BVbank-verlag

Bank-Verlag GmbH

BVqtime - Time-Stamp Policy und TSA Practice Statement

Version: 41
Datum: 2024-11-28
Status: Final

BVbank-verlag

Inhalt

1 Einleitung

Dieses Dokument beschreibt die Zertifikatsrichtlinie des vom Vertrauensdiensteanbieter Bank-Verlag GmbH betriebenen Dienstes "qualifizierte elektronische Zeitstempel", welcher unter dem Namen BVqtime angeboten wird, in Form einer Time-Stamp Policy sowie eines Trust Service Practice Statement (TSPS) und stellt die Anforderungen und Vorgaben für die von der Zertifizierungsstelle BVqtime betriebenen Public Key Infrastruktur (PKI) dar.

Die Struktur dieses Dokuments basiert auf der Norm ETSI EN 319 421, um einen einfachen Vergleich zwischen Vertrauensdiensteanbietern zu ermöglichen.

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

1.1 Überblick (Overview)

Der Zeitstempelanbieter (Time-Stamping Authority, im Folgenden die TSA genannt) ist die

Bank-Verlag GmbH
Vitalisstraße 67
50827 Köln.

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

Die TSA verfügt über die Konformitätsbewertung durch eine anerkannte Konformitätsbewertungsstelle, welche die Einhaltung der in der VO (EU) Nr. 910/2014 sowie den Normen ETSI EN 319 401, ETSI EN 319 421 und ETSI EN 319 422 festgelegten Anforderungen bestätigt.

Zertifikate, die im Rahmen von BVqtime von der TSA ausgegeben werden, unterliegen immer der Zertifizierung im Sinne der eIDAS-VO, VDG, VDV, ETSI EN 319 401, ETSI EN 319 421 und ETSI EN 319 422 . Die Bereitstellung des Zeitstempeldienstes steht im Einklang mit der ETSI Best practices time stamp policy (BTSP - OID: 0.4.0.2023.1.1) gemäß ETSI EN 319 421.

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

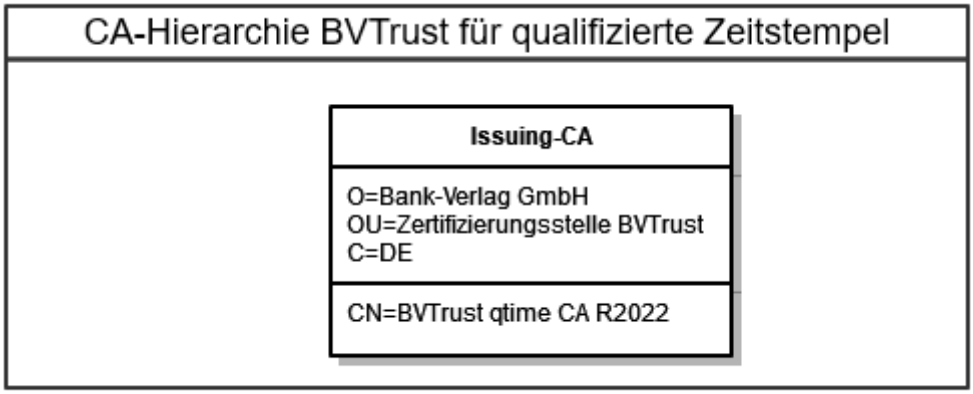
Der TSA kann Teilaufgaben an Partner oder externe Anbieter auslagern.

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

Dokumentenname: Zertifikatsrichtlinie BVqtime (TSPS) der Zertifizierungsstelle BVtrust der Bank-Verlag GmbH

Kennzeichnung (OID): 1.3.6.1.4.1.50833.1.6.2

Stand: Version 41 am 2024-11-28



1.3 Akronyme und Definitionen (Definitions and acronyms)

Begriff	Beschreibung
BTSP	Best practices time stamp policy
CA	Certificate Authority
CP	Certificate Policy
CPS	Certification Practice Statement
DSGVO	Datenschutz-Grundverordnung
EE	End Entity - Endanwender oder Subject
PKI	Public Key Infrastruktur
RA	Registration Authority
TSP	Trust Service Provider
VA	Validation Authority
TSPS	Trust Service Practice Statement
TSA	Time-Stamping Authority
TSU	Time Stamping Unit

1.4 Verwaltung der Zertifikatsrichtlinie (Policy administration)

1.4.1 Zuständigkeit für dieses Dokument(Organization administering the document)

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

1.4.2 Kontaktinformationen (Contact person)

Eine Kontaktaufnahme kann über folgende Adressen erfolgen:

Bank-Verlag GmbH
Security and Trusted Services
Vitalisstraße 67
50827 Köln

Tel: + 49 221 5490 724

E-Mail: bvtrust@bank-verlag.de

1.4.3 Pflege der Richtlinie

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

1.4.4 Genehmigungsverfahren dieses Dokuments

Der in Kapitel 1.1. benannte Herausgeber ist für dieses Dokument verantwortlich. Die Freigabe erfolgt durch das TSP Management und das Dokument wird unmittelbar nach der Freigabe auf der Webseite des TSP als aktuelle Version veröffentlicht. Alle vorangegangenen Versionen werden in ein Archiv verschoben und sind weiterhin verfügbar. Vergangene Versionen werden nicht gelöscht.

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

1.4.5 Streitschlichtungsverfahren (Dispute resolution provisions)

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

2 Gesamtkonzept (General concepts)

2.1 Allgemeine Richtlinien (General policy requirements concepts)

Die TSA stellt ausschließlich qualifizierte elektronische Zeitstempel aus.

2.2 Zeitstempeldienste (Time-stamping services)

Die Erbringung von Zeitstempeldiensten wird in diesem Dokument in die folgenden Komponenten untergliedert:

- **Erbringung von Zeitstempeln**:
  Die Erstellung von Zeitstempeln.
- **Verwaltung von Zeitstempeln:**
  Diese Dienstkomponente überwacht und steuert den Betrieb des Zeitstempeldienstes, um sicherzustellen, dass der Dienst den Vorgaben der TSA entspricht. Diese Dienstkomponente ist verantwortlich für die Überwachung und korrekte Konfiguration des Zeitstempeldienstes.

Diese Unterteilung der Dienste in einzelnen Komponenten dient nur der Verdeutlichung der in diesem Dokument aufgeführten Anforderungen und schränkt die Unterteilung einer Implementierung beim TSA in keiner Weise ein.

2.3 Zeitstempelanbieter (Time-Stamping Authority)

Der TSA trägt die Gesamtverantwortung für die Erbringung der in Abschnitt 4.2 genannten Zeitstempeldienste. Der TSA obliegt die Verantwortung für den Betrieb einer oder mehrerer Time-Stamping-Unit (TSU), die im Auftrag der TSA Zeitstempel erstellen und signieren.

Der TSA kann Dritte für die Erbringung von Teilen des Zeitstempeldiensts heranziehen. Der TSA obliegt jedoch stets die Gesamtverantwortung und er stellt sicher, dass die in diesem Dokument genannten Anforderungen und Richtlinien erfüllt werden.

2.4 Zeitstempeldienst Nutzer (Subscriber)

Die TSA stellt qualifizierte elektronische Zeitstempel nicht unmittelbar Endanwendern zur Verfügung. Subscriber des Zeitstempeldienstes sind natürliche oder juristische Personen, die qualifizierte elektronische Zeitstempel im Rahmen von vertraglichen Vereinbarungen beziehen. Diese Subscriber sind dafür verantwortlich die Endanwender über ihre Pflichten zu informieren und dass die Endanwender diese Pflichten nachkommen.

3 Zeitstempel Richtlinien und Verfahren (Policies and practices)

3.1 Risikoanalyse (Risk assessment)

Der TSA führt regelmäßig eine Risikoanalyse durch, um die Risiken der angebotenen Vertrauensdienste zu ermitteln, zu analysieren und zu bewerten

3.2 Trust Service Practice Statement

3.2.1 Zeitstempel Format

Die erstellten Zeitstempel sind RFC 3161 konform und beachten die Anforderungen aus ETSI EN 319 422. Es werden Schlüssel mit einer Stärke von 4096bit RSA oder ECDSA mind. 384 bit erzeugt. Im Falle von RSA wird als Signaturalgorithmus MGF1 genutzt, mindestens SHA256withRSAandMGF1.

3.2.2 Zeitgenauigkeit

Der Zeitstempeldienst wird in Deutschland betrieben und empfängt das Zeitsignal durch die gesetzlich gültige Zeit von der Physikalisch-Technische Bundesanstalt (PTB). Die Maximale Abweichung der Zeit zu UTC überschreitet in keinem Fall 1 Sekunde. Bei der Überschreitung der Abweichung von mehr 1 Sekunde, stellt der Zeitstempeldienst automatisch die Ausstellung von neuen Zeitstempeln ein. Schaltsekunden werden korrekt erkannt, protokolliert und bei der Ausstellung der Zeitstempel berücksichtigt.

3.2.3 Unzulässige Verwendung des Dienstes

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

Hierzu zählen Atomkraftwerke, Chemieproduktionsanlagen oder Luftfahrtsysteme.

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

3.2.4 Pflichten des Nutzers (subscriber's obligations)

Der Bank-Verlag stellt seinen Zeitstempeldienst nicht unmittelbar Endnutzern zur Verfügung. Der Zeitstempel Nutzer ist dafür verantwortlich, Zeitstempel so zu verwenden, dass die Verwendung den anwendbaren gesetzlichen Bestimmungen entspricht.

3.2.5 Pflichten der Vertrauenden Dritten (relying party's obligations)

Es gelten die mit dem TSA geschlossenen einzelvertraglichen Vereinbarungen.

3.2.6 Verifizierung des Zeitstempels (Verification of the time stamp)

1. Verifizierung des Ausstellers des Zeitstempels (verification of timestamp issuer)

Die Zertifikatskette kann erfolgreich bis zu einem vertrauenswürdigen Root-Zertifikat verifiziert werden, welches in der EUTL (European Trusted List) aufgeführt ist. Darüber hinaus

veröffentlicht der TSA auf der Website derTSA die CA Zertifikate, um Dritten die Möglichkeit zu bieten die ausgestellten Zertifikate zu prüfen.

2. Verifizierung der Widerruf- und Statusinformationen (verification of timestamp revocation or status information)

Die TSA bietet einen erreichbaren Verzeichnisdienst für Statusinformationen über OCSP an. 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.

3. Verifizierung der Integrität des Zeitstempels (Verification of the integrity of time stamp)

Die Integrität der ausgestellten Zeitstempel kann nach RFC 3161 verifiziert werden.

3.2.7 Anwendbares Recht (Applicable law)

Es gilt deutsches Recht sowie das Recht der europäischen Union, der Gerichtsstand ist Köln.

3.2.8 Verfügbarkeit des Zeitstempeldienstes (Service availability)

Der Zeitstempeldienst wird von der TSA in Rechenzentren der Bank-Verlag GmbH hochverfügbar betrieben und ist 24/7 erreichbar. Im Falle eines Ausfalls wird dieser schnellstmöglich wieder zur Verfügung gestellt. Es gelten die vereinbarten Service Level Agreements (SLA) zwischen Auftraggeber und Auftragnehmer.

3.3 Allgemeine Geschäftsbedingungen (Terms and conditions)

Es gelten die mit dem TSA geschlossenen einzelvertraglichen Vereinbarungen.

3.4 Informationssicherheitsrichtlinie (Information security policy)

Die TSA verfügt über eine von der Geschäftsführung der Bank-Verlag GmbH freigegebene und für alle Mitarbeiter:innen gültige Informationssicherheitsstrategie und Informationssicherheitsrichtlinie. Diese werden jährlich überprüft und gegebenenfalls aktualisiert. Änderungen werden durch die Geschäftsführung der Bank-Verlag GmbH freigegeben.

3.5 TSA Pflichten (TSA obligations)

Die TSA betreibt den Vertrauensdienst im Einklang mit dem geltenden Recht. Selbstaufsichtsmaßnahmen (Quality Assessments) werden von dafür qualifizierten TSA Mitarbeitern durchgeführt. Eine unabhängige Konformitätsbewertungsstelle überprüft den TSA-Betrieb im vorgesehenen Rhythmus.

3.6 Informationen für Vertrauende Dritte (Information for relying parties)

Die Zertifikate können von allen Zertifikatnehmern verwendet werden. Die Zertifikatnehmer und Dritte dürfen jedoch nur dann auf den Zeitstempel vertrauen, wenn folgende Voraussetzungen vorliegen:

- der Zeitstempel wurde korrekt signiert und der zur Signatur des Zeitstempels verwendete private Schlüssel wurde bis zum Zeitpunkt der Verifizierung nicht kompromittiert,
- die Gültigkeit des Zertifikates, welches zur Erstellung des Zeitstempels verwendet wurde, wird über den Statusabfragedienst (OCSP) bestätigt,
- der Zeitstempel wird gemäß den zulässigen Nutzungsarten verwendet und eventuelle Einschränkungen in der Zeitstempel Policy wurden beachtet,
- die Zertifikatskette kann erfolgreich bis zu einem vertrauenswürdigen Root-Zertifikat verifiziert werden, welches in der EUTL (European Trusted List) aufgeführt ist,
- alle weiteren Vereinbarungen und sonstigen Vorsichtsmaßnahmen wurden eingehalten.

4 Verwaltung und Betrieb des Zeitstempeldienstes (TSA management and operation)

4.1 Interne Organisation (Internal organization)

Siehel Kapitel 1.1

4.2 Personalkonzept (Personnel security)

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

Der Leiter des Trustcenters trägt in der Besetzung der Rollen dafür Sorge, dass eine angemessene Anzahl von Mitarbeitern mit den notwendigen Kenntnissen und Erfahrungen zur Ausübung der Tätigkeit eingesetzt werden.

4.2.2 Sicherheitsüberprüfung (Background check procedures)

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

4.2.3 Schulungen und Weiterbildungen (Training requirements)

Der TSA erfüllt die Anforderungen aus ETSI EN 319 411-2 bzgl. der Schulung und Weiterbildung des Personals des TSA.

4.2.4 Häufigkeit von Schulungen und Belehrungen (Retraining frequency and requirements)

Alle Mitarbeiter des TSA unterliegen mindestens alle 12 Monate einer Sicherheitsbelehrung.

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

Rollenwechsel werden dokumentiert. Die entsprechenden Mitarbeiter werden geschult.

4.2.6 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 zur Infrastruktur entzogen.

4.2.7 Anforderungen an freie Auftragnehmer (Independent contractor requirements)

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

4.2.8 Ausgehändigte Dokumentation (Documentation supplied to personnel)

Folgende Dokumentationen werden dem Personal zur Verfügung gestellt:

- Sicherheitskonzept
- Rollenbeschreibung und Arbeitsanweisungen
- Time-Stamp Policy und TSA Practice Statement
- Betriebs- und Fachkonzepte
- Spezifikationen
- Sicherheitsrichtlinie der Bank-Verlag GmbH

4.3 Asset Verwaltung (Asset management)

Um die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit zu erreichen, werden alle Assets identifiziert, dokumentiert und gemäß Risikobewertung klassifiziert.

4.3.1 Umgang mit Medien (Media handling)

Sämtliche Medien werden gemäß den Anforderungen des Klassifizierungssystems behandelt um unautorisierten Zugriff und Diebstahl zu verhindern. Medien, die sensible Daten enthalten, werden sicher entsorgt, sobald sie nicht mehr benötigt werden. Defekte und nicht benötigte Datenträger werden nach einem sicheren Verfahren zerstört.

4.4 Zugriffskontrolle (Access control)

4.4.1 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 TSA berufen werden, müssen frei von Interessenkonflikten oder anderen Einflüssen sein, die geeignet sind, das Vertrauen des TSAs 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.

4.4.2 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.

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

Das Rollenkonzept wird durch technische und organisatorische Maßnahmen, wie beispielsweise Zutrittsberechtigungen und Wissensabfragen, 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.

4.4.4 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 schädliches Handeln vorzubeugen.

4.5 Kontrollen kryptographischer Module (Cryptographic controls)

4.5.1 TSU Schlüsselgenerierung (TSU key generation)

Die Generierung aller Schlüsselpaare im Verantwortungsbereich des TSA 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 TSA.

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

Es werden Schlüssel mit einer Stärke von 4096bit RSA oder ECDSA mind. 384 bit erzeugt. Im Falle von RSA wird als Signaturalgorithmus MGF1 genutzt,
mindestens SHA256withRSAandMGF1

4.5.2 Schutz des privaten Schlüssels der TSU(TSU private key protection)

Der private Schlüssel für den Zeitstempeldienst CA liegt ausschließlich in sicheren, nach FIPS 140-2 Level 3 (oder höher) oder CEN/TS 419 221-5 konformen und zertifizierten HSMs vor.

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 TSA statt.

4.5.3 Zertifikat des öffentlichen Schlüssels der TSU (TSU public key certificate)

Die CA-Zertifikate, welche die dazugehörigen öffentlichen CA-Schlüssel beinhalten, werden in der nationalen Vertrauensliste veröffentlicht, welche durch die zuständige Aufsichtsbehörde verwaltet wird. Diese sind somit auch in der EU Trusted List enthalten. Darüber hinaus werden alle CA-Zertifikate nach ihrer Erstellung auf der Website des TSA veröffentlicht.

4.5.4 Schlüsselerneuerung (Rekeying TSU's key)

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. Beim Auslaufen der Eignung der eingesetzten Algorithmen oder der eingesetzten TSU werden die Schlüssel vor Ablauf der Zertifikatsgültigkeit gesperrt, so dass eine Ausstellung von Zeitstempeln nicht mehr möglich ist.

4.5.5 Lebenszyklusmanagement der signierenden kryptografischen Hardware (Life cycle management of signing cryptographic hardware)

Die verwendeten HSMs werden nach jedem Transport und vor der Inbetriebnahme durch qualifiziertes Personal im Vier Augen Prinzip auf Manipulationen überprüft. Die Ergebnisse dieser Untersuchungen werden protokolliert. Nur nach einer erfolgreichen Prüfung wird das HSM in Betrieb genommen.

Der Zugang zu den HSMs ist nur auf die dafür zuständigen Rollen beschränkt.

4.5.6 Lebenszyklus von Schlüsseln (Rekeying TSU's key / End of TSU key life cycle)

Die Gültigkeitsdauer der CA-Zertifikate ist variabel und dem Zertifikat zu entnehmen. Die Gültigkeitsdauer der privaten Schlüssel übersteigt nie die Gültigkeitsdauer der damit erstellten Zertifikate. Beim Auslaufen der Eignung der eingesetzten Algorithmen oder der eingesetzten TSU werden die Schlüssel vor Ablauf der Zertifikatsgültigkeit gesperrt. Nach Ablauf der Gültigkeitsdauer oder nach der Sperrung der privaten Schlüssel werden diese Schlüssel unwiederbringlich gelöscht, so dass eine Ausstellung von Zeitstempeln mit diesen privaten Schlüsseln nicht mehr möglich ist.

4.6 Time-stamping

4.6.1 Ausstellung von Zeitstempeln (Time-stamp issuance/Clock synchronization with UTC)

Die vom TSA erstellten Zeitstempel sind RFC 3161 konform und ebenfalls konform mit den Anforderungen aus ETSI EN 319 422.

Der Zeitstempeldienst wird in Deutschland betrieben und empfängt das Zeitsignal durch die gesetzlich gültige Zeit von der Physikalisch-Technische Bundesanstalt (PTB). Die Maximale Abweichung der Zeit zu UTC überschreitet in keinem Fall 1 Sekunde. Bei der Überschreitung der Abweichung von mehr 1 Sekunde, stellt der Zeitstempeldienst automatisch die Ausstellung von neuen Zeitstempeln ein. Schaltsekunden werden korrekt erkannt, protokolliert und bei der Ausstellung der Zeitstempel berücksichtigt.

Die Zeitstempel werden mit einem ausschließlich zu diesem Zweck erzeugten Schlüssel signiert. Nach Ablauf der Gültigkeitsdauer oder nach der Sperrung der privaten Schlüssel der dazugehörigen TSU werden keine Zeitstempel mehr mit diesem privaten Schlüssel ausgestellt.

4.7 Nicht-technische Sicherheitsmaßnahmen (Physical and environmental security)

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, ETSI EN 319 421 sowie CEN EN 419 241-1 regelmäßig wiederholt.

Ferner wurde dem Sicherheitsbereich des TSA 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.

4.8 Technische Sicherheitsmaßnahmen(Operation security)

Alle IT-Komponenten, welche im Rahmen von BVqtime 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 TSPS, eIDAS-VO, VDG, VDV, ETSI EN 319 401, ETSI EN 319 411-1, ETSI EN 319 411-2, ETSI EN 319 421 sowie CEN EN 419 241-1 betrieben werden. Dazu wird die Systemkonfiguration der eingesetzten Komponenten regelmäßig auf korrektheit geprüft. Das maximale Intervall zwischen zwei Überprüfungen der Systemkonfiguration beträgt ein Jahr.

Alle Mitarbeiter der TSA müssen die Arbeitseinweisungen der Vorgaben zur Computersicherheit einhalten. Defekte Datenträger werden nach einem sicheren Verfahren zerstört. Mitarbeiter der TSA 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 der übergeben werden.

4.9 Netzwerksicherheit (Network security)

Die IT-Systeme des TSA 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 behoben.

4.10 Behandlung von Vorfällen (Incident management)

Die TSA 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 der TSA eine kritische Schwachstelle oder eine Kompromittierung bekannt geworden ist, muss diese 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.

Die TSA 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.

4.11 Aufbewahrung von Beweismitteln (Collection of evidence)

Es wird zwischen Aufzeichnungen in elektronischer Form und papierbasierten Dokumenten unterschieden. Archiviert werden die vollständigen Antragsunterlagen (auch Folgeanträge), Dokumente zu Verfahrensrichtlinien, Zertifikate, Widerrufsdokumentation, elektronische Dateien, Protokolle zum Zertifikatslebenszyklus, Protokolle zum Lebenszyklus von TSU-Schlüsseln, TSU Zertifikate, Zeit Synchronisierung mit UTC und gegebenenfalls Erkennung von Synchronisationsverlusten. 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 NTP mind. täglich gegen die offizielle Zeit synchronisiert.

4.11.1 Aufbewahrungszeiten (Retention period for archive)

Dokumente zur Antragstellung und Prüfung, Daten zum Zertifikatslebenszyklus sowie die Zertifikate selbst, werden für die gesamte Betriebszeit des TSA aufbewahrt. Wird der Betrieb eingestellt, werden alle Dokumente und Daten entweder an die Institution, die den Dienst im Rahmen dieses TSPS übernehmen möchte, oder an die zuständige Aufsichtsbehörde übergeben.

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

4.11.2 Archivsicherheit (Protection of archive)

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

4.11.3 Datensicherung des Archivs (Archive backup procedures)

Die Sicherung der Daten erfolgt nach dem Stand der Technik.

4.11.4 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.

4.11.5 Ort der Archivierung (Archive collection system (internal or external))

Die Archivierung erfolgt intern bei der TSA.

4.11.6 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 der TSA.

4.12 Business continuity management (Business continuity management)

Je nach Art des Vorfalls entscheidet im Notfall der TSA über die Vorgehensweise nach einer Kompromittierung oder nach einem Katastrophenfall. Dieser entscheidet, wie der Betrieb wiederaufgenommen werden soll. Wenn der Betrieb wiederaufgenommen wird, entscheidet die TSA, ob eine Wiederherstellung der Backups der TSU 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.

4.13 Beendigungsplan (TSA termination and termination plans)

Für den Fall, dass die TSA den Betrieb einstellt, liegt ein Beendigungsplan vor, der regelmäßig auf Aktualität überprüft wird. Ist absehbar, dass der komplette Betrieb des TSP oder Teile davon eingestellt werden, so wird gemäß dem Beendigungplans verfahren. Der TSP hat zu prüfen, ob eine Übernahme des jeweiligen Dienstes durch einen anderen qualifizierten Vertrauensdiensteanbieter möglich ist. In dem Fall werden alle vom TSP ausgegebenen Zertifikate und Widerrufsinformationen für den zu beendenden Dienst in elektronischer Form an den neuen Vertrauensdiensteanbieter übergeben.

Ist eine Übernahme des Dienstes durch einen TSP ausgeschlossen, so werden alle vom TSP ausgegebenen Zertifikate und Widerrufsinformationen für den zu beendenden Dienst in elektronischer Form an die Bundesnetzagentur zur Übernahme in die Vertrauensinfrastruktur übergeben. Alle zu diesem Dienst zugehörigen Zeitstempelzertifikate werden vor der Übergabe an die Bundesnetzagentur widerrufen. Alle Zugriffsmöglichkeiten auf die entsprechende TSU CA und den dazugehörigen privaten Schlüssel werden beendet. Sobald sichergestellt ist, dass alle notwendigen Schritte aus dem Beendigungsplan geschehen sind, wird der Schlüsselspeicher (HSM) zerstört, so dass keine neuen Zertifikate ausgestellt werden können. Gegebenenfalls sind weitere Schritte mit der jeweiligen Aufsichtsbehörde abzustimmen.

Banken und vergleichbare Institutionen (Endprovider), die den Zeitstempeldienst integriert haben, werden rechtzeitig, gemäß der im Vertrag angegebenen Frist, über die Einstellung des Dienstes informiert.

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

4.14 Konformität (Compliance)

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

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

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

4.14.2 Identität/Qualifikation des Prüfers (Identity/qualifications of assessor)

Die TSA-spezifischen Konformitätsprüfungen werden von qualifizierten Dritten durchgeführt.

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

Die TSA wird von einer unabhängigen Konformitätsbewertungsstelle überprüft.

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

4.14.4 Abgedeckte Bereiche der Prüfung (Topics covered by assessment)

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

- Ausstellung von Zeitstempelzertifikate und Lebenszyklus der dafür genutztes Schlüssel
- Ausstellung von Zeitstempeln
- Re-Zertifizierungen
- Zertifikatswiderrufe
- Zutrittsschutz
- Berechtigungs- und Rollenkonzept
- Einbruchshemmende Maßnahmen
- Personal

In jedem Fall wird nach den jeweils gültigen Versionen der Audit-Kriterien nach eIDAS-VO, VDG, VDV, DSGVO, ETSI EN 319 401, ETSI EN 319 421 geprüft.

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

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

4.14.6 Mitteilung der Ergebnisse (Communication of results)

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

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

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

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

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

4.15.2 Anwendbares Recht (Governing law)

Es gilt deutsches Recht sowie das Recht der europäischen Union, der Gerichtsstand ist Köln.

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

5.1 7.1. Zertifikatsprofil (Certificate profile)

5.1.1 7.1.1. Versionsnummern (Version number(s))

Die Zertifikate werden im Format X.509v3 und gemäß ETSI EN 319 412-1 bis -5, ETSI EN 319 421, ETSI EN 319 422 ausgegeben.

5.1.2 Zertifikatserweiterungen (Certificate extensions)

5.1.2.1 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=1.3.6.1.4.1.50833.1.6.2 policyQualifier:policyQualifierId=1.3.6.1.5.5.7.2.1 policyQualifier:qualifier:cPSuRI= https://www.bank-verlag.de/bvtrust

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

5.1.2.2 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	Ca=FALSE, pathLenConstraint=None

Feld	OID	Kritisch	Beschreibung	Wert
			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=1.3.6.1.4.1.50833.1.6.2 policyQualifier:policyQualifierId=1.3.6.1.5.5.7.2.1 policyQualifier:qualifier:cPSuRI= https://www.bank-verlag.de/bvtrust
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.

5.1.2.3 EE-Zertifikate für Zeitstempel

EE-Zertifikate für Zeitstempel enthalten folgende Erweiterungen:

Feld	OID	Kritisch	Erforderlich	Beschreibung	Wert
keyUsage	2.5.29.15	ja	muss	Verwendungszweck	digitalSignature
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
extendedKeyUsage	2.5.29.37	ja	muss		1.3.6.1.5.5.7.3.8 (id-kp-timeStamping)
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/

Feld	OID	Kritisch	Erforderlich	Beschreibung	Wert
certificatePolicies	2.5.29.32	nein	muss	Verweis auf gültige Policy	policyIdentifier=1.3.6.1.4.1.50833.1.6.2 policyQualifier:policyQualifierId=1.3.6.1.5.5.7.2.1 policyQualifier:qualifier:cPSuRI = https://www.bank-verlag.de/bvtrust
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)

Ergänzende Erweiterungen können aufgenommen werden, müssen RFC 5280, RFC 6960, RFC 6818 und ETSI EN 319 412-1 bis -5, ETSI EN 319 421, ETSI EN 319 422 entsprechen oder in einem referenzierten Dokument beschrieben sein.