Angaben im Zertifikat oder
- bei Einstellung der Tätigkeit als Zertifizierungs-/Vertrauensdiensteanbieter.

Unabhängig davon muss der TSP Zertifikatswiderrufe veranlassen, wenn

- der private Schlüssel der ausstellenden oder einer übergeordneten CA kompromittiert wurde,
- die den angewendeten Verfahren zugrundeliegenden Algorithmen gebrochen wurden oder wenn Gründe vorliegen, die annehmen lassen, dass die den angewendeten Verfahren zugrundeliegenden Algorithmen gebrochen wurden,
- die eingesetzte Hard- oder Software Sicherheitsmängel aufweist, die ernste Risiken für die erlaubten Anwendungen während der Zertifikatlaufzeit darstellen,
- die eindeutige Zuordnung des Schlüsselpaars zum Endanwender nicht mehr gegeben ist,
- der TSP Nachweise dafür erhält, dass die Prüfung auf Besitz durch den Endanwender für jegliche im Zertifikat aufgeführte FQDNs nicht vertrauenswürdig ist,
- ein Zertifikat nicht mehr konform mit der CP oder CPS, unter der es ausgestellt wurde, ist,
- dem TSP Änderungen, die die Gültigkeit eines Zertifikats beeinflussen, bekannt werden,
- die verwendete Kryptographie eines Zertifikats die Bindung zwischen privatem und öffentlichem Schlüssel nicht mehr gewährleistet,
- die Autorisierung des TPPs zurückgezogen wurde oder eine im Zertifikat aufgeführte PSD2-Rolle zurückgezogen wurde,
- ein Zertifikat aufgrund falscher Angaben erwirkt oder anderweitig missbraucht wurde oder
- das Vertragsverhältnis gekündigt oder in sonstiger Weise beendet wurde.

Widerrufe enthalten eine Angabe des Zeitpunkts des Widerrufs des Zertifikats. Zertifikate können nicht rückwirkend widerrufen werden. Weiterhin kann ein Widerruf nicht rückgängig gemacht werden.

Widerrufsberechtigte müssen sich gemäß Abschnitt 3.4 authentifizieren.

4.9.2. Widerrufsberechtigung (Who can request revocation)

Zum Widerruf des Zertifikats sind berechtigt

- der TSP,
- der Endanwender,
- der Zertifikatnehmer und
- Widerrufsberechtigte Dritte.

Gemäß ETSI TS 119 495 4.6 ist die NCA, die den PSP registriert hat, ein Widerrufsberechtigter Dritter. Es wird sicher gestellt, dass der Antrag zum Zertifikatswiderruf tatsächlich durch die NCA veranlasst wurde.

4.9.3. Verfahren für einen Widerrufsantrag (Procedure for revocation request)

Die Authentifizierung der Widerrufsberechtigten erfolgt gemäß Abschnitt 3.4. Nicht authentifizierte Widerrufsanträge werden verworfen, solange kein berechtigter Grund für einen Widerruf im Antrag angegeben wurde. Existiert ein berechtigter Grund, wird der Antrag bearbeitet und gemäß 4.9.5 umgesetzt.

Anträge auf Widerruf von Zertifikaten werden durch Validation Specialists geprüft, woraufhin Kontakt mit dem Zertifikatnehmer aufgenommen wird.

Treten Incidents oder Certificate Problem Reports auf, so wird der BVtrust-Leiter durch das Incident-Management umgehend benachrichtigt. Certificate Problem Reports und Incidents werden umgehend, unter Einbeziehung des Zertifikatnehmers, insofern die Benachrichtigung des Zertifikatsnehmers notwendig und der Zertifikatnehmer erreichbar ist, bearbeitet.

Ist der Zertifikatnehmer nicht zu erreichen oder wird zwischen dem TSP und dem Zertifikatnehmer keine Einigung über das weitere Verfahren erreicht, so obliegt die Entscheidung über das weitere Vorgehen dem BVtrust-Leiter.

Die Entscheidung eines Widerrufs wird vom Leiter BVTrust getroffen, wenn diese nicht durch den Zertifikatnehmer beantragt wird. Im Falle der Beantragung durch den Zertifikatnehmer wird das Zertifkat auf jeden Fall widerrufen.

Der Widerruf sowie die vom Widerrufsantragsteller angegebenen Widerrufsgründe werden mittels eines automatisch erzeugten Widerrufsprotokolls dokumentiert. Ferner wird der Zertifikatnehmer über den Widerruf informiert, sofern möglich.

Der Widerruf eines Zertifikats kann nicht rückgängig gemacht werden. Die Antragstellung für einen zukünftigen Widerruf von Zertifikaten wird nicht angeboten.

4.9.4. Fristen für einen Widerrufsantrag (Revocation request grace period)

Zertifikatnehmer und Endanwender haben Zertifikate unverzüglich zu widerrufen, wenn Gründe für einen Widerruf vorliegen.

4.9.5. Zeitspanne für die Bearbeitung des Widerrufsantrags (Time within which CA must process the revocation request)

Eintreffende Widerrufsanträge werden nach erfolgreicher Authentifizierung unverzüglich bearbeitet und innerhalb von 24 Stunden entschieden und umgesetzt. Ausgenommen von dieser Frist sind berechtigte, jedoch nicht gemäß 4.9.3 authentifizierte Widerrufsanträge durch eine NCA.

Widerrufe sind nach Durchführung unverzüglich, jedoch spätestens nach 60 Minuten, über OCSP abrufbar.

4.9.6. Methoden zum Prüfen von Widerrufsinformationen (Revocation checking requirement for relying parties)

Widerrufinformationen können über einen Statusabfragedienst abgefragt werden. Die Adresse des Dienstes ist Teil des Zertifikats.

4.9.7. Häufigkeit der Veröffentlichung von Widerrufslisten (CRL issuance frequency (if applicable))

Es werden keine öffentlichen Widerrufslisten erstellt.

4.9.8. Maximale Latenzzeit für Widerrufslisten (Maximum latency for CRLs (if applicable))

Siehe 4.9.7.

4.9.9. Online-Verfügbarkeit von Widerrufsinformationen (On-line revocation/status checking availability)

Zur Onlineprüfung steht ein Statusabfragedienst zur Verfügung. Genaue Informationen sind dem Abschnitt 4.10 zu entnehmen.

4.9.10. Notwendigkeit zur Online-Prüfung von Widerrufsinformationen (On-line revocation checking requirements)

Um einem Zertifikat vertrauen zu können, muss die Gültigkeit des Zertifikats wurde über den Statusabfragedienst (OCSP) bestätigt werden.

Es gilt Abschnitt 4.5.2.

4.9.11. Andere Formen zur Anzeige von Widerrufsinformationen (Other forms of revocation advertisements available)

Es existieren keine anderen Formen zur Anzeige von Widerrufsinformationen.

4.9.12. Spezielle Anforderungen bei Kompromittierung des privaten Schlüssels (Special requirements re key compromise)

Bei Kompromittierung eines privaten CA-Schlüssels wird die Bundesnetzagentur als Verwalter der Trusted List unverzüglich informiert. Weitere Schritte werden mit der Bundesnetzagentur und dem Bundesamt für Sicherheit in der Informationstechnik nach 5.7.3. abgestimmt und das weitere Vorgehen besprochen.

Wenn ein privater Schlüssel eines EE-Zertifikats kompromittiert wurde, so muss dies dem TSP unverzüglich mitgeteilt werden. Das dazugehörige Zertifikat wird widerrufen und der private Schlüssel darf durch den Endanwender nicht mehr verwendet werden.

4.9.13. Suspendierung des Zertifikats (Circumstances for suspension)

Die Suspendierung des Zertifikats ist nicht vorgesehen.

4.10. Statusabfragedienst (Certificate status services)

4.10.1. Funktionsweise des Statusabfragedienstes (Operational characteristics)

Der Statusabfragedienst ist über das Protokoll OCSP nach RFC 6960 verfügbar. Die Erreichbarkeit des Dienstes wird als URL in den Zertifikaten angegeben. Der Statusabfragedienst ist hochverfügbar und wird in den redundant ausgelegten Rechenzentren des TSP betrieben, um einen Ausfall des Dienstes zu verhindern. Der TSP wird Störungen des Statusabfragedienstes im Rahmen der bestehenden technischen und betrieblichen Möglichkeiten spätestens nach 12 Stunden beseitigen.

Die Systemzeit des OCSP-Responder wird stetig gegen die offizielle Zeit synchronisiert.

Es wird für Anfragen an den Statusabfragedienst kein Stapling verwendet.

Weitere Informationen sind im Abschnitt 7 beschrieben.

4.10.2. Verfügbarkeit des Statusabfragedienstes (Service availability)

Der Statusabfragedienst ist 24 Stunden an 7 Tagen der Woche verfügbar.

4.10.3. Optionale Leistungen (Optional features)

Keine.

4.11. Beendigung des Zertifizierungsdienstes (End of subscription)

Die Verträge können vom TSP und dem Zertifikatnehmer gemäß der jeweiligen vertraglichen Vereinbarungen gekündigt werden.

Der TSP verfügt über einen fortlaufend aktualisierten Beendigungsplan, in dem Einzelheiten für den Fall der Einstellung der Tätigkeit niedergelegt sind.

Der TSP benachrichtigt Endanwender, Zertifikatnehmer und die zuständigen Aufsichtsbehörde rechtzeitig, mindestens aber zwei Monate vorher, über die Einstellung des Zertifizierungs- und Vertrauensdienstes per E-Mail. Relying Parties werden über die Website des TSP informiert.

Der TSP widerruft alle noch gültigen Zertifikate zum Zeitpunkt der Beendigung des Zertifizierungsdienstes. Alle privaten Schlüssel der betroffenen CAs werden unwiderruflich zerstört, sodass sichergestellt ist, dass eine Zertifizierung nicht mehr möglich ist.

4.12. Schlüsselhinterlegung und -wiederherstellung (Key escrow and recovery)

4.12.1. Bedingungen und Verfahren für die Hinterlegung und Wiederherstellung privater Schlüssel (Key escrow and recovery policy and practices)

Es wird keine Hinterlegung und Wiederherstellung von privaten Schlüsseln angeboten, da sich diese privaten Schlüssel zu jedem Zeitpunkt im Besitz des Endanwenders befinden.

4.12.2. Bedingungen und Verfahren für die Hinterlegung und Wiederherstellung von Sitzungsschlüsseln (Session key encapsulation and recovery policy and practices)

Das Hinterlegen und Wiederherstellen von Sitzungsschlüsseln wird nicht angeboten.

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

Die Beschreibungen dieses Kapitels beziehen sich auf die betriebene Infrastruktur, die beim TSP im Rahmen von eIDAS-VO, VDG, VDV, ETSI EN 319 401, ETSI EN 319 411-1 sowie ETSI EN 319 411-2 betrieben wird.

5.1. Bauliche Sicherheitsmaßnahmen (Physical controls)

Für die baulichen Sicherheitsmaßnahmen liegt eine detaillierte Dokumentation vor, die bei begründetem Interesse in den relevanten Teilen eingesehen werden kann. Das Sicherheitskonzept wurde durch eine anerkannte Konformitätsbewertungsstelle nach Artikel 3, Nr. 18 der Verordnung (EU) Nr. 910 /2014 geprüft. Die Prüfung und Bestätigung wird gemäß eIDAS-VO, VDG, VDV, ETSI EN 319 401, ETSI EN 319 411-1 sowie ETSI EN 319 411-2 regelmäßig wiederholt.

Ferner wurde dem Sicherheitsbereich des TSPs durch den TÜV-IT die Anwendung und Umsetzung der „Infrastrukturmaßnahmen für hohen Schutzbedarf – Level 3“ beurkundet. Mit diesem TÜV-IT-Zertifikat „Trusted Site Infrastructure“ werden alle infrastrukturrelevanten Aspekte bewertet. Diese Prüfung wird alle zwei Jahre wiederholt. Das genannte Zertifikat bestätigt, dass die Bank-Verlag GmbH diesen hohen Sicherheitsstandard der nicht-technischen Sicherheitsmaßnahmen einhält.

5.2. Verfahrensvorschriften (Procedural controls)

5.2.1. Rollenkonzept (Trusted roles)

Das implementierte und im Sicherheitskonzept dokumentierte Rollenkonzept sieht eine Aufteilung in operative, administrative, führende und auditierende Rollen vor. Personen, die in vertrauenswürdige Rollen des TSP berufen werden, müssen frei von Interessenkonflikten oder anderen Einflüssen sein, die geeignet sind, das Vertrauen des TSPs erheblich zu beeinträchtigen. Alle Mitarbeiter erhalten durch einen definierten Prozess die Rollen, die zum Ausüben der Tätigkeit notwendig sind. Ein Rollenausschlussprinzip garantiert, dass keine einzelne Person sicherheitsrelevante Änderungen vornehmen oder unberechtigt Zertifikate ausstellen kann.

5.2.2. Mehraugenprinzip (Number of persons required per task)

Sicherheitskritische Vorgänge müssen grundsätzlich mindestens im Vier-Augen-Prinzip erfolgen. Dies wird durch technische und organisatorische Maßnahmen umgesetzt.

5.2.3. Identifizierung und Authentifizierung für einzelne Rollen (Identification and authentication for each role)

Das Rollenkonzept wird durch technische und organisatorische Maßnahmen, wie beispielsweise Zutrittsberechtigungen und Abfrage von Wissen, durchgesetzt. Die durchführende Person muss sich, bevor sie Zugriff auf sicherheitskritische Anwendungen erhält, erfolgreich authentifizieren. Über Event-Logs kann die durchführende Person nachträglich einer Aktion zugeordnet werden; sie ist rechenschaftspflichtig.

5.2.4. Rollenausschlüsse (Roles requiring separation of duties)

Das Rollenkonzept sieht diverse Rollenausschlüsse vor, um Interessenskonflikte zu verhindern. Des Weiteren sieht das Rollenkonzept vor, das Mehraugenprinzip zu erzwingen und schädlichem Handeln vorzubeugen.

5.3. Personalkonzept (Personnel controls)

5.3.1. Qualifikation, Erfahrung und Zuverlässigkeit des Personals (Qualifications, experience, and clearance requirements)

Der Leiter des Trustcenters trägt in der Besetzung der Rollen dafür Sorge, dass Mitarbeiter mit den notwendigen Kenntnissen und Erfahrungen zur Ausübung der Tätigkeit eingesetzt werden, die durch Prüfung des Personalausweises korrekt identifiziert wurden.

5.3.2. Sicherheitsüberprüfung (Background check procedures)

Alle Mitarbeiter des TSP müssen vor Stellenantritt unter anderem ein polizeiliches Führungszeugnis vorlegen. Die Vorlage einer aktuellen Fassung des Führungszeugnisses muss in regelmäßigen Abständen wiederholt werden.

5.3.3. Schulungen und Weiterbildungen (Training requirements)

Der TSP erfüllt die Anforderungen aus ETSI EN 319 411-1 und ETSI EN 319 401 bzgl. der Schulung und Weiterbildung des Personals des TSP.

5.3.4. Häufigkeit von Schulungen und Belehrungen (Retraining frequency and requirements)

Alle Mitarbeiter des TSP unterliegen mindestens alle 12 Monate einer Security-Awareness-Schulung.

5.3.5. Häufigkeit und Folge von Arbeitsplatzrotation (Job rotation frequency and sequence)

Es sind keine Arbeitsplatzrotationen bzw. Rollenwechsel vorgesehen.

5.3.6. Maßnahmen bei unerlaubten Handlungen (Sanctions for unauthorized actions)

Es sind Maßnahmen implementiert, die die Einhaltung der Rollenanweisung kontrollieren. Unerlaubte Handlungen können zudem arbeitsrechtliche und strafrechtliche Konsequenzen haben. In jedem Fall werden mindestens vorübergehend alle Zugänge zu der Infrastruktur entzogen.

5.3.7. Anforderungen an freie Auftragnehmer (Independent contractor requirements)

Externe Dienstleister, die Aufgaben innerhalb des Trust Services übernehmen, müssen sich an alle gesetzlichen Regeln und Normen halten. Weiterhin müssen alle Dienstleister, die Aufgaben innerhalb des Trust Services übernehmen, von einem unabhängigen Dritten zertifiziert und akkreditiert sein.

Zudem sollte ein Vertragsverhältnis zwischen dem TSP und dem externen Dienstleister bestehen, welches entsprechende Pflichten, die die Bereitstellung des Teilservice betreffen, delegiert.

5.3.8. Ausgehändigte Dokumentation (Documentation supplied to personnel)

Folgende Dokumentationen werden dem Personal zur Verfügung gestellt:

- Sicherheitskonzept
- Rollenbeschreibung und Arbeitsanweisungen
- CP/CPS/PDS

- Betriebs- und Fachkonzepte
- Spezifikationen
- Sicherheitsrichtlinie der Bank-Verlag GmbH

Das Personal wird per E-Mail über Änderungen an CP und CPS informiert.

5.4. Protokollierung von Überwachungsmaßnahmen (Audit logging procedures)

5.4.1. Überwachung des Zutritts

Der TSP betreibt umfangreiche Überwachungsmaßnahmen. Alle Zutritte zu den sicherheitsrelevanten Bereichen des TSP sind nur durch autorisiertes Personal möglich und werden protokolliert sowie über den Zeitraum eines Jahres gespeichert. Der Zutritt durch Gäste ist nur in Begleitung von zugriffsberechtigten Mitarbeitern möglich und wird ebenfalls protokolliert.

5.4.2. Überwachung von organisatorischen Maßnahmen

Die organisatorischen Maßnahmen, die zum sicheren Betrieb des Trustcenters notwendig sind, werden regelmäßig durch den TSP-Leiter überprüft. Alle Änderungen dieser Maßnahmen werden im Sicherheitskonzept dokumentiert.

5.5. Datenarchivierung (Records archival)

5.5.1. Art der archivierten Datensätze (Types of records archived)

Es wird zwischen Aufzeichnungen in elektronischer Form und papierbasierten unterschieden. Archiviert werden die vollständigen Antragsunterlagen (auch Folgeanträge), Dokumente zu Verfahrensrichtlinien (CP, CPS), PDS, Zertifikate, Widerrufsdokumentation, elektronische Dateien und Protokolle zum Zertifikatslebenszyklus. Dabei werden die Vorgänge zeitlich erfasst. Wenn anwendbar, umfasst dies auch die entsprechenden Systemprotokolle, die im Rahmen der genannten Ereignisse entstehen.

Weiterhin werden sicherheitsrelevante Ereignisse entsprechend aufgezeichnet. Die Systemzeit wird über GPS, DCF77 und NTP täglich gegen die offizielle Zeit synchronisiert.

5.5.2. Aufbewahrungszeiten (Retention period for archive)

Dokumente zur Antragstellung und Prüfung, Daten zum Zertifikatslebenszyklus, Widerrufsinformationen sowie die Zertifikate selbst werden für die gesamte Betriebszeit des TSP aufbewahrt. Wird der Betrieb eingestellt, werden alle dienstspezifischen Dokumente und Daten unbefristet im Archiv des TSP vorgehalten.

Wenn anwendbar, umfasst dies auch die entsprechenden Systemprotokolle, die im Rahmen der genannten Ereignisse entstehen.

5.5.3. Archivsicherheit (Protection of archive)

Das Archiv befindet sich in gesicherten Räumen und unterliegt dem Rollen- und Zutrittskontrollkonzept des TSP.

5.5.4. Datensicherung des Archivs (Archive backup procedures)

Die Sicherung der Daten erfolgt nach dem Stand der Technik.

5.5.5. Anforderungen zum Zeitstempeln von Aufzeichnungen (Requirements for time-stamping of records)

Die Systemzeit der für die Archivierung zuständigen Systeme wird fortlaufend mit der gesetzlich gültigen Zeit abgeglichen.

5.5.6. Ort der Archivierung (Archive collection system (internal or external))

Die Archivierung erfolgt intern beim TSP.

5.5.7. Verfahren zur Beschaffung und Verifikation von Archivinformationen (Procedures to obtain and verify archive information)

Das Verfahren zur Beschaffung und Verifikation von Archivinformationen unterliegt dem Rollenkonzept des TSP.

5.6. Schlüsselwechsel (Key changeover)

Ein Schlüsselwechsel der CA-Schlüssel ist gleichgestellt mit der neuen Generierung einer neuen CA-Instanz. Dieser findet mindestens 2 Jahre vor Ablauf des CA-Zertifikats statt. Sobald das neue CA-Zertifikat erstellt und entsprechend verteilt und veröffentlicht wurde, wird ausschließlich das neue CA-Zertifikat verwendet. Das alte CA-Zertifikat wird nicht mehr zur Ausstellung neuer EE-Zertifikate verwendet. Für EE-Zertifikate sind keine Schlüsselwechsel vorgesehen. Es muss ein neues Zertifikat erstellt werden.

5.7. Notfallkonzept (Disaster Recovery) (Compromise and disaster recovery)

5.7.1. Behandlung von Vorfällen und Kompromittierungen (Incident and compromise handling procedures)

Der TSP verfügt über ein Notfallkonzept sowie einen Wiederanlaufplan, die den beteiligten Rollen bekannt sind und von ihnen im Bedarfsfall umgesetzt werden. Die Verantwortlichkeiten sind klar verteilt und bekannt.

Nachdem dem TSP eine kritische Schwachstelle oder eine Kompromittierung bekannt geworden ist, muss dieser unverzüglich handeln und entsprechende Maßnahmen ergreifen. Je nach Art der Kompromittierung werden in Absprache mit der Aufsichtsbehörde die Auswirkungen analysiert und ggf. weitere Schritte zur Behebung veranlasst.

Der TSP benachrichtigt innerhalb von 24 Stunden nach dem Vorfall die entsprechenden Parteien im Falle von Sicherheitsverletzungen, die erhebliche Auswirkungen auf den bereitgestellten Vertrauensdienst haben.

5.7.2. Wiederherstellung nach Kompromittierung von Ressourcen (Computing resources, software, and /or data are corrupted)

Das Notfallkonzept und der Wiederanlaufplan beschreiben die Durchführung von Recovery-Prozeduren.

5.7.3. Kompromittierung des privaten CA-Schlüssels (Entity private key compromise procedures)

Bei einer Kompromittierung von privaten CA-Schlüsseln wird das Bundesamt für Sicherheit in der Informationstechnik, die Bundesnetzagentur und die BaFin unverzüglich informiert und die betroffenen CA-Zertifikate sowie, sofern notwendig, durch diese ausgestellte EE-Zertifikate widerrufen. Betroffene En danwender und Zertifikatnehmer werden über den Vorfall und dessen Auswirkungen mithilfe der vorliegenden Kontaktdaten aus der Registrierung informiert. Siehe auch 5.7.1.

Aus der Analyse der Gründe für die Kompromittierung werden, wenn möglich, Maßnahmen ergriffen, um zukünftige Kompromittierungen zu vermeiden. Unter Berücksichtigung der Gründe für die Kompromittierung werden neue CA-Signaturschlüssel generiert und neue CA-Zertifikate ausgestellt.

Der gleiche Prozess erfolgt, sobald die verwendeten Algorithmen in Absprache mit der entsprechenden Aufsichtsbehörde als nicht mehr sicher gelten oder die Konformität der zertifizierten HSMs ausläuft bzw. widerrufen wird. Dies betrifft auch alle ausgestellten Zertifikate und deren Schlüssel.

5.7.4. Weiterführung des Betriebs nach Kompromittierung oder Katastrophenfall (Business continuity capabilities after a disaster)

Je nach Art des Vorfalls entscheidet im Notfall der TSP über die Vorgehensweise nach einer Kompromittierung oder nach einem Katastrophenfall. Dieser e ntscheidet, wie der Betrieb wiederaufgenommen werden soll. Wenn der Betrieb wiederaufgenommen wird, entscheidet der TSP, ob eine Wiederherstellung der in Abschnitt 6.2.4 beschriebenen Sicherung der CA durchgeführt werden soll oder ob eine Neuinstallation erforderlich ist oder ob eine Kombination aus beiden Verfahren notwendig ist.

Zuvor wird jedoch sichergestellt, dass geeignete Maßnahmen getroffen wurden, um die Ursachen des Ausfalls oder der Kompromittierung zukünftig auszuschließen.

5.8. Einstellung des Betriebs (CA or RA termination)

Wird der Betrieb des TSP eingestellt, so beendet der TSP alle Zugriffsmöglichkeiten auf die entsprechende CA und den dazugehörigen privaten Schlüssel. Sobald sichergestellt ist, dass alle notwendigen Schritte aus dem Beendigungsplan geschehen sind, wird der zugehörige private CA-Schlüssel im HSM gelöscht. Werden alle Dienste des TSP eingestellt, so wird das HSM physikalisch zerstört. Siehe auch 4.11.

6. Technische Sicherheitskontrollen (TECHNICAL SECURITY CONTROLS)

6.1. Generierung und Installation von Schlüsselpaaren (Key pair generation and installation)

6.1.1. Generierung von Schlüsselpaaren (Key pair generation)

Die Generierung aller Schlüsselpaare im Verantwortungsbereich des TSP geschieht in sicheren, nach FIPS 140-2 Level 3 (oder höher) konformen und zertifizierten Utimaco Cryptoserver-HSMs. Alle HSMs befinden sich im Hochsicherheitsbereich des TSP.

Die CA-Schlüssel werden unter Einhaltung des Rollenkonzepts im Vier-Augen-Prinzip erzeugt. Die Erzeugung von CA-Schlüsseln wird stets durch einen unabhängigen Auditor überprüft und bestätigt. Weiterhin wird die Erstellung von CA-Schlüsseln gemäß ETSI EN 319 411-1 und ETSI EN 319 411-2 dokumentiert.

Die Generierung aller Schlüsselpaare für EE-Zertifikate werden von den Endanwendern durchgeführt und liegen somit im Verantwortungsbereich des Endanwenders. Für die Generierung der Schlüsselpaare ist durch den Endanwender ein nach SOG-IS als sicher geltender Algorithmus zu verwenden.

6.1.2. Auslieferung privater Schlüssel an Zertifikatnehmer (Private key delivery to subscriber)

Es werden keine privaten Schlüssel an Endanwender ausgeliefert, da der TSP die privaten Schlüssel des Endanwenders nicht generiert.

6.1.3. Lieferung öffentlicher Schlüssel an den TSP (Public key delivery to certificate issuer)

Der Endanwender erstellt seinen privaten und öffentlichen Schlüssel selbst und übermittelt den öffentlichen Schlüssel via CSR an den TSP.

6.1.4. Auslieferung der öffentlichen CA-Schlüssel (CA public key delivery to relying parties)

Die CA-Zertifikate, welche die dazugehörigen öffentlichen CA-Schlüssel beinhalten, werden in der nationalen Trusted List, welche durch die Bundesnetzag entur verwaltet wird, und somit auch in der EU Trusted List veröffentlicht. Darüber hinaus werden alle CA-Zertifikate nach ihrer Erstellung auf der Website des TSP veröffentlicht.

6.1.5. Schlüssellängen (Key sizes)

Die CA-Zertifikate des TSP, welche zum Ausstellen von EE-Zertifikaten im Rahmen dieses CPS verwendet werden, verwenden derzeit RSA-Schlüssel mit einer Schlüssellänge von mindestens 4096 bit (siehe 7.1.3).

Für EE-Zertifikate werden derzeit RSA-Schlüssel mit einer Schlüssellänge von mindestens 4096 bit (siehe 7.1.3) verwendet.

Anfragen für Zertifikate mit abweichender Schlüssellänge werden technisch automatisiert abgelehnt.

6.1.6. Festlegung der Schlüsselparameter und Qualitätskontrolle der Parameter (Public key parameters generation and quality checking)

Alle Schlüsselparameter und die eingesetzten HSM richten sich nach der jeweils gültigen Vorgabe aus dem von der Bundesnetzagentur empfohlenen Kryptokatalog sowie der Zertifizierung des HSM. Derzeit muss der SOG-IS-Kryptokatalog befolgt werden. Die Einhaltung dieser Vorgaben wird kontinuierlich vom TSP geprüft.

6.1.7. Schlüsselverwendungen gemäß x.509v3-Erweiterung "key usage" (Key usage purposes (as per X.509 v3 key usage field))

Alle verwendeten Zertifikatserweiterungen sind im Abschnitt 7.1.2 beschrieben.

6.2. Schutz privater Schlüssel und technische Kontrollen kryptographischer Module (Private Key Protection and Cryptographic Module Engineering Controls)

6.2.1. Standards und Sicherheitsmaßnahmen für kryptographische Module (Cryptographic module standards and controls)

Der TSP verwendet ausschließlich zertifizierte HSMs, welche den gesetzlichen Anforderungen und Normen entsprechen (vgl. Abschnitt 6.1). Diese werden gemäß der Zertifizierung in einer gesicherten Umgebung betrieben (vgl. Abschnitt 5.1). Die HSMs sind durch technische sowie organisatorische Maßnahmen vor Zugriffen Unbefugter geschützt. Die HSMs werden überprüft und während des gesamten Lebenszyklus der HSMs gegen Kompromittierung überwacht . Bei Gerätestilllegung oder im RMA-Fall werden alle sensitiven und nicht-sensitiven Daten auf dem HSM gelöscht, bevor es die sichere Umgebung verlässt.

6.2.2. Mehraugen-Zugriffssicherung zu privaten Schlüsseln (Private key (n out of m) multi-person control)

Der Zugriff auf den privaten CA-Schlüssel sowie dessen Aktivierung durch das RA-Personal ist ausschließlich im Vier-Augen-Prinzip möglich.

Die Zugriffssicherung zu den privaten Schlüsseln für EE-Zertifikate erfolgt im Verantwortungsbereich des Endanwenders.

6.2.3. Hinterlegung von privaten Schlüsseln (Private key escrow)

Es wird keine Hinterlegung privater Schlüssel angeboten.

6.2.4. Sicherung von privaten Schlüsseln (Private key backup)

Alle privaten Schlüssel der CAs werden verschlüsselt gesichert. Um dieses Backup wiederherzustellen, ist ein Prozess mit mehreren Personen aus verschiedenen Rollen, die für diese Tätigkeit autorisiert sind, notwendig und findet in der sicheren Umgebung des TSP statt. Weitere Kopien privater CA-Schlüssel existieren nicht.

Die Verantwortung für das Backup des privaten Schlüssels eines EE-Zertifikats obliegt dem jeweiligen Endanwender.

6.2.5. Archivierung privater Schlüssel (Private key archival)

Private Schlüssel werden nicht archiviert.

6.2.6. Übertragung privater Schlüssel in oder aus kryptographischen Modulen (Private key transfer into or from a cryptographic module)

Eine Übertragung privater CA-Schlüssel in das oder aus dem HSM erfolgt nur zu Backup- und Wiederherstellungszwecken. Ein Vier-Augen-Prinzip wird technisch und kryptographisch erzwungen. Bei Export/Import in ein anderes HSM schützt eine Verschlüsselung den privaten CA-Schlüssel.

6.2.7. Speicherung privater Schlüssel auf kryptographischen Modulen (Private key storage on cryptographic module)

Die privaten CA-Schlüssel werden verschlüsselt im HSM gespeichert. Eine Extraktion der Schlüssel aus dem HSM ist technisch nicht möglich. Eine Speicherung der privaten Schlüssel findet nur zu Backup-Zwecken statt. Der Prozess wird in 6.2.4 dieses CPS beschrieben.

6.2.8. Aktivierung privater Schlüssel (Method of activating private key)

Private CA-Schlüssel werden gemäß Abschnitt 6.2.2 aktiviert.

Der private Schlüssel von Endanwenderzertifikaten wird einmalig durch Hinterlegen des Zertifikates für die Domain aktiviert.

6.2.9. Deaktivierung privater Schlüssel (Method of deactivating private key)

Private Schlüssel sind immer deaktiviert, sofern diese nicht nach 6.2.8 aktiviert wurden.

6.2.10. Vernichtung privater Schlüssel (Method of destroying private key)

Alle privaten Schlüssel im Verfügungsbereich des TSP werden bei Widerruf des zugeordneten Zertifikats oder Beendigung des Betriebs vernichtet.

Die Vernichtung der privaten Schlüssel im Verfügungsbereich des Endanwenders kann nicht durch den TSP überprüft und überwacht werden.

Anmerkung: Die Gültigkeit von Zertifikaten ist über einen hochverfügbaren Abfragedienst abrufbar. Sollte eine Entität versuchen, ein ungültiges EE-Zertifikat mit zugehörigem Private Key zu verwenden, so kann ein Dritter feststellen, dass dieses Zertifikat zwar zum zugehörigen Public Key / Zertifikat gehört, aber ebenso, dass dieses Zertifikat ungültig ist.

6.2.11. Beschreibung der kryptografischen Module (Cryptographic Module Rating)

Der TSP betreibt geeignete und zertifizierte HSMs zur Schlüsselgenerierung. Die eingesetzten HSMs sind zu FIPS 140-2 Level 3 konform. Der TSP überwacht den Zertifizierungsstatus der HSMs. Sollte die Zertifizierung der HSMs zurückgezogen werden, wird dieser Umstand durch den TSP-Leiter und ggf. anderen Parteien wie der Konformitätsbewertungsstelle oder dem Bundesamt für Sicherheit in der Informationstechnik bewertet. Aus dieser Bewertung resultierende Maßnahmen werden entsprechend durchgeführt.

6.3. Weitere Aspekte der Verwaltung von Schlüsselpaaren (Other aspects of key pair management)

6.3.1. Archivierung öffentlicher Schlüssel (Public key archival)

Alle ausgestellten Zertifikate werden für die gesamte Betriebszeit des TSP archiviert.

6.3.2. Gültigkeitsdauer von Zertifikaten und Schlüsselpaaren (Certificate operational periods and key pair usage periods)

Die Gültigkeitsdauer der CA-Zertifikate ist variabel und dem Zertifikat zu entnehmen. Die maximale Gültigkeitsdauer beträgt 15 Jahre. Es werden keine Zertifikate durch die CA ausgestellt, welche eine längere Gültigkeitsdauer als das auszustellende CA-Zertifikat haben.

Die Gültigkeitsdauer der OCSP-Zertifikate ist variabel und dem Zertifikat zu entnehmen. Die maximale Gültigkeitsdauer beträgt zwei Jahre.

Die Gültigkeitsdauer der EE-Zertifikate ist variabel und dem Zertifikat zu entnehmen. Die maximale Gültigkeitsdauer beträgt zwei Jahre.

6.4. Aktivierungsdaten (Activation data)

6.4.1. Generierung und Installation von Aktivierungsdaten (Activation data generation and installation)

Die manuelle Aktivierung privater Schlüssel von CA-Zertifikaten ist nur nach erfolgreicher Zwei-Faktor-Authentifizierung sowie im Vier-Augen-Prinzip möglich. Die Autorisierung des TSP-Personals erfolgt durch die TSP-Leitung.

Die Aktivierung privater Schlüssel von EE-Zertifikaten geschieht durch den Endanwender. Der Besitznachweis des privaten Schlüssels wird in 3.2.2. näher beschrieben.

6.4.2. Schutz von Aktivierungsdaten (Activation data protection)

Die Aktivierungsdaten müssen durch die entsprechende Person sicher verwahrt werden (geistige Aktivierungsdaten) oder durch physische Maßnahmen gesichert werden (Smartcards, HSMs oder ähnliches).

6.4.3. Weitere Aspekte von Aktivierungsdaten (Further aspects of activation data)

Nicht anwendbar.

6.5. Computer-Sicherheitsmaßnahmen (Computer security controls)

6.5.1. Spezifische technische Sicherheitsanforderungen an Computer (Specific computer security technical requirements)

Alle IT-Komponenten, welche im Rahmen von BVtrust verwendet werden, sind mittels verschiedener technischer und organisatorischer Maßnahmen gesichert, sodass diese Systeme ausschließlich für den designierten Zweck verwendet werden können. Außerdem ist sichergestellt, dass die Systeme konform zum Sicherheitskonzept und nicht im Widerspruch zur CP, CPS, ETSI EN 319 401, ETSI EN 319 411-2 und ETSI TS 119 495 sowie betrieben werden.

Alle Mitarbeiter des TSP müssen die Arbeitsanweisungen der Vorgaben zur Computersicherheit einhalten. Eine Wiederverwendung von Datenträgern, die sensitive Daten enthalten, ist ausgeschlossen, da diese Datenträger nach Ende des dienstspezifischen Verwendungszwecks vernichtet werden. Defekte Datenträger werden nach einem sicheren Verfahren zerstört. Mitarbeiter des TSP sind gemäß den geltenden gesetzlichen Bestimmungen für ihr Handeln verantwortlich.

Es wird sichergestellt, dass sicherheitsrelevante Softwareupdate in angemessener Zeit auf den betroffenen Systemen eingespielt werden. Die angemessene Zeit richtet sich nach der Kritikalität des Fehlers im betroffenen Systems. Sollten Gründe existieren, die einem Update widersprechen, so müssen diese dokumentiert und dem Risikomanagement des TSP übergeben werden.

Security Patches, die als hochriskant eingestufte Sicherheitslücken beheben, werden nach entsprechender Risikobewertung auch außerhalb der zuvor definierten Zeitintervalle und damit zeitnah auf den betroffenen Systemen eingespielt.

Alle Endanwender müssen ihrerseits sicherstellen, dass für alle IT-Komponenten, die im Verfügungsbereich des Endanwenders stehen und die im Rahmen des Zertifizierungsdienstes verwendet werden, ausschließlich vertrauenswürdige Computer und Software verwendet werden.

6.5.2. Bewertung der Computersicherheit (Computer security rating)

Alle eingesetzten Systeme, die private Schlüssel von CA-Zertifikaten verarbeiten, werden durch eine anerkannte Konformitätsbewertungsstelle regelmäßig geprüft und werden durch entsprechendes Monitoring stetig überwacht.

6.6. Technische Kontrollen während des Lebenszyklus (Life cycle technical controls)

6.6.1. Sicherheitsmaßnahmen bei Entwicklung und Erweiterung der IT-Systeme und Softwarekomponenten (System development controls)

Während der Entwurfs- und Entwicklungsphase aller vom TSP oder im Auftrag des TSP durchgeführter Systementwicklungsprojekte werden die Sicherheitsanforderungen analysiert und entsprechend umgesetzt.

6.6.2. Sicherheitsmaßnahmen beim Computermanagement (Security management controls)

Ausschließlich autorisiertes Personal darf die TSP-Systeme administrieren. Durch ein entsprechendes Rollenkonzept ist festgelegt, unter welchen Voraussetzungen dies erlaubt ist (bspw. Mehraugenkonzept). Durch entsprechendes Monitoring können Regelverletzungen und andere Vorfälle erkannt werden.

6.6.3. Sicherheitsmaßnahmen während des Betriebs (Life cycle security controls)

Alle IT-Systeme, die im Rahmen von BVtrust verwendet werden, werden überwacht und mit regelmäßigen Systemchecks überprüft. Bei Entdeckung sicher heitsrelevanter Ereignisse wird das Ereignis durch das Sicherheitsmanagement geprüft und bewertet. Je nach Bewertung wird das Ereignis entsprechend behandelt. Zu jedem Zeitpunkt wird sichergestellt, dass keine sensiblen Daten zugänglich gemacht werden. Darüber hinaus werden alle sicherheitsrelevanten Prozesse sowie Zugriffe der Mitarbeiter und Zugriffsversuche protokolliert. Protokolliert werden in dem Zusammenhang

- Start und Beendigung der relevanten IT-Systeme (insbesondere Firewall, Netzwerkkomponenten, HSMs, CA-Systeme),
- Systemabstürze,
- Ausfall von Hardware und
- Zugriffsversuche auf das PKI-System.

Alle sicherheitsrelevanten Protokollierungen bzw. Logs, insbesondere der CA-Systeme sowie der HSMs, werden in der Art und Weise gesichert, dass eine Löschung des gesamten Logs oder auch einzelner Einträge im Log entweder nicht oder nur im Mehraugenprinzip möglich ist. Die Logs werden über die gesamte Betriebszeit der CA, d.h. bis zur Einstellung des Betriebes aufbewahrt.
Das maximale Intervall zwischen zwei Überprüfungen der Systemkonfiguration beträgt ein Jahr.

Es wird ausschließlich vertrauenswürdige Software aus gesicherten Quellen verwendet. Sobald sicherheitskritische Fehler allgemein bekannt werden, wird der Fehler in angemessener Zeit behoben bzw. werden sicherheitsrelevante Updates eingespielt. Jede Änderung an Software wird vorab in einer Testumgebung ausgiebig getestet, so dass schwerwiegende Fehler, die durch ein Update entstehen könnten, minimiert werden.

Alle Daten werden redundant gesichert, sodass Datenverluste aufgrund alternder Datenträger vermieden werden. Besonders kritische Daten wie Verschlüsselungsschlüssel für private Schlüssel und ähnliche sensible Daten, welche nicht automatisch synchronisiert werden, können im Rahmen einer Notfallwiederherstellung im Vier-Augen-Prinzip wiederhergestellt werden.

Der TSP lässt regelmäßig Schwachstellenscans und Penetrationstests durch einen unabhängigen und fachkundigen Dritten durchführen. Alle Ergebnisse werden protokolliert und analysiert. Wenn Schwachstellen bei diesen Tests bekannt werden, werden diese bewertet und behoben, soweit dies erforderlich ist.

6.7. Netzwerksicherheit (Network security controls)

Die IT-Systeme des TSP werden durch Firewalls geschützt. Es existieren verschiedene Netzwerkzonen mit unterschiedlichen Sicherheitsleveln. Je nach Sicherheitslevel ist die jeweilige Zone durch mehrere Firewallsysteme geschützt. Das Netzwerk wird regelmäßig durch anerkannte Konformitätsbewertungs stellen sowie Penetrationstests geprüft. Werden in dem Zusammenhang Schwachstellen bekannt, werden diese bewertet und zeitnah behoben.

Nach signifikanten Änderungen der Systeme werden erneut Schwachstellenscans und Penetrationstests durchgeführt.

6.8. Zeitstempel (Time-stamping)

Der TSP betreibt keinen Zeitstempeldienst.

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

7.1. Zertifikatsprofil (Certificate profile)

Um Compliance zu RFC5280 und CA/B BRG zu gewährleisten, entspricht

issuerDN-CA-Zertifikat = subjectDN-CA-Zertifikat = issuerDN-EE-Zertifikat | mit DN = distinguishedName

mit folgenden Werten:

Feld	OID	Kritisch	Beschreibung	Wert
issuerDN-CA-Zertifikat subjectDN-CA-Zertifikat issuerDN-EE-Zertifikat			Aussteller des Zertifikats (TSP)	CN=BVtrust PSD2 QWAC CA R2019 OU=BVtrust O=Bank-Verlag GmbH C=DE

7.1.1. Versionsnummern (Version number(s))

Die Zertifikate werden im Format X.509v3 und gemäß ETSI EN 319 411-1, ETSI TS 119 495 und ETSI EN 319 412-4 ausgegeben. ETSI EN 319 412-4 verweist seinerseits auf geforderte Zertifikatsprofile, die in den CA/Browser Forum Baseline Requirements und CA/B Extended Validation Guidelines genau definiert sind.

7.1.2. Zertifikatserweiterungen (Certificate extensions)

7.1.2.1. CA-Zertifikate

CA-Zertifikate erhalten die folgende Erweiterung:

Feld	OID	Kritisch	Beschreibung	Wert
keyUsage	2.5.29.15	ja	Verwendungszweck	keyCertSign
basicConstraints	2.5.29.19	ja	Beschränkung Verwendung ausgestellter Zertifikate	cA=TRUE, pathLenConstraint=0
authorityKeyIdentifier	2.5.29.35	nein	Identifizierung des öffentlichen Schlüssels des Ausstellers	
subjectKeyIdentifier	2.5.29.14	nein	Identifizierung des öffentlichen Schlüssels des Inhabers	
certificatePolicies	2.5.29.32	nein	Referenzierung zur zugehörigen CP	CP policyIdentifier=1.3.6.1.4.1.50833.1.2.2 policyQualifier:policyQualifierId=1.3.6.1.5.5.7.2.1 policyQualifier= https://www.bank-verlag.de/bvtrust-psd2-qwac

Ergänzende Erweiterungen können aufgenommen werden, müssen RFC 5280, RFC 6960 und RFC 6818 entsprechen oder in einem referenzierten Dokument beschrieben sein.

7.1.2.2. OCSP-Zertifikate

OCSP-Zertifikate erhalten die folgende Erweiterung:

Feld	OID	Kritisch	Beschreibung	Wert
keyUsage	2.5.29.15	ja	Verwendungszweck	digitalSignature
extendedKeyUsage	2.5.29.37	nein	Erweiterter Verwendungszweck	1.3.6.1.5.5.7.3.9 (ocspSigning)
basicConstraints	2.5.29.19	ja	Beschränkung Verwendung ausgestellter Zertifikate	Ca=FALSE, pathLenConstraint=None
authorityKeyIdentifier	2.5.29.35	nein	Identifizierung des öffentlichen Schlüssels des Ausstellers	
subjectKeyIdentifier	2.5.29.14	nein	Identifizierung des öffentlichen Schlüssels des Inhabers	
certificatePolicies	2.5.29.32	nein	Referenzierung zur zugehörigen CP	CP policyIdentifier=1.3.6.1.4.1.50833.1.2.2 policyQualifier:policyQualifierId=1.3.6.1.5.5.7.2.1 policyQualifier= https://www.bank-verlag.de/bvtrust-psd2-qwac
ocspNoCheck	1.3.6.1.5.5.7.48.1.5	nein		NULL

Ergänzende Erweiterungen können aufgenommen werden, müssen RFC 5280, RFC 6960 und RFC 6818 entsprechen oder in einem referenzierten Dokument beschrieben sein.

7.1.2.3. EE-Zertifikate für Website-Zertifikate

Feld	OID	Kritisch	Erforderlich	Beschreibung	Wert
keyUsage	2.5.29.15	ja	muss	Verwendungszweck	digitalSignature, keyEncipherment
extendedKeyUsage	2.5.29.37	nein	muss	erweiterter Verwendungszweck	1.3.6.1.5.5.7.3.1 (id-kp-serverAuth) AND 1.3.6.1.5.5.7.3.2 (id-kp-clientAuth)
basicConstraints	2.5.29.19	ja	muss	Beschränkung Verwendung ausgestellter Zertifikate	CA=FALSE
subjectKeyIdentifier	2.5.29.14	nein	muss	Identifizierung des öffentlichen Schlüssels des Inhabers	Hash
authorityKeyIdentifier	2.5.29.35	nein	muss	Identifizierung des öffentlichen Schlüssels des Ausstellers	Hash
authorityInfoAccess	1.3.6.1.5.5.7.1.1	nein	muss	Verweis auf Zertifikat und OCSP-Dienst Aussteller	calssuers= http://ocsp.bank-verlag.de/cacert?sHash=<*searchKey of issuer as defined in RFC4387*> ocsp= http://ocsp.bank-verlag.de/
certificatePolicies	2.5.29.32	nein	muss	Verweis auf gültige Policy	policyIdentifier = 0.4.0.194112.1.4 (qcp-web) ---------- policyIdentifier=1.3.6.1.4.1.50833.1.2.2 policyQualifier:policyQualifierId=1.3.6.1.5.5.7.2.1 policyQualifier:qualifier:cPSuRI= https://www.bank-verlag.de/bvtrust-psd2-qwac

qcStatements	1.3.6.1.5.5.7.1.3	nein	muss	Geben Auskunft über explizite Eigenschaften des Zertifikats	id-qcs-pkixQCSyntax-v2=1.3.6.1.5.5.7.11.2 id-qcs-pkixQCSyntax-v2:id-etsi-qcs-SemanticsId-Legal=0.4.0.194121.1.2 () qcPDS= 0.4.0.1862.1.5 (id-etsi-qcs-QcPDS) https://www.bank-verlag.de/bvtrust-psd2-qwac QcCompliance= 0.4.0.1862.1.1 (id-etsi-qcs-QcCompliance) QCType = 0.4.0.1862.1.6 QCType:id-etsi-qct-web =0.4.0.1862.1.6.3 etsi-psd2-qcStatement = 0.4.0.19495.2 (id-etsi-psd2-qcStatement) inklusive RolesOfPSP: RoleOfPsp = 0.4.0.19495.1 PSP_AS = 0.4.0.19495.1.1 PSP_PI = 0.4.0.19495.1.2 PSP_AI = 0.4.0.19495.1.3 PSP_IC = 0.4.0.19495.1.4 NCAName: NCAName := UTF8String (SIZE (1..256)) NCAId: NCAId := UTF8String (SIZE (1..256))
subjectAltName	2.5.29.17	nein	muss	Verweis auf Subject Alternative Name	Jeder Eintrag muss ein FQDN sein. Der im Zertifikatsfeld subject:commonName eingetragene FQDN muss im subjectAltName als dNSName eingetragen werden. Leere Domain-Namen und Domain-Namen, die Unterstriche beinhalten, sind in ausgestellten Zertifikaten nicht erlaubt. Wildcard-Zertifikate werden nicht ausgestellt.

Ergänzende Erweiterungen können aufgenommen werden, müssen RFC 5280, RFC 6960, RFC 6818 und ETSI EN 319 412-1 bis -5 entsprechen oder in einem referenzierten Dokument beschrieben sein.

7.1.3. Objekt-Kennungen (OIDs) von Algorithmen (Algorithm object identifiers)(unbearbeitet)

In den CA-, OCSP-, und EE-Zertifikaten werden derzeit folgende Signatur- und Hash-Algorithmen verwendet:

OID	Beschreibung
1.2.840.113549.1.1.11	sha256RSA

7.1.4. Namensformen (Name forms)

In den Feldern *subject* und *issuer* werden Namen nach X.501 als DistinguishedName vergeben. Es werden die Attribute aus Abschnitt 3.1.4 sowie 7.1 vergeben.

Im Feld SubjectAltName (Alternativer Endanwendername) können Namen gemäß [RFC 5280], [RFC 6818] (kodiert als IA5String) stehen.

7.1.5. Namensbeschränkung (Name constraints)

Die Erweiterung *NameConstraints* wird nicht benutzt.

7.1.6. Object Identifier für Zertifizierungsrichtlinien (Certificate policy object identifier)

Die Erweiterung *CertificatePolicies* enthält die OIDs der unterstützten CP. EE-Zertifikate enthalten in der Erweiterung *CertificatePolicies* zusätzlich die OID der Policy QCP-w aus ETSI EN 319 411-2.

7.1.7. Nutzung der Erweiterung *PolicyConstraints* (Usage of Policy Constraints extension)

Die Erweiterung *PolicyConstraints* wird nicht benutzt.

7.1.8. Syntax und Sematik von *PolicyQualifiers* (Policy qualifiers syntax and semantics)

Die Erweiterung *PolicyQualifier* wird in allen Zertifikaten verwendet, um die URL zu dem zur CP zugehörigen CPS anzugeben.

7.1.9. Verarbeitungssemantik der kritischen Erweiterung *CertificatePolicies* (Processing semantics for the critical Certificate Policies extension)

In allen Zertifikaten ist die Erweiterung *CertificatePolicies* nicht kritisch. Es liegt im Ermessen der Zertifikatnehmer und -nutzer, diese Erweiterung auszuwerten.

7.2. Widerruflistenprofil (CRL profile)

7.2.1. Versionsnummer (Version number(s))

Es werden keine öffentlichen Widerruflisten erstellt.

7.2.2. Erweiterungen von Widerruflisten und Widerrufslisteneinträgen (CRL and CRL entry extensions)

Es werden keine öffentlichen Widerruflisten erstellt.

7.3. OCSP-Profil (OCSP profile)

Der Statusabfragedienst (OCSP) gibt Auskunft über die Gültigkeit eines Zertifikats für einen anfragenden Dritten. Dabei werden folgende Status gemäß RFC 6960 zurückgeliefert:

- *good* – Das Zertifikat ist im Verzeichnisdienst vorhanden und nicht widerrufen,
- *unknown* – Das Zertifikat ist nicht im Verzeichnisdienst vorhanden,
- *revoked* – Das Zertifikat wurde zu dem angegebenen Zeitpunkt widerrufen.

Der OCSP-Dienst unterstützt die GET-Methode bei der Abfrage von Auskünften. Es wird kein Stapling genutzt.

Zum Ablaufzeitpunkt des CA-Zertifikats wird für alle Zertifikate ein letzter OCSP-Response bis zum 31.12.9999 23:59:59 Uhr vorgeneriert. Dabei wird in der Response das nextUpdate Feld mit "99991231235959Z" befüllt.

7.3.1. Versionsnummern (Version number(s)

Zur Statusabfrage der Zertifikate wird OCSP v1 gemäß RFC 6960 betrieben.

7.3.2. OCSP-Erweiterung (OCSP extensions)

Der Statusabfragedienst (OCSP) verwendet bei Antworten folgende nach RFC 6960 definierten Erweiterungen:

Feld	Beschreibung
ArchiveCutoff	Zeitraum, für den der OCSP-Responder nach Ausstellung des Zertifikats die Statusinformationen bereitstellt. Die Aufbewahrungsfrist ist laut eIDAS-Verordnung unbegrenzt. Das ArchiveCutOff-Datum wird auf das Erstellungsdatum des CA-Zertifikats gesetzt.

8. Konformitätsprüfung (COMPLIANCE AUDIT AND OTHER ASSESSMENTS)

Siehe Abschnitt 8 der zugehörigen Zertifikatsrichtlinie (CP) des TSP BVtrust.

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

Siehe Abschnitt 9 der zugehörigen Zertifikatsrichtlinie (CP) des TSP BVtrust.