Zertifikatskonzept (BVSign) (Certification Practice Statement) der Zertifizierungsstelle BVtrust der Bank-Verlag GmbH für qualifizierte Signaturzertifikate

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 im Zusammenhang mit der eIDAS-konformen Fernsignaturlösung, welche unter dem Namen BVsign angeboten werden.

Das CPS nimmt Bezug auf die Zertifikatsrichtlinie der Zertifizierungsstelle der Bank-Verlag GmbH (im Folgenden CP genannt) mit der Kennung 1.3.6.1.4.1. 50833.1.4.2 sowie die gesetzlichen Bestimmungen und Normen eIDAS-VO, VDG, VDV, ETSI EN 319 401, ETSI EN 319 411-1, ETSI EN 319 411-2 und CEN EN 419 241-1. Es beschreibt die Umsetzung der daraus resultierenden Anforderungen.

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

Maßgeblich ist allein die deutsche Fassung der 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.

Angebotene Dienste, die diesem CPS unterliegen, sind

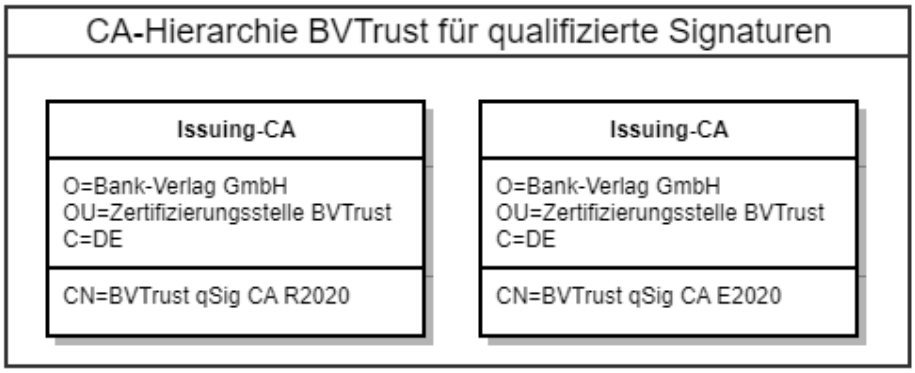
- die Ausgabe von qualifizierten Zertifikaten für elektronische Signaturen für natürliche Personen sowie
- das Ausstellen von Fernsignaturen i.S.d. der VO (EU) Nr. 910/2014.

Der Dienst der Zertifikatsausstellung und alle damit verbundenen Themen werden, wie alle CA-Dienste, unter dem Namen BVtrust angeboten. Die Fernsignaturlösung, welche es ermöglicht, qualifizierte Fernsignaturen zu verwenden, wird unter dem Namen BVsign angeboten, welcher im Folgenden als Begriff für diese Fernsignaturlösung verwendet wird. BVsign kann ausschließlich von einem Endanwender verwendet werden. Zur Nutzung des Dienstes muss der Endanwender eine Schnittstelle zu BVsign verwenden. Die Authentifizierung und Identifizierung des Endanwenders wird vom Endprovider übernommen. Der Endprovider stellt dabei dem Endanwender die Nutzung von qualifizierten Fernsignaturen über ein Online-Portal (webbasiert und/oder mobil) oder sonstige, geeigneten IT-Anwendungen, zur Verfügung. Der Begriff "Endprovider" beschreibt dabei in diesem Dokument die Gesamtheit der juristischen Personen die an BVsign angeschlossene Systeme betreiben, welche zur Bereitstellung der angebotenen Dienste benötigt werden.

Die Nutzung der qualifizierten Zertifikate für elektronische Signaturen erfordert den Einsatz einer qualifizierten Signaturerstellungseinheit (Qualified Electronic Signature Creation Device, im Folgenden QSCD genannt). Diese werden vom TSP in einer gesicherten Umgebung betrieben und können über eine geeignete gesicherte Schnittstelle verwendet werden.

Dieses Dokument beschreibt das Zertifizierungskonzept (CPS) der oben angegebenen Vertrauensdienste. Dieses Konzept ist in Form eines Certification Practice Statement (CPS) beschrieben und stellt die Anforderungen und Vorgaben für diese Vertrauensdienste dar. Die Policy QCP-n qscd aus ETSI EN 319 411-2 wird erfüllt.

Dieses CPS betrachtet die PKI für die Ausstellung von Zertifikaten für qualifizierte Signaturen. Diese ist in einer 1-Tier Hierarchie aufgebaut. Es wird nicht zwischen Root-CA und Issuing-CA unterschieden. Die Zertifikate der ausstellenden CAs werden in die *EU Trusted List* aufgenommen. Es werden zwei CA-Zertifikate erstellt, jeweils mit einem RSA- und ECDSA-Schlüssel für qualifizierte Signaturen.



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

Dokumentenname: Zertifikatskonzept (BVsign) (Certification Practice Statement) der Zertifizierungsstelle BVtrust der Bank-Verlag GmbH für qualifizierte Signaturzertifikate

Kennzeichnung (OID): 1.3.6.1.4.1.50833.1.4.1

Stand: Version 43 am 2021-07-19

1.3. PKI-Beteiligte (PKI participants)

1.3.1. Zertifizierungsstellen (Certification authorities)

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

1.3.2. Registrierungsstellen (Registration authorities)

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

1.3.3. Zertifikatnehmer und Endanwender (Subscribers/End Entity)

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

1.3.4. Vertrauender Dritter (Relying parties)

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

1.3.5. Andere Teilnehmer (Other participants)

Der TSP bietet mit BVsign eine Schnittstelle an, mit der verschiedene Endprovider, den jeweils zum Endprovider zugehörigen Endanwendern, den Dienst einer qualifizierten Fernsignatur anbieten können. Der Endprovider übernimmt in dem Fall die Identifizierung der Endanwender und initiiert den Registrierungsprozess beim TSP. Ebenso übernimmt der Endprovider die Aufgabe der korrekten Authentifizierung zur Verwendung des privaten Schlüssels. Der Endprovider kann den Dienst der Identifizierung an eine andere nach der VO (EU) Nr. 910/2014 zugelassene Identifizierungsinstanz übertragen.

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 Subject oder End Entity, kurz EE), CA-Zertifikate werden nicht ausgestellt. Die Endanwenderzertifikate können im Sinne der VO (EU) Nr. 910/2014 verwendet werden.

1.4.2. Unzulässige Verwendung von Zertifikaten (Prohibited certificate uses)

Alle Verwendungen, die nicht dem Punkt 1.4.1 sowie dem 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 Zertifikatsrichtlinie (CP) der Zertifizierungsstelle der Bank-Verlag GmbH beschrieben.

1.5.3. Pflege der Richtlinie

Dieses CPS 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 (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
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)

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

2.2. Veröffentlichung von Zertifikatsinformationen (Publication of certification information)

Der TSP veröffentlicht zu den von ihr ausgegebenen Zertifikaten

- die CP,
- dieses CPS,
- Nutzungsbedingungen
- PDS
- Datenschutzerklärung
- CA-Zertifikate und
- Statusinformationen (OCSP).

Alle Informationen können auf der Website des TSP abgerufen werden bzw. im Falle der Statusinformationen können diese direkt via OCSP abgefragt werden. Website und Statusinformationsdienst werden hochverfügbar betrieben und sind 24/7 erreichbar. Sie werden im Falle eines Ausfalls schnellstmögli ch, spätestens nach 48 Stunden, wieder zur Verfügung gestellt.

Alle Dokumente werden versioniert inkl. Zeitpunkt der Aktualisierung veröffentlicht. Anhand des Zeitpunktes der Ausstellung eines Zertifikats ist somit ermittelbar, welche Dokumentenversion das jeweilige Zertifikat heranzuziehen ist.

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

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

2.4. Zugang auf Verzeichnisdienste (Access controls on repositories)

Dieser Abschnitt wird in der 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 Endanwenders wird für alle auszustellenden Zertifikate durch den Endprovider geprüft. Die Zertifikate entsprechen dem Profil des Standards ITU-T Recommendation X.509v3. Qualifizierte Zertifikate für natürliche Personen enthalten den Namen zusammengesetzt aus Vor- und Familienname.

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 serialNumber mit einer einmalig vergebenen UUID.

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)

Die Attribute des DN von EE-Zertifikaten für natürliche Personen werden wie folgt interpretiert:

DN-Bestandteil	Interpretation
G (given name)	Vorname(n) der natürlichen Person.
SN (surname)	Familienname der natürlichen Person.
CN (common name)	Gebräuchlicher Name in der Form "Vorname Familienname".
C (Country)	Das aufzuführende Land entspricht entweder dem Wohnsitz der Person gemäß Ausweisdokument oder dem Land der ausstellenden Behörde des Ausweisdokumentes mit dem die natürliche Person identifiziert wurde und ist gemäß ISO3166 zu notieren.
serialNumber	Seriennummer in Form einer UUID als Namenszusatznummer, welche die Eindeutigkeit des DN sicherstellt.
description	Beinhaltet den Text "test certificate" im Falle von ausgestellten Zertifikaten für Testzwecke sowie entweder den Text "Country based on physical address" falls das Feld "Country" des DNs den Wohnort der natürlichen Person beschreibt oder "Country based on identification document" falls das Feld "Country" das Land der ausstellenden Behörde des Ausweisdokumentes beschreibt mit dem die natürliche Person identifiziert wurde.

Die Verwendung von Künstlernamen (Pseudoynmen) ist nicht gestattet.

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.

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 vergeben werden. Diese Seriennummer muss in Form einer UUID angegeben werden. Eine Gefahr der möglichen Verwechslung durch zwei Personen mit gleichem Namen ist somit ausgeschlossen.

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 eines privaten Schlüssels (Method to prove possession of private key)

Der Endanwender nutzt die Umgebung von BVsign und greift über eine Schnittstelle zu BVsign auf seinen privaten Schlüssel zu. Das Schlüsselpaar wird durch den TSP verwaltet. Der TSP stellt sicher, dass die Schlüsselpaare nur durch ein geeignetes QSCD und ausschließlich mithilfe eines geeigneten Zweifaktor-Authentifizierungsverfahrens durch den Endanwender verwendet werden können.

3.2.2. 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. Nach VDG §11 Abs. 4 ist es möglich Idenditätsdaten zu nutzen, die zu einem früheren Zeitpunkt erhoben wurden.

Folgende Daten werden mandatorisch erhoben:

- Vor- und Zuname,
- Geburtsdatum,
- E-Mail-Adresse,
- Identifizierungsmethode,
- Identifizierungsmittel

Mandatorisch werden entweder

- vollständige Adresse laut eingetragenem Wohnsitz, oder
- eine nutzerspezifische Kennung (Unique Identifier) und Land der ausstellenden Behörde des zur Identifizierung genutzten Dokuments

erhoben. Optional können beide Datensätze erhoben werden

Darüber hinaus können folgende Daten optional erhoben werden:

- Staatsangehörigkeit
- Telefonnummer,
- Telefaxnummer,
- Geburtsname

Darüber hinaus können folgende Daten optional, oder je nach gewähltem Authentifizierungsmittel verpflichtend erhoben werden:

- Mobilfunknummer

Natürliche Personen können qualifizierte Zertifikate über eine Schnittstelle zu BVsign beantragen. Die Identifizierung und Authentifizierung wird vom Endprovider durchgeführt.

Zusätzliche Prüfungen werden nach Bedarf durchgeführt.

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

Alle Informationen, welche in ein Zertifikat übernommen werden und im Rahmen der Authentifizierung nach 3.2.2 erhoben werden, müssen verifiziert werden.

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

Bei natürlichen Personen wird der Identitätsnachweis mittels der Verfahren gemäß Abschnitt 3.2.2 ermittelt und geprüft bzw. bestätigt.

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 Zertifikatswiderrufung (Identification and authentication for re-key after revocation)

Eine Schlüsselerneuerung nach Zertifikatswiderruf ist nicht vorgesehen.

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

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

Möchte ein Endanwender einen Widerrufantrag einreichen, so ist dieser

- über einen Einmal-Link (vorrangig) oder
- über seinen Endprovider

einzureichen. Wird der Widerrufantrag über den Endprovider eingereicht, so gibt der Endanwender dem Endprovider das zu widerrufende Zertifikat bekannt, welcher den Widerrufprozess via BVsign auslöst. Ist dies nicht möglich oder gewünscht, kann sich ein Endanwender direkt an den TSP wenden. Hierzu bietet der TSP als Self-Service einen elektronischen Widerrufantrag auf seiner Website unter https://www.bank-verlag.de/bvtrust an.

Über den Self-Service wird eine E-Mail an die bei der Registrierung angegebene Adresse versendet, die eine Auflistung aller aktuell gültigen Zertifikate enthält, welche unter Angabe dieser E-Mail-Adresse beantragt wurden. Der Endanwender erhält zu jedem aufgelisteten Zertifikat einen temporär gültigen Einmallink, über den das Zertifikat abgerufen oder sofort und unwiderruflich widerrufen werden kann.

Der Endprovider kann einen Widerruf über seine Verbindung zum TSP auslösen. Andere Widerrufberechtigte können sich für einen Widerruf direkt an den TSP wenden unter Nutzung der in Kapitel 1.5.2 des CP angegebenen Kontaktinformationen.

Der Endanwender erhält zu jedem Widerruf eine Bestätigung per E-Mail oder wird wird über den Endprovider über den Widerruf des Zertifikats informiert, sofern nicht

- bestehende Zertifikate des Endanwenders im Rahmen einer Neuausstellung eines Zertifikats widerrufen werden oder
- der Zugang des Endanwenders in den Systemen des Endproviders gelöscht wird und der Endanwender darüber informiert wird.

Dieses Vorgehen über die Benachrichtigung der Endanwender greift auch für in der Vergangenheit ausgestellte Zertifikate und steht nicht im Widerspruch zu älteren Versionen dieses CPS.

Der Widerruf sowie die vom Widerrufantragsteller angegebenen Widerrufgründe werden mittels eines automatisch erzeugten Widerrufprotokolls dokumentiert. Der Widerruf wird protokolliert und kann nur durch autorisiertes Personal durchgeführt werden.

Der Widerruf eines Zertifikats kann nicht rückgängig gemacht werden.

Certificate Problem Reports können an bvtrust@bank-verlag.de 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 dürfen von natürlichen Personen gestellt werden. Natürliche Personen beantragen das Zertifikat über einen Dienste- und Identifizierungsanbieter, welcher als Endprovider den Dienst von BVsign verwendet.

Der TSP ist dazu berechtigt, Anträge anzulehnen.

4.1.2. Registrierungsprozess und Verantwortlichkeiten (Enrollment process and responsibilities)

Die Einhaltung des Registrierungsprozesses gewährleistet der TSP bzw. der Endprovider unter Einhaltung der von TSP gestellten Anforderungen. Diese sind in einem Vertragsdokument formuliert, welches Teil des Vertrags zwischen TSP und juristischen Personen des Endproviders ist.

Dem Endanwender liegen vor Abschluss des Registrierungsprozesses alle Dokumente wie CP, CPS, PDS und Nutzungsvereinbarungen vor, zu deren Einhaltung sich der Endanwender verpflichtet. Die Dokumente sind öffentlich. Der Antrag beinhaltet weiterhin die Einverständniserklärung des Endanwenders zur Veröffentlichung oder Nicht-Veröffentlichung der Zertifikate. Alle Nachweise und Vertragsdokumente werden für die Dauer, die vertraglich vereinbart wurde, elektronisch oder papierbasiert hinterlegt.

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.

Registriert sich ein Zertifikatnehmer über einen Endprovider, so ist der Endprovider für die ordentliche Authentifizierung nach Art. 24 Abs. 1 der VO (EU) Nr. 910/2014 verantwortlich. Nach erfolgreicher Authentifizierung kann der Registrierungsprozess fortgesetzt werden.

Die Identifizierung und Authentifizierung der Antragsteller muss vor der Ausstellung des Zertifikats abgeschlossen sein.

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

Treten bei der Prüfung der Identität im Rahmen der Authentifizierung durch den Endprovider 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 einer juristischen Person des Endproviders gegenüber dem TSP oder
- Umstände, die den Verdacht begründen, dass eine Zertifikatsausstellung den Betreiber der CA in Misskredit bringt.
- weitere Gründe, die der Endprovider definiert

Der TSP ist berechtigt, Zertifikatsanträge auch ohne die Angabe von Gründen abzulehnen.

4.2.3. Bearbeitungsdauer von Zertifkatsanträgen (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)

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

Wird der Registrierungsprozess durch einen Endprovider durchgeführt, so überträgt dieser den Registrierungsantrag inkl. der Identitätsdaten in einem gesicherten Verfahren über die vom TSP zur Verfügung gestellten Schnittstelle. Dieses wird in einem automatisierten Verfahren bearbeitet, sodass ein Zertifikat ausgegeben wird. Der private Schlüssel verbleibt beim TSP für die Nutzung des Fernsignaturdienstes mit Hilfe eines QSCDs (Qualified Signature Creation Device).

Das Zertifikat wird dem Endprovider zur Verfügung gestellt. Diesem obliegt es, ob er das Zertifikat dem Endanwender zur Verfügung stellen möchte. Zusätzlich hat der Endanwender die Möglichkeit das Zertifikat über den Self-Service des TSPs abzurufen.

Der Zugriff auf den privaten Schlüssel erfolgt immer über BVsign.

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

Eine gesonderte Benachrichtigung des Zertifikatnehmers erfolgt nicht.

4.4. Zertifikatsübergabe (Certificate acceptance)

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

Wird ein Endprovider zur Registrierung verwendet, bekommt dieser das soeben erstellte Zertifikat direkt zurückgesendet.

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

Der TSP bietet einen intern wie extern erreichbaren Verzeichnisdienst für Statusinformationen 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)

Der TSP antwortet über die aufgerufene Schnittstelle, über die die Beantragung durch den Endanwender stattgefunden hat, mit dem generierten Zertifikat, sofern die Antragsstellung fehlerfrei ist.

Das Zertifikat wird dem Endprovider zur Verfügung gestellt. Diesem obliegt es, ob er das Zertifikat dem Endanwender zur Verfügung stellen möchte. Zusätzlich hat der Endanwender die Möglichkeit das Zertifikat über den Self-Service des TSPs abzurufen.

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 dürfen ihre privaten Schlüssel ausschließlich für die Anwendungen nutzen, die in Übereinstimmung mit den im Zertifikat angegebenen Nutzungsarten stehen. Für Endanwender 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)

Die Zertifikate können von allen Endanwendern verwendet werden. Die Endanwender und Dritte dürfen jedoch nur dann auf den öffentlichen Schlüssel und das Zertifikat vertrauen, wenn folgende Voraussetzungen vorliegen:

- das Zertifikat wird gemäß den zulässigen Nutzungsarten benutzt und eventuelle Einschränkungen im Zertifikat wurden beachtet,
- 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. Zertifikatswiderruf und Suspendierung (Certificate revocation and suspension)

4.9.1. Bedingungen für einen Widerruf(Circumstances for revocation)

Endanwender oder betroffenen 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 wurden oder Daten des Zertifikats nicht mehr korrekt sind.

Der TSP muss ein Zertifikat widerrufen

- auf Verlangen des Endanwenders, eines Widerrufberechtigten Dritten oder der entsprechenden Aufsichtsbehörde ,
- bei fehlerhaften Angaben im Zertifikat oder
- bei Einstellung der Tätigkeit als Zertifizierungs-/Vertrauensdiensteanbieter, wenn kein anderer Zertifizierungs-/Vertrauensdiensteanbieter diese übernimmt.

Unabhängig davon muss der TSP Widerrufe 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,
- das Zertifikat nicht mehr konform zum gültigen CP bzw. CPS ist,
- dem TSP Änderungen bekannt sind, die sich auf die Gültigkeit des Zertifikats auswirken,
- ein Zertifikat aufgrund falscher Angaben erwirkt oder anderweitig missbraucht wurde oder
- das Vertragsverhältnis mit dem zugehörigen Endprovider 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.

Widerrufberechtigte müssen sich gemäß Abschnitt 3.4 authentifizieren.

4.9.2. Widerrufberechtigung (Who can request revocation)

Zum Widerruf des Zertifikats sind berechtigt

- der TSP,
- der Endanwender,
- der Endprovider und
- andere widerrufberechtigte Dritte .

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

Die Authentifizierung des Widerrufsberechtigten erfolgt gemäß Abschnitt 3.4.

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

Der Widerruf eines Zertifikats kann nicht rückgängig gemacht werden.

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

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.

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)

Widerrufsinformationen 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 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)

Keine.

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

Wenn ein privater Schlüssel kompromittiert wurde, so muss dies dem TSP unverzüglich mitgeteilt werden. Das dazugehörige Zertifikat wird widerrufen und der private Schlüssel muss (sofern technisch möglich) vernichtet werden.

4.9.13. Suspendierung des Zertifikats (Circumstances for suspension)

Die Suspendierung des Zertifikats ist nicht möglich.

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, 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.

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 Endprovider 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 und Dritte, einschließlich Vertrauender Dritter und der zuständigen Aufsichtsbehörde und ggf. den fortführenden TSP, rechtzeitig, mindestens aber zwei Monate vorher, über die Einstellung des Zertifizierungs- und Vertrauensdienstes. Diese Information wird auch auf der Website des TSPs unter https://www.bank-verlag.de/bvtrust veröffentlicht.

Der TSP widerruft bei Übergabe an die Aufsichtsbehörde oder einen anderen fortführenden TSP alle noch gültigen Zertifikate zum Zeitpunkt der Beendigung des Zertifizierungsdienstes. Die ausgegebenen Zertifikate sowie deren Statusinformationen werden in diesem Fall in die von der entsprechenden Aufsichtsbehörde geschaffene Vertrauensinfrastruktur, oder ggf. in die Vertrauensinfrastruktur des fortführenden TSP, überführt. 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)

Private Schlüssel werden treuhänderisch vom TSP verwaltet. Der private Schlüssel wird sicher verwaltet. Es ist über den TSP sichergestellt, dass ausschließlich der Endanwender Zugriff auf den privaten Schlüssel seines Zertifikats hat und diesen nutzen kann. Sobald das zu dem privaten Schlüssel zugehörige Zertifikat abläuft oder widerrufen wird, wird der private Schlüssel gelöscht und kann nicht wiederhergestellt werden.

In allen anderen Fällen wird keine Hinterlegung und Wiederherstellung von privaten Schlüsseln angeboten.

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 319 411-1, ETSI EN 319 411-2 sowie CEN EN 419 241-1 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, ETSI EN 319 411-2 sowie CEN EN 419 241-1 regelmäßig wiederholt.

Ferner wurde dem Sicherheitsbereich des TSP 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 Mehr-Augen-Prinzip 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.

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 Führungszeugisses muss in regelmäßigen Abständen wiederholt werden.

5.3.3. Schulungen und Weiterbildungen (Training requirements)

Der TSP erfüllt die Anforderungen aus ETSI EN 319 411-2 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 Sicherheitsbelehrung.

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

Rollenwechsel werden dokumentiert. Die entsprechenden Mitarbeiter werden geschult.

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)

Es werden keine freien Auftragnehmer für den Betrieb des TSP eingesetzt.

5.3.8. Ausgehändigte Dokumentation (Documentation supplied to personnel)

Folgende Dokumentationen werden dem Personal zur Verfügung gestellt:

- Sicherheitskonzept
- DV-Konzept
- Rollenbeschreibung und Arbeitsanweisungen
- CP/CPS/PDS
- Betriebs- und Fachkonzepte
- Spezifikationen
- Sicherheitsrichtlinie der Bank-Verlag GmbH
- Nutzungsbedingungen

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 eine angemessene Zeit lang 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), 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 sowie die Zertifikate selbst, werden für die gesamte Betriebszeit des TSP aufbewahrt. Wird der Betrieb eingestellt, werden alle Dokumente und Daten entweder an die Institution, die den Dienst im Rahmen dieses CPS übernehmen möchte, oder an die zuständige Aufsichtsbehörde übergeben.

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.

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 und die dort verarbeiteten personenbezogenen Daten 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 die entsprechende Aufsichtsbehörde unverzüglich informiert und die betroffenen CA-Zertifikate sowie, sofern notwendig, durch diese ausgestellte EE-Zertifikate widerrufen. Betroffene 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 entscheidet, 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 Schlüsselspeicher (HSM) 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) oder CEN/TS 419 221-5 konformen und zertifizierten 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.

Nutzerschlüssel für qualifizierte Zertifikate, die in Hoheit des TSP generiert werden (BVsign), sind technisch den QSCDs des TSPs verknüpft und können nicht anderweitig verwendet oder exportiert werden.

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

Es werden keine privaten Schlüssel an Endanwender ausgeliefert.

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

Nicht vorgesehen.

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 zuständige Aufsichtsbehörde 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 sowie ECDSA-Schlüssel mit einer Schlüssellänge von mindestens 384 bit mit Domain-Parametern der NIST- und Brainpool-Familie (siehe 7.1.3).

Für EE-Zertifikate werden derzeit RSA-Schlüssel mit einer Schlüssellänge von mindestens 4096 bit verwendet sowie ECDSA-Schlüssel mit einer Schlüssellänge von mindestens 384 bit mit Domain-Parametern der der NIST- und Brainpool-Familie (siehe 7.1.3).

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

Alle Schlüsselparameter und die eingesetzten HSMs richten sich nach der jeweils gültigen Vorgabe aus dem von der Bundesnetzagentur empfohlenen Kryptokatalog sowie der Konformitätsbewertung des QSCDs. 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. Wird ein EE-Zertifikat über BVsign beantragt, geschieht dies in einem automatischen und festgelegten kryptographisch abgesicherten Prozess, welcher nicht manuell aktiviert werden kann.

Private Schlüssel von EE-Zertifikaten, die durch BVsign verwaltet werden, können ausschließlich nach erfolgreicher Zwei-Faktor-Authentifizierung durch den Endanwender über die Schnittstelle zu BVsign aktiviert werden.

6.2.3. Hinterlegung von privaten Schlüsseln (Private key escrow)

Im Rahmen von BVsign werden private Schlüssel von EE-Zertifikaten ausschließlich durch den TSP verwaltet und können niemals die gesicherte Umgebung des TSP verlassen. In allen anderen Fällen wird eine Hinterlegung privater Schlüssel nicht 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.

Alle privaten Schlüssel von EE-Zertifikaten werden im Rahmen der Hochverfügbarkeit des BVsign-Dienstes in verschlüsselter Form gesichert. Diese gesicherten Schlüssel können ausschließlich im QSCD wiederhergestellt und verwendet werden.

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 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.

Private Schlüssel von EE-Zertifikaten werden verschlüsselt vorgehalten und an das QSCD übertragen.

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

Die privaten CA-Schlüssel liegen verschlüsselt im HSM vor.

Private Schlüssel von EE-Zertifikaten werden im QSCD erstellt und verschlüsselt in einer Datenbank gespeichert.

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

Private CA-Schlüssel werden gemäß Abschnitt 6.2.2 aktiviert.

Private Schlüssel von EE-Zertifikaten können ausschließlich durch den Endanwender aktiviert und verwendet werden. Diese müssen für jede Verwendung aktiviert werden.

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

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

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

Alle privaten Schlüssel werden nach Ende der Gültigkeit, bei Widerruf des zugeordneten Zertifikats und Beendigung des Betriebs vernichtet.

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 oder QSCDs nach CEN EN 419 221-5 und CEN EN 419 241-2. Der TSP überwacht den Zertifizierungsstatus des QSCDs. Sollte die Zertifizierung des QSCDs zurückgezogen werden, wird dieser Umstand durch den TSP-Leiter und ggf. anderen Parteien wie der Konformitätsbewertungsstelle oder der Bundesnetzagentur 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 2 Jahre.

Die Gültigkeitsdauer der EE-Zertifikate ist variabel und dem Zertifikat zu entnehmen. Die maximale Gültigkeitsdauer beträgt 2 Jahr.

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 über das BVsign eigene Tokenkonzept. Dieses garantiert, dass ausschließlich der Endanwender mittels seiner Zwei-Faktor-Authentifizierung seinen zugeordneten privaten Schlüssel verwenden kann. Hierzu werden existierende als sicher geltende Zwei-Faktor-Verfahren verwendet, die dem Sicherheitsniveau von Passwort und TAN im Online-Banking gleichgestellt sind.

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 und BVsign 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, eIDAS-VO, VDG, VDV, ETSI EN 319 401, ETSI EN 319 411-1, ETSI EN 319 411-2 sowie CEN EN 419 241-1 betrieben werden.

Alle Mitarbeiter des TSP müssen die Arbeitseinweisungen der Vorgaben zur Computersicherheit einhalten. 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. Sollten Gründe existieren, die einem Update widersprechen, so müssen diese dokumentiert und dem Risikomanagement des TSP übergeben werden.

Alle Endanwender und Zertifikatnutzer müssen vertrauenswürdige Computer und Software verwenden.

6.5.2. Bewertung der Computersicherheit (Computer security rating)

Alle eingesetzten Systeme, die private Schlüssel von CA- oder EE-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 und BVsign verwendet werden, werden überwacht. Bei Entdeckung sicherheitsrelevanter 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 Mehr-Augen-Prinzip möglich ist.

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, sodass schwerwiegende Fehler, die durch ein Update entstehen könnten, minimiert werden.

Alle Daten werden redundant gesichert, so dass 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 Desaster-Recovery-Vorfall 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 Sicherheitslevel. Je nach Sicherheitslevel ist die jeweilige Zone durch mehrere Firewallsysteme geschützt. Das Netzwerk wird regelmäßig durch anerkannte Konformitätsbewertungsstellen sowie Penetrationstests geprüft. Werden in dem Zusammenhang Schwachstellen bekannt, werden diese bewertet und zeitnah behoben.

6.8. Zeitstempel (Time-stamping)

Der TSP betreibt keinen Zeitstempeldienst.

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

7.1. Zertifikatsprofil (Certificate profile)

7.1.1. Versionsnummern (Version number(s))

Die Zertifikate werden im Format X.509v3 und gemäß ETSI EN 319 412-2 und ETSI EN 319 412-5 ausgegeben.

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	digitalSignature, keyCertSign, cRLSign
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	

				policyIdentifier=1.3.6.1.4.1.50833.1.4.2 policyQualifier:policyQualifierId=1.3.6.1.5.5.7.2.1 policyQualifier= https://www.bank-verlag.de/bvtrust-bvsign

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	
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	policyIdentifier=1.3.6.1.4.1.50833.1.4.2 policyQualifier:policyQualifierId=1.3.6.1.5.5.7.2.1 policyQualifier:qualifier:cPSuRI= https://www.bank-verlag.de/bvtrust-bvsign
ocspNoCheck	1.3.6.1.5.5.7.48.1.5			

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 Signaturen

EE-Zertifikate für Signaturen enthalten folgende Erweiterungen:

Feld	OID	Kritisch	Erforderlich	Beschreibung	Wert
keyUsage	2.5.29.15	ja	muss	Verwendungszweck	contentCommitment
basicConstraints	2.5.29.19	ja	muss	Beschränkung Verwendung ausgestellter Zertifikate	
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= 0.4.0.194112.1.2 (qcp-natural-qscd) policyIdentifier=1.3.6.1.4.1.50833.1.4.2 policyQualifier:policyQualifierId=1.3.6.1.5.5.7.2.1 policyQualifier:qualifier:cPSuRI= https://www.bank-verlag.de/bvtrust-bvsign
qcStatements	1.3.6.1.5.5.7.1.3	nein	muss	QCStatements	QcEuPDS= 0.4.0.1862.1.5 (id-etsi- qcs-QcPDS) https://www.bank-verlag.de/bvtrust QcCompliance= 0.4.0.1862.1.1 (id-etsi-qcs-QcCompliance) QcType= 0.4.0.1862.1.6 id-etsi-qct-esign = 0.4.0.1862.1.6.1 QcSSCD= 0.4.0.1862.1.4 (id-etsi-qcs-QcSSCD)

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)

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

OID	Beschreibung
1.2.840.113549.1.1.10	PKCS#1 RSASSA-PSS
1.2.840.10045.4.3.2	ANSI x9.62 ECDSA with SHA256
1.2.840.10045.4.3.3	ANSI x9.62 ECDSA with SHA384
1.2.840.10045.4.3.4	ANSI x9.62 ECDSA with SHA512

Im Fall von RSASSA-PSS werden folgende Hash-Algorithmen sowie folgende Mask-Generation-Funktion verwendet:

OID	Beschreibung
2.16.840.1.101.3.4.2.1	SHA256
2.16.840.1.101.3.4.2.2	SHA384
2.16.840.1.101.3.4.2.3	SHA512
2.16.840.1.101.3.4.2.8	SHA3-256
2.16.840.1.101.3.4.2.9	SHA3-384
2.16.840.1.101.3.4.2.10	SHA3-512

OID	Beschreibung
1.2.840.113549.1.1.8	MGF1

Folgende Kurven für ECDSA-Signaturen werden verwendet:

OID	Beschreibung
1.3.132.0.34	secp384r1/NIST P-384
1.3.132.0.35	secp521r1/NIST P-521
1.3.36.3.3.2.8.1.1.11	brainpoolP384r1
1.3.36.3.3.2.8.1.1.12	brainpoolP384t1
1.3.36.3.3.2.8.1.1.13	brainpoolP512r1
1.3.36.3.3.2.8.1.1.14	brainpoolP512t1

7.1.4. Namensformen (Name forms)

In den Feldern *subject* und *issuer* werden Namen nach X.501 als DistinguishedName vergeben. Es können die Attribute aus Abschnitt 3.1.4 vergeben werden. Die Kodierung erfolgt als UTF8-String.

In den Feldern SubjectAltName (Alternativer Endanwendername) und Issuer-AltName (Alternativer Ausstellername) 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 CA- und OCSP-Zertifikate enthalten in der Erweiterung CertificatePolicies die OID der unterstützten CP. EE-Zertifikate enthalten in der Erweiterung *Cer tificatePolicies* zusätzlich die OID der Policy QCP-n-qscd 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 CA-Zertifikaten verwendet, um die URL zu dem zum CP zugehörigen CPS anzugeben.

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

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

7.2. Widerrufslistenprofil (CRL profile)

7.2.1. Versionsnummer (Version number(s))

Es werden keine öffentlichen Widerrufslisten erstellt.

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

Es werden keine öffentlichen Widerrufslisten 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.

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 in seinen Antworten folgende, nach RFC 6960 definierten Erweiterungen:

Feld	Beschreibung
ArchiveCutoff	Zeitraum, für den der OCSP-Responder nach Ausstellung des Zertifikats die Statusinformationen bereitstellt. Die Retention Period 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 Zertifikatsrichtlinie (CP) des TSP BVtrust.

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

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