Vertrauensdiensteanbieter der Bundesagentur für Arbeit | 08.11.2023

Time-Stamping Authority Practice Statement der Bundesagentur für Arbeit

IT-Systemhaus

Inhaltsverzeichnis

1 Einleitung

1.1. Überblick

Die Bundesagentur für Arbeit (BA) hat seit dem 01.07.2016 für die Erstellung von qualifizierten elektronischen Zeitstempeln den Status eines qualifizierten Vertrauensdiensteanbieters (VDA) im Sinne der [eIDAS].

Die Nutzung dieser Zeitstempeldienste ist für Mitarbeiter und Verfahren im Rechtskreis SGB II oder SGB III frei. Die Nutzung der Zeitstempeldienste durch einen Mandanten impliziert eine *vorausgehende* vertragliche Vereinbarung zwischen der BA und der Institution (Mandant).

Ausgestellte qualifizierte Zeitstempel beruhen auf Dienstezertifikaten, die der Vertrauensdiensteanbieter (VDA) der BA selbst im Rahmen seiner Zertifizierungstätigkeit erstellt und verwaltet. Daher wird zunächst ein Überblick über die Zertifizierungstätigkeit des VDA der BA gegeben, vgl. [CPS].

Durch den VDA der BA ausgestellte Zertifikate können in zwei unterschiedliche Zertifikatshierarchien eingebunden sein.

- Die Legacy-Hierarchie
- Die Standard-Hierarchie.

Die folgende Grafik zeigt die Legacy-Hierarchie:

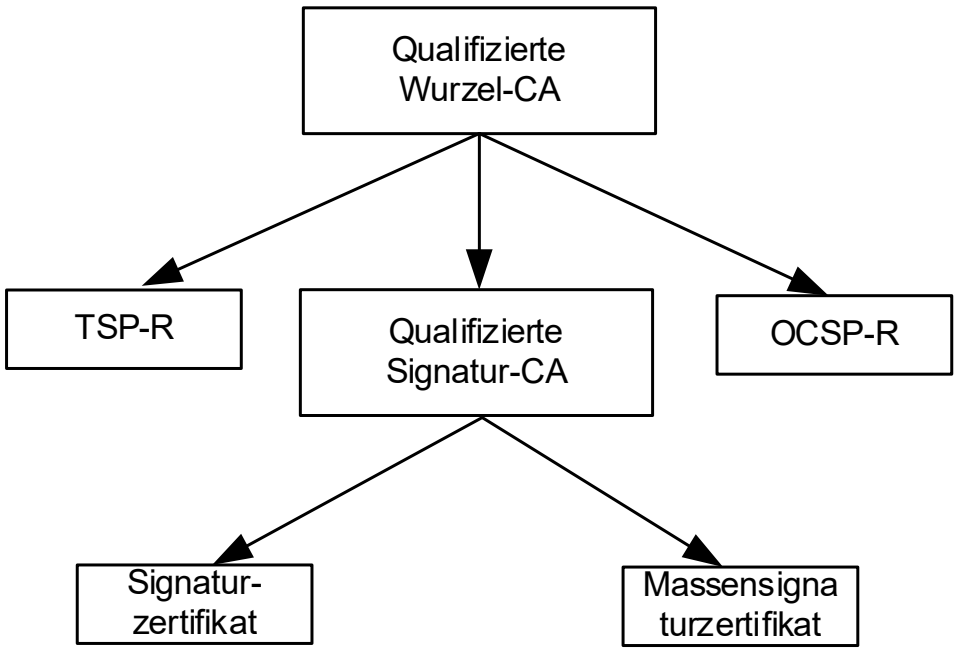
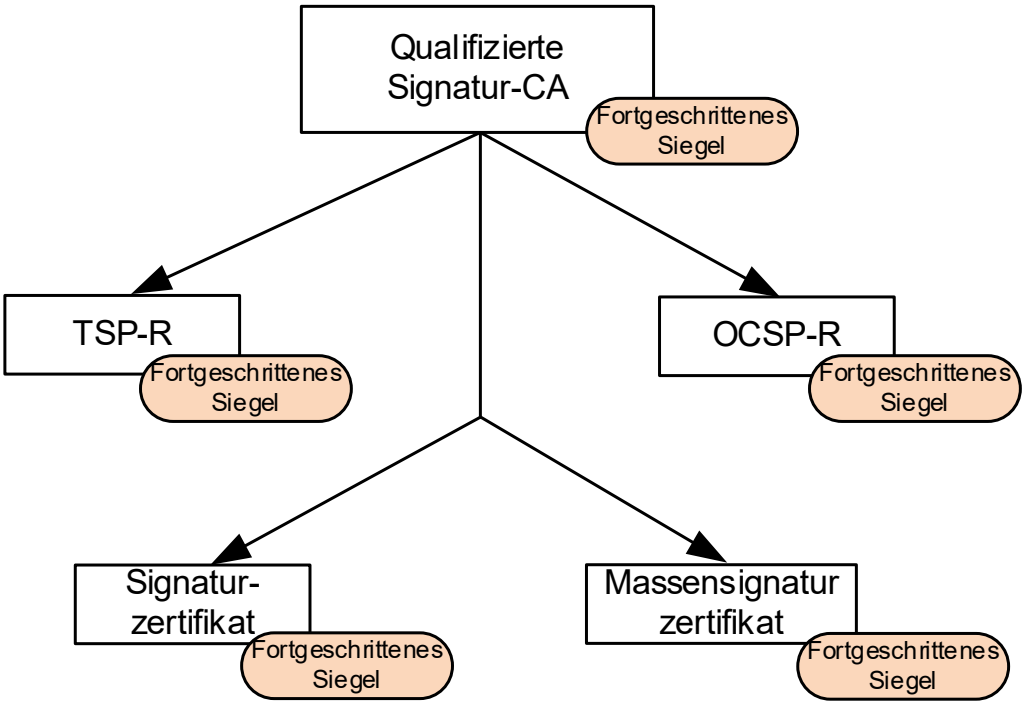


Abbildung 1 - qualifizierte Zertifikate in der Legacy-Hierarchie

Die beiden oberen Ebenen zeigen qualifizierte Zertifikate, die im Betrieb des Trustcenters (TCs) eingesetzt werden. Diese Zertifikate werden Dienstezertifikate genannt. Zu diesen Diensten gehören die Zeitstempeldienste (TSP-R in Abbildung 1). Alle Zertifikate der Legacy-Hierarchie sind qualifizierte Zertifikate für elektronische Signaturen nach [eIDAS]. Sie enthalten eine qualifizierte elektronische Signatur des VDA der BA.

Die Legacy-Hierarchie wird spätestens Ende 2023 außer Betrieb genommen. Die OCSP-Responder der Standard-Hierarchie beauskunften dann die Zertifikate der Legacy-Hierarchie.

Neue Zertifikate gehören dann zu folgender Standard-Hierarchie:



Die beiden oberen Ebenen zeigen nach wie vor Zertifikate, die im Betrieb des Trustcenters (TCs) eingesetzt werden. Diese Zertifikate werden nach wie vor Dienstezertifikate genannt. Im Unterschied zur Legacy-Hierarchie handelt es sich um Zertifikate für elektronische Siegel nach [eIDAS]. Die qualifizierten Dienste (qualifizierte Signatur-CA, TSP-R, OCSP-R) werden also durch nicht qualifizierte Zertifikate für elektronische Siegel gekennzeichnet.

Alle Zertifikate der Standardhierarchie enthalten ein fortgeschrittenes elektronische Siegel des VDA der BA. OCSP-Auskünfte und Zeitstempel aus der Standard-Hierarchie enthalten ebenfalls ein fortgeschrittenes elektronisches Siegel des VDA der BA.

Qualifizierte Zertifikate für elektronische Signaturen werden ausschließlich für Benutzer, z. B. Mitarbeiter der BA, ausgestellt. Diese Zertifikate werden, je nach Ausprägung, Signaturzertifikate oder Massensignaturzertifikate genannt.

Das Schlüsselpaar für die Erstellung und Prüfung eines fortgeschrittenen elektronischen Siegels bzw. einer qualifizierten elektronischen Signatur wird in der sicheren Umgebung des VDA der BA unter Verwendung einer qualifizierten Siegel- bzw. Signaturerstellungseinheit im Sinne der [eIDAS] erzeugt.

Vorliegendes Dokument ist das Time-Stamping Authority Practice Statement der Bundesagentur für Arbeit (TSAPS). Seine Kapitelstruktur wurde vom CPS der BA [CPS] übernommen. Sofern Kapitel des CPS für den Zeitstempeldienst nicht anwendbar sind, wird das entsprechend vermerkt oder das entsprechende Kapitel wird umgewidmet[1].

Entsprechend den Vorgaben des [CPS] und [RFC3647] legt das TSAPS die Praktiken dar, die der VDA bei der Beantragung, Generierung und Verwaltung qualifizierter Zeitstempel anwendet.

Es beschreibt, wie die Vorgaben der für die Zeitstempeltätigkeit maßgeblichen Policy BTSP aus [ETSI-POLTS] umgesetzt werden. Das vorliegende TSAPS ermöglicht somit eine qualitative Einschätzung der Zeitstempeltätigkeit des VDA der BA.

Sofern es nur seine Zertifizierungstätigkeit betrifft, wird der VDA in vorliegendem Dokument auch als Zertifizierungsdiensteanbieter bezeichnet.

[1] So wird etwa Kapitel 1.4 von „Anwendung von Zertifikaten“ zu „Anwendung von Zeitstempeln“

1.2. Dokumentidentifikation

Die Dokumentenbezeichnung für das vorliegende TSAPS lautet:

Time-Stamping Authority Practice Statement der Bundesagentur für Arbeit, Version: 2.1, Datum 23.06.2023

Das Dokument wird über den Object Identifier (OID) referenziert 1.3.6.1.4.1.21679.1.1.8.

1.3. Teilnehmer des Dienstes

1.3.1. Zeitstempelgeber

Die Zeitstempelgeber[2] werden durch den VDA der BA betrieben. Sie erstellen qualifizierte Zeitstempel.

Außerdem betreibt der VDA der BA einen Dienst zur sicheren Online-Abfrage von Informationen zum Sperrstatus der zugehörigen Dienstezertifikate.

1.3.2. Registrierungsinstanzen

Nicht relevant.

1.3.3. Antragsteller

1.3.3.1. Bezieher (Subscriber[3])

Bezieher eines Zeitstempels sind

- Mitarbeiter oder Fachverfahren der Rechtskreise SGB II oder SGB III und
- Mitarbeiter oder Fachverfahren des Mandanten.

1.3.3.2. Zertifikatsinhaber

Nicht relevant.

1.3.4. Vertrauende Dritte (Relying Parties)

- BA-interne oder BA-externe Empfänger von Daten oder Dokumenten, die einen qualifizierten Zeitstempel des VDA der BA tragen.

1.3.5. Weitere Teilnehmer

Keine.

1.4. Anwendung von Zeitstempeln

1.4.1. Zulässige Anwendung von Zeitstempeln

Die von der BA ausgestellten qualifizierten Zeitstempel erfüllen die Anforderungen der [eIDAS] an qualifizierte elektronische Zeitstempel. Insbesondere haben diese Zeitstempel folgende Rechtswirkung:

(1) Einem elektronischen Zeitstempel darf die Rechtswirkung und die Zulässigkeit als Beweismittel in Gerichtsverfahren nicht allein deshalb abgesprochen werden, weil er in elektronischer Form vorliegt oder nicht die Anforderungen an qualifizierte elektronische Zeitstempel erfüllt.

(2) Für qualifizierte elektronische Zeitstempel gilt die Vermutung der Richtigkeit des Datums und der Zeit, die darin angegeben sind, sowie der Unversehrtheit der mit dem Datum und der Zeit verbundenen Daten.

---

[2] Time-Stamping Unit im Sinne von [ETSI-POLTS]

[3] subscriber: legal or natural person to whom a time-stamp is issued and who is bound to any subscriber obligations, vgl. [ETSI-POLTS]

(3) Ein in einem Mitgliedstaat ausgestellter qualifizierter elektronischer Zeitstempel wird in allen anderen Mitgliedstaaten als qualifizierter elektronischer Zeitstempel anerkannt.

Qualifizierte elektronische Zeitstempel dürfen dabei ausschließlich für dienstliche Zwecke verwendet werden. Für die Einschränkung der Verwendung von Zeitstempeln durch Mitarbeiter oder Fachverfahren eines Mandanten ist der Mandant verantwortlich.

Weitergehende Einschränkungen können sich aus mitgeltenden Dokumenten ergeben. In Frage kommen hier BA-interne Weisungen oder vertragliche Vereinbarungen, Gesamtkatalog der BA für gemeinsame Einrichtungen, Verwaltungsvereinbarung mit Mandanten.

Sofern der Bedarf für langfristige Beweiserhaltung besteht, sind gemäß §15 [VDG] qualifiziert elektronisch signierte, gesiegelte oder zeitgestempelte Daten durch geeignete Maßnahmen neu zu schützen, bevor der Sicherheitswert der vorhandenen Signaturen, Siegel oder Zeitstempel durch Zeitablauf geringer wird. Die neue Sicherung muss nach dem Stand der Technik erfolgen.

1.4.2. Unzulässige Anwendung von Zeitstempeln

Insbesondere gelten folgende Nutzungsbeschränkungen und -verbote:

- Zeitstempel sind nicht zur Verwendung oder zum Weitervertrieb als Kontroll- oder Steuerungseinrichtung in gefährlichen Umgebungen oder für Verwendungszwecke, bei denen ein ausfallsicherer Betrieb erforderlich ist bzw. der Betrieb von nuklearen Einrichtungen, Flugzeugnavigations- oder Kommunikationssystemen, Luftverkehrs-Kontrollsystemen oder Waffenkontrollsystemen, wobei ein Ausfall direkt zum Tode, zu Personenschäden oder zu schweren Umweltschäden führen kann, vorgesehen oder darauf ausgelegt. Eine Verwendung zu solchen Zwecken wird ausdrücklich ausgeschlossen.

1.5. Policy-Verwaltung

1.5.1. Organisation für die Verwaltung dieses Dokuments

Die Verwaltung des Dokuments erfolgt durch den VDA der BA. Informationen zur Änderung der Richtlinie finden Sie in Abschnitt 9.12. Für Kontaktinformationen zum VDA siehe Abschnitt 1.5.2.

1.5.2. Kontaktperson

Die Revision und Freigabe des vorliegenden TSAPS unterliegt der ausschließlichen Verantwortung des VDA der BA.

Ansprechpartner für Fragen bezüglich dieses TSAPS ist:

Bundesagentur für Arbeit
IT-Systemhaus
Vertrauensdiensteanbieter
Regensburger Straße 104
90478 Nürnberg
Internet: https://www.pki.arbeitsagentur.de/
E-Mail: IT-Systemhaus.Vertrauensdienste@arbeitsagentur.de

1.5.3. Zuständigkeit für die Abnahme des TSAPS

Für die Verabschiedung dieses TSAPS ist die VDA-Leitung zuständig. Zur Gültigkeit des TSAPS siehe Abschnitt 9.10.

1.5.4. Abnahmeverfahren des TSAPS

Das TSAPS wird bei Bedarf durch den VDA der BA fortgeschrieben, vgl. Abschnitt 9.12. Nach einer Eignungsprüfung durch den Datenschutzbeauftragten und die Rechtsabteilung wird sie von der VDA-Leitung abgenommen.

1.6. Definition und Abkürzungen

Definitionen und Abkürzungen stehen am Ende des Dokumentes.

2 Veröffentlichung und Verzeichnisdienst

2.1. Verzeichnisdienste

Der VDA der BA betreibt die folgenden Verzeichnisdienste:

- Auf einer Webseite des VDA der BA werden Informationen des VDA wie Kontaktinformationen, TSAPS, und die Dienstezertifikate veröffentlicht. Die Webseite ist unter der URL
  https://www.pki.arbeitsagentur.de/
  erreichbar.
- Über einen OCSP-Verzeichnisdienst kann der Status von qualifizierten Zertifikaten und Dienstezertifikaten abgerufen werden. Sofern der Zertifikatsinhaber zugestimmt hat, kann über den OCSP-Verzeichnisdienst auch das qualifizierte Zertifikat abgerufen werden. Die Verbindungsparameter des OCSP-Verzeichnisdienstes werden auf oben genannter Webseite veröffentlicht. Weitere Informationen zum OCSP-Verzeichnisdienst befinden sich in Abschnitt 4.10.
- Über einen Verzeichnisdienst können die Zertifikate der qualifizierten Signatur-CAs abgerufen werden. Der zugehörige Abrufpfad ist ab 2023 in den Endbenutzerzertifikaten hinterlegt.

2.2. Veröffentlichung von Zertifikatsinformationen

Die folgende Tabelle gibt einen Überblick über die durch den VDA der BA veröffentlichten Informationen sowie deren Veröffentlichungsort.

Zertifikatstyp	veröffentlicht in	Link
Qualifizierte Zertifikate und Dienstezertifikate	OCSP-Verzeichnis	http://ocsp.pki.arbeitsagentur.de/
Sperrstatusinformationen für qualifizierte Zertifikate und Dienstezertifikate	OCSP-Verzeichnis	http://ocsp.pki.arbeitsagentur.de/
Zertifikat und zugehöriger Hashwert (Fingerprint) der CA	Web-Verzeichnis	https://www.pki.arbeitsagentur.de/
Signatur-CA-Zertifikate	LDAP/Web-Verzeichnis	Ab 2023 als AIA-Pfad im Endbenutzerzertifikat
Zertifikat und zugehöriger Hashwert (Fingerprint) des OCSP-Responders (Auskunftsdienst)	Web-Verzeichnis	https://www.pki.arbeitsagentur.de/
Zertifikat und zugehöriger Hashwert (Fingerprint) des TSP-Responders (Zeitstempeldienst)	Web-Verzeichnis	https://www.pki.arbeitsagentur.de/
CP für qualifizierte Zertifikate	Web-Verzeichnis	https://www.pki.arbeitsagentur.de/
TSAPS (vorliegendes Dokument)	Web-Verzeichnis	https://www.pki.arbeitsagentur.de/

Tabelle 1 - Veröffentlichte Informationen

Das Sicherheitskonzept des VDA der BA sowie die technischen Spezifikationen, Betriebskonzepte und Arbeitsanweisungen enthalten vertrauliche Informationen und werden daher weder im Intranet noch im Internet veröffentlicht.

2.3. Häufigkeit und Zyklen für Veröffentlichungen

Vor der Verwendung wird ein Dienstezertifikat veröffentlicht.

Die Veröffentlichung des TSA Practice Statements erfolgt jeweils nach der Freigabe der aktualisierten Version. Aktualisierungen des TSAPS werden in Kap. 9.12 behandelt.

2.4. Zugriffskontrolle auf Verzeichnisse

Die im Internet veröffentlichte Information ist öffentlich zugänglich. Der Lesezugriff auf den Verzeichnisdienst ist also nicht beschränkt. Dagegen haben nur berechtigte Rollenträger oder Systeme Änderungsrechte für den Verzeichnisdienst.

Die BA hat entsprechende Sicherheitsmaßnahmen implementiert, um ein unbefugtes Ändern von Einträgen in den Verzeichnisdiensten zu verhindern.

3 Identifizierung und Authentisierung

3.1. Namensgebung

Nachfolgende Beschreibungen erläutern die in Dienstezertifikaten verwendeten Namen.

3.1.1. Namenstypen

Es gelten die Regelungen des Standard [X509] bzw. seiner Profilierung in [RFC5280] bzw. dessen Profilierung in [COMPKI]. Zertifikatsprofile finden sich in Abschnitt 7.1.

3.1.2. Anforderungen an die Bedeutung von Namen

Es gelten die Regelungen des Standard [X509] bzw. seiner Profilierung in [RFC5280] bzw. dessen Profilierung in [COMPKI].

Für das Feld `Subject` gelten zusätzlich folgende Festlegungen:

- Attribut `CountryName`: <DE>
- Attribut `Organization`: <Bundesagentur fuer Arbeit>
- Attribut `CommonName` (CN): Bei Dienstekarten enthält der CN in jedem Fall ein Pseudonym, vgl. Abschnitt 3.1.3.
- Attribut `SerialNumber`: Nur in Dienstezertifikaten der Legacy-Hierarchie[4]. Der Wert wird vom VDA der BA generiert und bezeichnet den Zertifikatsinhaber eindeutig. Zu seiner Bestimmung werden Vorname, zweiter Vorname, Geburtsname, Geburtsort und Geburtsdatum des Zertifikatsinhabers benutzt.

3.1.3. Anonymität und Pseudonyme für Zertifikatsinhaber

Für die Dienstezertifikate werden, abhängig von der CA-Hierarchie, unterschiedliche Zertifikate eingesetzt:

• In der Legacy-Hierarchie werden für die benötigten qualifizierten Zertifikate der CA sowie des OCSP-Responder und des Zeitstempeldienstes (Dienstezertifikate) auf Mitarbeiter des Zertifizierungsdienstes (Rolle Sicherheitsoffizier) ausgestellte Zertifikate verwendet. Die Sicherheitsoffiziere können anhand des Attributes SerialNumber im Feld Subject des Dienstezertifikates identifiziert werden. Dienstezertifikate tragen ein Pseudonym im Attribut CommonName des Subject, das mit dem Suffix „:PN“ gekennzeichnet ist.

• In der Standard-Hierarchie werden für die benötigten Zertifikate der CA sowie des OCSP-Responder und des Zeitstempeldienstes (Dienstezertifikate) Zertifikate für elektronische Siegel eingesetzt. Dienstezertifikate tragen ein Pseudonym im Attribut CommonName des Subject, das mit dem Suffix „:PN“ gekennzeichnet ist.

3.1.4. Regeln zur Interpretation verschiedener Namensformen

Es gelten die Regelungen des Standard [X509] bzw. seiner Profilierung in [RFC5280] bzw. dessen Profilierung in [COMPKI].

3.1.5. Eindeutigkeit von Namen

Qualifizierte Zertifikate können anhand des Attributes `SerialNumber` im Feld `Subject` eindeutig ihrem Inhaber zugeordnet werden. Aufgrund der Generierung der `SerialNumber`, vgl. Abschnitt 3.1.2, sind verschiedenen Personen verschiedene Werte der `SerialNumber` zugeordnet.

4 Bei Dienstezertifikaten der Standard-Hierarchie handelt es sich um Siegelzertifikate.

3.1.6. Erkennung, Authentisierung und Rolle von geschützten Namen

Der Namensraum der verwendeten Pseudonyme in den Dienstezertifikaten wird vom Zertifizierungsdienst geprüft und freigegeben.

3.2. Erstmalige Identitätsprüfung

Nicht relevant.

3.3. Identifizierung und Authentifizierung bei Schlüsselerneuerung

Nicht relevant.

3.4. Identifizierung und Authentifizierung beim Sperrantrag

Nicht relevant.

3.5. Identifizierung und Authentifizierung beim Antrag auf Schlüsselwiederherstellung

Nicht relevant.

4 Anforderungen an den Lebenszyklus des Zeitstempels

4.1. Antragstellung für Zeitstempel

4.1.1. Wer kann einen Zeitstempel beantragen

Die zulässigen Antragsteller sind in Abschnitt 1.3.3 aufgeführt.

4.1.2. Antragsprozess und Verantwortlichkeiten

Vor der Nutzung durch einen Mandanten ist eine vertragliche Vereinbarung zwischen der BA und dem Mandanten erforderlich. Nach Abschluss der Vereinbarung wird der Mandant vom VDA der BA technisch berechtigt, den Zeitstempeldienst zu nutzen. Mitarbeiter oder Fachverfahren der Rechtskreise SGB II oder SGB III sind per se nutzungsberechtigt.

Die Beantragung eines Zeitstempels erfolgt durch Übermittlung einer entsprechenden Anfrage an den Zeitstempeldienst.

4.2. Antragsbearbeitung

4.2.1. Durchführung der Identifikation und Authentifizierung

Der Mandant wird anhand der vereinbarten Merkmale authentifiziert. Denkbar ist die Nutzung eines definierten IP-Bereiches.

4.2.2. Annahme bzw. Ablehnung des Antrags

Anträge werden in folgenden Fällen abgelehnt:

- Der Antragsteller ist nicht berechtigt (siehe Abschnitt 4.1.1).
- Die notwendige vertragliche Vereinbarung bzw. der Einkauf der entsprechenden Dienstleistung fehlt (siehe Abschnitt 4.1.2).
- Die gestellte Anfrage an den Zeitstempeldienst ist nicht korrekt.

Sofern der Antrag angenommen wird, erstellt das System automatisiert einen Zeitstempel und übermittelt ihn an den Antragsteller.

4.2.3. Fristen für die Antragsbearbeitung

Kategorie	Zugesagter Wert
Servicezeit	Mo – Do: 6:30 bis 18:00 Uhr Fr: 6:30 bis 16:00 Uhr nicht an bundeseinheitlichen Feiertagen sowie an BA arbeitsfreien Tagen
Erreichbarkeitszeit	Mo – Do: 6:30 bis 18:00 Uhr Fr: 6:30 bis 16:00 Uhr nicht an bundeseinheitlichen Feiertagen
Ausfallzeit	8 Stunden im Monat
Wiederherstellzeit	max. 8 Stunden während der Servicezeit
Gesamtverfügbarkeit pro Jahr	96,3%

Tabelle 2 - Fristen für die Antragsbearbeitung

4.3. Zertifikatserstellung

Nicht relevant.

4.4. Zertifikatsannahme

Nicht relevant.

4.5. Nutzung des Zeitstempels

4.5.1. Nutzung durch den Zertifikatsinhaber

Nicht relevant.

4.5.2. Nutzung durch vertrauende Dritte

Vertrauende Dritte sollten einem Zeitstempel des VDA der BA nur dann vertrauen, wenn dieser auf Basis der Dienstezertifikate des VDA der BA geprüft werden kann.

Bei der Prüfung von qualifizierten Zertifikaten ist zur Prüfung das Kettenmodell gemäß [COMPKI] SiG-Profiles anzuwenden.

Vor dem Vertrauen auf einen Zeitstempel hat der vertrauende Dritte folgendes zu prüfen:

- den Sperrstatus des Dienstezertifikats und aller darüber liegenden CA-Zertifikate der Zertifizierungskette. Bei qualifizierten Zertifikaten entsprechend den Status der Zertifikate zum Zeitpunkt der Signaturerstellung,
- die Eignung der Nutzung eines Zertifikats für einen bestimmten Zweck, der durch das vorliegende TSAPS und [CPS] nicht verboten oder anderweitig beschränkt ist,
- dass die Nutzung des Zertifikats den im Zertifikat enthaltenen KeyUsage-Felderweiterungen entspricht.

Der vertrauende Dritte hat sich zudem regelmäßig auf der Webseite des Vertrauensdienstes, siehe Abschnitt 2.1, und bei der Aufsichtsstelle im Sinne der [eIDAS] zu informieren.

4.6. Zertifikatserneuerung unter Beibehaltung des alten Schlüssels (Re-Zertifizierung)

Nicht relevant.

4.7. Schlüssel- und Zertifikatserneuerung (Re-Key)

Nicht relevant.

4.8. Zertifikatsmodifizierung

Nicht relevant.

4.9. Sperrung und Suspendierungen von Zertifikaten

4.9.1. Gründe für eine Sperrung

Ein Dienstezertifikat ist in den folgenden Fällen zu sperren:

- Wenn der Zertifikatsinhaber seine privaten Schlüssel nicht mehr nutzen kann oder der Verdacht auf Kompromittierung besteht.
- Wenn der Verdacht besteht, dass die für die Erzeugung und Anwendung der privaten Schlüssel eingesetzten Algorithmen und Geräte keine ausreichende Sicherheit mehr bieten.
- Wenn ein Sperrberechtigter nach 4.9.2 es verlangt.

Wenn die BA ihren Zeitstempeldienst einstellt, werden sämtliche dafür genutzten Dienstezertifikate gesperrt (siehe Abschnitt 5.8).

4.9.2. Sperrberechtigte

Die folgenden Stellen sind berechtigt, die Sperrung von Dienstezertifikaten zu beantragen:

- Zertifikatsinhaber
- die zuständige Aufsichtsstelle nach [eIDAS]
- VDA-Leitung, TC-Leitung.

4.9.3. Verfahren zur Sperrung

Es sind folgende Verfahren für die Sperrung von Zertifikaten definiert:

- **Sperrung von Dienstezertifikaten:** Ein Sperrberechtigter stellt einen schriftlichen Sperrauftrag. Die Durchführung erfolgt im 4-Augen-Prinzip in der sicheren Umgebung des VDA.

In der folgenden Tabelle ist angegeben, über welche Kanäle Sperrberechtigte die Sperrung veranlassen können.

Antragsteller	Telefon (UHD)	Schriftlich	LRA
Inhaber		✓	
Sperrung von Amts wegen			
Vertrauensdiensteanbieter		✓	
BNetzA		✓	

Tabelle 3 - Zuordnung der Sperrberechtigungen zu den Sperrmöglichkeiten

4.9.4. Fristen für die Beantragung einer Sperrung

Der Sperrberechtigte, vgl. Abschnitt 4.9.2, muss bei Vorliegen entsprechender Gründe unverzüglich die Sperrung initiieren.

4.9.5. Bearbeitungszeit für Anträge auf Sperrung

Schriftliche Sperranträge werden unverzüglich bearbeitet.

4.9.6. Prüfung des Zertifikatsstatus durch Dritte

Vertrauende Dritte müssen bei der Prüfung von Zeitstempeln den Sperrstatus der Dienstezertifikate über die angebotenen Verzeichnisdienste aus Abschnitt 2 prüfen.

4.9.7. Periode für die Erstellung der Sperrlisten

Für qualifizierte Zertifikate werden keine Sperrlisten veröffentlicht.

4.9.8. Maximale Latenz der Sperrlisten

Für qualifizierte Zertifikate werden keine Sperrlisten veröffentlicht.

4.9.9. Verfügbarkeit von Online-Sperrinformationen

Der VDA der BA bietet den OCSP-Verzeichnisdienst für die Online-Prüfung von qualifizierten Zertifikaten an (siehe Abschnitt 2.1). Dieser ist hochverfügbar (24x7).

4.9.10. Nutzung der Online-Sperrinformationen durch Dritte

Vertrauende Dritte müssen bei der Prüfung von qualifizierten Zertifikaten den Sperrstatus über den OCSP-Verzeichnisdienst prüfen. Für die Verbindungsparameter siehe Abschnitt 2.

4.9.11. Andere verfügbare Formen der Bekanntmachung von Sperrinformationen

Keine.

4.9.12. Spezielle Anforderungen bei Kompromittierung privater Schlüssel

Keine.

4.9.13. Gründe für die Suspendierung

Eine Suspendierung (gemeint ist die Aussetzung im Sinne der [eIDAS], also der vorübergehende Verlust der Gültigkeit) von ausgestellten Zertifikaten wird nicht unterstützt. D.h., die Sperrung eines Zertifikates ist immer endgültig und kann nicht aufgehoben werden.

4.9.14. Wer kann eine Suspendierung beantragen

Es ist keine Suspendierung von Zertifikaten möglich, siehe Abschnitt 4.9.13.

4.9.15. Verfahren zur Suspendierung

Es ist keine Suspendierung von Zertifikaten möglich, siehe Abschnitt 4.9.13.

4.9.16. Maximale Sperrdauer bei Suspendierung

Es ist keine Suspendierung von Zertifikaten möglich, siehe Abschnitt 4.9.13.

4.10. Auskunftsdienste über den Zertifikatsstatus

4.10.1. Betriebseigenschaften

Der Auskunftsdienst für den Sperrstatus qualifizierter Zertifikate basiert auf dem Online Certificate Status Protocol (OCSP).

Die Verbindungsparameter des OCSP-Verzeichnisdienstes werden auf der in Abschnitt 2.1 genannten Webseite veröffentlicht. Aktuell ist der OCSP-Verzeichnisdienst über die URL

http://ocsp.pki.arbeitsagentur.de

erreichbar.

Der OCSP-Verzeichnisdienst verwendet als Übertragungsprotokoll HTTP und implementiert das Online Certificate Status Protocol (OCSP) gemäß [RFC2560] und [COMPKI] mit den folgenden Eigenschaften:

- Die Anfragen (OCSP-Requests) müssen nicht signiert sein; signierte Anfragen werden jedoch auch unterstützt.
    - Die Hash-Werte in den Anfragen (Felder issuerNameHash und issuerKeyHash) müssen mit SHA-1 erstellt worden sein.
- Auskünfte des OCSP-Verzeichnisdienstes werden
    - innerhalb der Legacy-Zertifikatshierarchie mit einer qualifizierten elektronischen Signatur unterzeichnet.
    - innerhalb der Standard-Zertifikatshierarchie mit einem fortgeschrittenen elektronischen Siegel versiegelt.
- Das verwendete Dienstezertifikat und alle zugehörigen CA-Zertifikate der Hierarchie werden vom OCSP-Responder im Feld certs der BasicResponse der Antwort mitgeliefert.

- Das Feld `nextUpdate` in `SingleResponse` wird nicht verwendet.
- Sperrgründe werden nicht in der Antwort mitgegeben.
- Die unterstützten Erweiterungen sind in Abschnitt 7.3.2 angegeben.
- Statusinformationen zu einem qualifizierten Zertifikat werden über den Ablauf seiner Gültigkeitsdauer hinaus bereitgestellt, siehe dazu die Erweiterung `ArchiveCutoff` in Abschnitt 7.3.2.

4.10.2. Verfügbarkeit

Der OCSP-Verzeichnisdienst hat eine zugesicherte Verfügbarkeit von 99,80 Prozent.

4.10.3. Optionale Funktionen

Der OCSP-Verzeichnisdienst unterstützt die folgenden optionalen Funktionen:

- Eine Anfrage an den OCSP-Verzeichnisdienst für den Zertifikatsstatus kann die Erweiterung `Nonce` enthalten. Diese Extension dient der Vorbeugung gegen Angriffe durch Senden alter Antworten (Replay-Attacks). Der in der Anfrage übergebene Wert wird vom Auskunftsdienst in die Extension `Nonce` der Antwort kodiert.
- Eine Anfrage an den OCSP-Verzeichnisdienst kann für den Zertifikatsstatus die spezielle Erweiterung `RetrieveIfAllowed` aus dem SigG-Profile[5] von [COMPKI] enthalten. In diesem Fall kodiert der OCSP-Verzeichnisdienst das Zertifikat, dessen Status abgefragt wurde, gemäß dem SigG-Profile von [COMPKI] in die spezielle Erweiterung `RequestedCertificate` der Antwort.

4.11. Ende der Nutzung (End of subscription)

Die Nutzung des Dienstes endet, wenn

- der Bezieher aus dem Dienst der BA ausscheidet,
- das Arbeitsverhältnis des Beziehers als Mitarbeiter der gemeinsamen Einrichtung nach SGB II endet,
- das Fachverfahren eingestellt wird,
- das Dienstleitungsverhältnis zwischen der BA und dem Mandanten beendet wird.

Bei Beendigung des Dienstleistungsverhältnisses wird der Zugriff des Mandanten auf den Zeitstempeldienst gesperrt. Die genauen Modalitäten werden zwischen den Vertragspartnern geregelt.

4.12. Schlüsselhinterlegung und –wiederherstellung

Nicht relevant

[5] Zur Bezeichnung vgl. den zugehörigen Eintrag in Kapitel 11

5 Infrastrukturelle, organisatorische und personelle Sicherheitsmaßnahmen

5.1. Infrastrukturelle Sicherheitsmaßnahmen

5.1.1. Lage und Konstruktion des Standortes

Die Vertrauensdienste werden an zwei räumlich getrennten Standorten betrieben:

- Der Hauptstandort - an diesem Standort wird die produktive Infrastruktur der Vertrauensdienste betrieben.
- Der Backupstandort - an diesem Standort wird die Backup-Infrastruktur der Vertrauensdienste betrieben.

An beiden Standorten gewährleisten bauliche Maßnahmen einen hohen Schutz gegen unbefugtes Eindringen, unbefugten Zutritt und Zugriff sowie unbefugte Einsichtnahme auf die sicherheitsrelevanten Einrichtungen des VDA der BA. Diese Maßnahmen sind im Sicherheitskonzept des VDA der BA dargelegt. Das Gebäude ist zum angrenzenden öffentlichen Bereich durch einen Perimeterschutz begrenzt (Hauptstandort) bzw. grenzt mit der einzigen Fensterfront an einen nicht frei zugänglichen Innenhof der Liegenschaft (Backupstandort). Beide Standorte verfügen über eine eigene Einbruchmeldeanlage (EMA), die von der Sicherheitszentrale am Hauptstandort auf Alarm- und Stördaten 7x24 überwacht wird. Die Sicherheitszentrale verständigt im Bedarfsfall die Polizei. Die einzelnen Räume beider Standorte werden mit Bewegungsmeldern überwacht. Der Hauptstandort unterliegt zusätzlich einer regelmäßigen Kontrolle durch den Wachdienst. An beiden Standorten gibt es in den normal zugänglichen Lageplänen keine Hinweise auf die Räumlichkeiten des VDA der BA.

5.1.2. Zutrittskontrolle

In den beiden Standorten gewährleisten umfassende mehrstufige Maßnahmen zur Zutrittskontrolle einen hohen Schutz gegen unbefugtes Eindringen in die einzelnen Räume und unbefugten Zugriff auf die sicherheitskritischen Systeme und Daten. Diese Maßnahmen sind im Detail im Sicherheitskonzept des VDA der BA dargelegt. Zu beiden Standorten ist der Zutritt ausschließlich über eine alarmüberwachte Personenvereinzelungsschleuse (PVE) möglich. Zusätzlich zur PVE ist eine ständig verschlossene und überwachte Tür zur Flucht und Lieferung installiert. Alle Zutritte werden über eine eigene Zutrittskontrollanlage protokolliert. Die PVE sowie die Flucht- bzw. Liefertür werden videoüberwacht.

Der Zutritt zu einzelnen Räumen beider Standorte selbst, die jeweils in mehrere Zutrittszonen unterteilt sind, kann nur mit Hilfe eines Identifikationsmerkmalträgers (Zutrittskarte, Besitz und Wissen) erfolgen. Zutritt ist nur berechtigten Personen möglich, zu bestimmten Bereichen wird ein Zugang nur im 4-Augen-Prinzip je nach Rolle gewährt. Techniker- oder Besucherzutritte erfolgen nur in Begleitung eines autorisierten Rolleninhabers.

Die Leitung des VDA der BA hat gegenüber allen Rolleninhabern des Vertrauensdienstes bzgl. ihrer Tätigkeiten innerhalb des VDA fachliche Weisungsbefugnis.

5.1.3. Stromversorgung und Klimakontrolle

Die beiden Standorte des Vertrauensdienstes sind jeweils mit einer unterbrechungsfreien Stromversorgung und Schutzeinrichtungen gegen Überspannung ausgestattet. Am Hauptstandort gewährleistet eine zweite Stromeinspeisung von einem redundanten Umspannwerk sowie eine automatische Umschaltung eine unabhängige und redundante Stromversorgung. Beide Standorte sind zusätzlich über dedizierte unterbrechungsfreie Stromversorgungen (USV) mit ausreichender Kapazität abgesichert.

Haupt- und Backupstandort sind mit eigenen, zentral überwachten redundanten Klimaanlagen ausgestattet.

5.1.4. Schutz vor Wasserschäden

Es befinden sich keine fließenden oder stehenden Gewässer in räumlicher Nähe der beiden Standorte. Passiver Wasserschutz ist durch entsprechende Boden- und Rackbauweise sowie zusätzliche Wasserdetektion und automatische Abschaltung gewährleistet.

5.1.5. Brandschutz

An beiden Standorten wird der Brandschutz durch umfassende aktive, passive und organisatorische Maßnahmen realisiert. Diese sind im Sicherheitskonzept des VDA der BA dargelegt. Dazu gehören u. a. die Verwendung entsprechender Baumaterialien, die Aufteilung auf Brandabschnitte, die Brandfrüherkennung und –alarmierung über Rauchmelder sowie die ereignisgesteuerte Brandlöschung des jeweiligen Objektes. Die Überwachung erfolgt am ständig besetzten Hauptstandort. Zusätzlich wird die Feuerwehr im Zweischleifenprinzip alarmiert.

5.1.6. Lagerung von Datenträgern

Datenträger mit sicherheitskritischen Informationen werden in verschlossenen Behältnissen aufbewahrt. Datenträger mit besonders kritischen Informationen werden ausschließlich in Tresoren aufbewahrt.

5.1.7. Entsorgung von Datenträgern

Sämtliche für sicherheitskritische Systeme oder Informationen des VDA der BA genutzte Datenträger und Smartcards werden vor der Entsorgung sicher gelöscht oder physikalisch unbrauchbar gemacht. Papierdokumente, die vertrauliche Informationen enthalten, werden mindestens gemäß DIN 32757 Sicherheitsstufe 3 entsorgt.

5.1.8. Ausgelagertes Backup

An beiden Standorten wird regelmäßig ein Backup der Produktionsdaten durchgeführt. Die Datensicherung umfasst die ausgestellten Zeitstempel, die Protokolldaten und weitere wichtige Daten. Die Backupdatenträger werden sicher aufbewahrt (siehe Abschnitt 5.1.6) und verlassen die gesicherten Bereiche nur unter Maßgabe gemäß Abschnitt 5.1.7.

5.2. Organisatorische Sicherheitsmaßnahmen

5.2.1. Sicherheitskritische Rollen

Sicherheitskritische Tätigkeiten im VDA der BA sind Rollen zugeordnet, die in einem internen Rollenkonzept beschrieben werden. Diese Tätigkeiten dürfen ausschließlich von Personen durchgeführt werden, die den entsprechenden Rollen zugewiesen sind. Die Anzahl der Rolleninhaber ist auf die notwendige Zahl beschränkt.

5.2.2. Anzahl benötigter Personen bei sicherheitskritischen Aufgaben

Besonders kritische Tätigkeiten werden ausschließlich unter Mitwirkung einer zweiten Person (4-Augen-Prinzip) durchgeführt.

5.2.3. Identifikation und Authentisierung von Rollen

Die Identifikation und Authentisierung der Rolleninhaber erfolgt beim Zutritt zu sicherheitsrelevanten Räumen durch eine Smartcard mit zugehöriger individueller PIN sowie beim Zugriff auf besonders sicherheitsrelevante Systeme mit Hilfe eines zwischen den jeweilig berechtigten Rolleninhabern geteilten Passwortes. Für Systeme im Trustcenter, die keine Smartcard-Authentisierung unterstützen, erfolgt eine rollenspezifische Anmeldung über personalisierte Accounts mit Benutzername und Passwort. Eine Anmeldung mit administrativen Gruppenkonten ist nicht gestattet. Die Passwörter unterliegen einer Passwortpolicy.

5.2.4. Trennung von Rollen und Aufgaben

Grundsätzlich können Mitarbeiter des Vertrauensdienstes mehrere Rollen einnehmen. Für die Sicherheit ist es jedoch unerlässlich, gewisse Rollen personell zu trennen.

Dem Rollenkonzept liegen die folgenden Basisregeln und Rollenausschlüsse zugrunde:

- Leitende Rollen dürfen keine operativen oder administrativen Rollen übernehmen.
- Kontrollierende und beratende Rollen dürfen keine operativen oder administrativen Rollen übernehmen.
- Administrative Rollen dürfen keine operativen Rollen übernehmen.

Die Einhaltung der Rollenausschlüsse wird bei der Benennung der Rolleninhaber geprüft. Ein Rollenwechsel ist *nicht* möglich, wenn dadurch die Einhaltung des Rollenkonzeptes über die Zertifikatsprozesse gefährdet ist. Deshalb wird über den Rollenwechsel einer Person immer im Einzelfall entschieden. Sicherheitskritische Tätigkeiten werden im 4-Augen-Prinzip und durch die definierten Rolleninhaber unter Einhaltung der vorgegebenen Prozesse durchgeführt.

5.3. Personelle Sicherheitsmaßnahmen

5.3.1. Anforderungen an die Fachkunde und Erfahrung

Der VDA der BA stellt durch geeignete Schulungen sicher, dass alle eingesetzten Rolleninhaber, so die Sicherheitsoffiziere, Systemadministratoren und leitende Rollen, die für ihre Aufgabe notwendige Fachkunde, Erfahrungen und Qualifikationen besitzen. Dies trifft sowohl auf alle BA-Angehörigen als auch auf von Vertragspartnern beauftragte und eingesetzte Mitarbeiter zu. Für alle Rollen gibt es Vertreter.

5.3.2. Anforderungen an die Zuverlässigkeit

Der VDA der BA stellt sicher, dass in den Vertrauensdiensten eingesetztes Personal die für einen sicheren Betrieb notwendige Zuverlässigkeit besitzt. Alle Rolleninhaber mit Ausnahme der Archivare müssen sich vor Übernahme einer Rolle gemäß §9 Abs. 1 Ziffer 3 Sicherheitsüberprüfungsgesetz (SÜG) einer erweiterten Sicherheitsüberprüfung im Bereich Sabotageschutz unterziehen. Die Sicherheitsüberprüfung ohne Beanstandung ist auch Voraussetzung für den Einsatz von beauftragten Mitarbeitern externer Vertragspartner. Die Archivare benötigen vor der Übernahme einer Rolle ein aktuelles Führungszeugnis nach § 30 Abs. 1 und 5 des Bundeszentralregistergesetzes.

5.3.3. Anforderungen an die Schulung

Die für die Vertrauensdienste eingesetzten Rolleninhaber werden vor Aufnahme der Tätigkeit ausreichend zu IT-Sicherheit und Fachkunde über rollenspezifische Schulungsmodule geschult und Sicherheitsbelehrungen durchgeführt. Diese Schulungen werden dokumentiert.

5.3.4. Wiederholungen der Schulungen

Der VDA der BA ordnet Wiederholungsschulungen für das in den Vertrauensdiensten eingesetzte Personal bei Bedarf dann an, wenn der Eindruck entsteht, dass die Fachkunde eines Rolleninhabers für seine Aufgabe nicht mehr ausreichend ist. Dies kann z. B. im Rahmen eines Audits festgestellt werden. Die Schulungsinhalte werden regelmäßig auf ihre Aktualität überprüft. Hinsichtlich IT-Sicherheit erfolgen jährlich dokumentierte Belehrungs- und Sensibilisierungsmaßnahmen.

5.3.5. Häufigkeit und Abfolge von Rollenwechsel

Ein regelmäßiger Rollenwechsel findet nicht statt. Siehe dazu auch Abschnitt 5.2.4.

5.3.6. Sanktionen bei unzulässigen Handlungen

Sollte ein Rolleninhaber die Anweisungen und Vorschriften verletzen oder sollten auffallend häufig Fehler auftreten, werden Maßnahmen zur zukünftigen Verhinderung ergriffen. Dies beinhalten gegebenenfalls auch den Entzug, die Suspendierung oder die Änderung seiner Rollen, Aufgaben und Zugriffsrechte. In schweren Fällen kann dies auch arbeits- und strafrechtliche Maßnahmen beinhalten.

5.3.7. Vertragsbedingungen mit dem Personal beauftragter Dritter

Für Beschäftigte beauftragter Dritter, sofern sie eine Rolle im Vertrauensdienst einnehmen, gelten dieselben Anforderungen an Zuverlässigkeit und Fachkunde wie für internes Personal.

5.3.8. An das Personal ausgehändigte Dokumente

Dem Personal des VDA der BA werden die folgenden Dokumente zur Verfügung gestellt, sofern sie zur Durchführung der Tätigkeiten oder zur Einhaltung von Anweisungen oder gesetzlichen Vorschriften notwendig sind:

- Informationen zu den relevanten Gesetzen und Verordnungen, insbesondere zur elektronischen Signatur und zum Datenschutz
- Interne Betriebskonzepte und Handlungsanweisungen der Vertrauensdienste
- Betriebshandbücher der Systeme und Software
- Relevante technische Normen
- Rollenspezifische Schulungsunterlagen.

5.4. Protokollierung sicherheitskritischer Ereignisse

5.4.1. Protokollierte Ereignisse

Sicherheitsrelevante Ereignisse werden von den IT-Systemen elektronisch protokolliert:

- Ereignisse im Lebenszyklus der Hardware Sicherheitsmodule der Vertrauensdienste (z. B. Initialisierung und Konfiguration eines HSM, Schlüsselgenerierung, Schlüsselbackup und -wiederherstellung, Löschen von Schlüsseln, Änderungen der Policy),
- Sicherheitsrelevante Systemereignisse und Fehlermeldungen der kritischen Systeme, Firewall und Router,
- Bei Systemen, die auf die gesetzliche Zeit angewiesen sind, alle zeitbezogenen Ereignisse wie die Synchronisierung der Uhren oder Fehler beim Bezug der aktuellen Zeit,
- Zutritte zu den Räumlichkeiten,
- Sicherheitskritische Ereignisse der Zutrittskontrollanlagen,
- Zuweisung und Entzug von Rollen,
- Ausgestellte qualifizierte Zeitstempel,
- Start und Stopp von Systemen, Hardwarefehler, Abstürze.

Zu jedem Ereignis werden dabei die folgenden Daten erfasst:

- Zeitpunkt (Datum und Uhrzeit),
- Art des Ereignisses,
- Ursprung des Ereignisses (z. B. System, Ort, Benutzer).

Neben der elektronischen erfolgt auch eine nicht-technische Protokollierung. Dabei werden Protokolle der sicherheitsrelevanten internen Prozeduren und Prozesse angefertigt.

5.4.2. Auswertung von Protokolldaten

Alle Protokolldaten werden regelmäßig und zusätzlich bei Verdacht auf Unregelmäßigkeiten umgehend überprüft.

Die Monitoringsysteme bereiten die gesammelten Protokolldaten durch Konsolidierung und Korrelationen auf, zeigen die Ergebnisse den verantwortlichen Rolleninhabern an und führen gegebenenfalls eine Alarmierung durch.

5.4.3. Aufbewahrungsfristen für Protokolldaten

Die Protokolldaten werden vom VDA der BA maximal ein Jahr aufbewahrt.

5.4.4. Schutz der Protokolldaten

Alle Protokolldaten werden durch die Zugriffskontrollmechanismen der speichernden Systeme vor unbefugtem Zugriff und vor Manipulation geschützt.

5.4.5. Sicherungsverfahren für Protokolldaten

Alle elektronischen Protokolldaten werden im Rahmen der Sicherung der Produktivsysteme der Vertrauensdienste regelmäßig gesichert.

5.4.6. Internes/externes Protokollierungssystem

Die Protokollierung erfolgt durch interne Systeme des VDA der BA.

5.4.7. Benachrichtigung des Auslösers eines Ereignisses

Eine Benachrichtigung erfolgt ggf. im Rahmen der Untersuchung außergewöhnlicher Ereignisse.

5.4.8. Schwachstellenbewertung

Evtl. Schwachstellen werden durch permanente Überwachung und durch Sicherheits-Audits durch die Beauftragten für IT-Sicherheit und regelmäßig im Rahmen von Schwachstellentests durch externe Auditoren bewertet.

5.5. Archivierung von Protokolldaten

Die Archivierung relevanter Daten erfolgt in Übereinstimmung mit Artikel 24 Absatz 2 Buchstabe h) der [eIDAS] sowie §16 Abs. 4 [VDG]. Archivierte Daten werden vor unbefugter Einsichtnahme, Manipulation und Vernichtung geschützt.

5.5.1. Arten von zu archivierenden Daten

Siehe Abschnitt 5.4.1.

5.5.2. Archivierungsfristen

Ausgestellte Zeitstempel werden für die gesamte Zeit des Betriebes des VDA der BA archiviert.

5.5.3. Schutzvorkehrungen für das Archiv

Elektronische Daten werden durch die Speicherung in den Produktivsystemen und ihren Backups archiviert. Für die archivierten elektronischen Daten sind daher die entsprechenden Schutzmaßnahmen (siehe Abschnitte 5.1, 5.2.2 und 0) wirksam.

5.5.4. Sicherungsverfahren für das Archiv

Archivierte elektronische Daten werden im Rahmen der Datensicherung der Systeme gesichert.

5.5.5. Anforderungen an den Zeitstempel[6] der archivierten Daten

Archivierte elektronische Daten werden mit einer Zeitangabe versehen.

Die Zeitangabe zu archivierten elektronischen Daten entspricht der Systemzeit zur Erstellung der Daten, vgl. Abschnitt 6.8.

5.5.6. Internes oder externes Archivierungssystem

Die Archivierung erfolgt durch interne Systeme und im zentralen Archiv des Vertrauensdienstes.

[6] Diese Zeitstempel sind *nicht* Gegenstand dieses TSAPS.

5.5.7. Verfahren zur Beschaffung und Verifizierung von Archivdaten

Im Sicherheitskonzept des VDA der BA sind die Vorgaben für die Beschaffung von Archivdaten festgelegt.

5.6. Schlüsselwechsel der Zertifizierungsinstanzen

Nicht relevant.

5.7. Kompromittierung und Wiederherstellung (Disaster Recovery)

5.7.1. Prozeduren bei Sicherheitsvorfällen

Es existiert ein Notfallkonzept, in dem die Prozesse, Prozeduren und Verantwortlichkeiten bei Notfällen geregelt sind. Zielsetzung dieser Notfallprozeduren ist die Minimierung von Ausfällen der Vertrauensdienste bei gleichzeitiger Aufrechterhaltung der Sicherheit. Die Ursachen des Vorfalls werden nach Wiederherstellung des Regelbetriebes analysiert und beseitigt.

5.7.2. Wiederherstellung nach Kompromittierung von Ressourcen

Nach einer vermuteten oder tatsächlichen Kompromittierung von Ressourcen, Software oder Daten finden die Notfallprozeduren Anwendung (siehe Abschnitt 5.7.1).

5.7.3. Wiederherstellung nach Schlüsselkompromittierung

Im Falle der Kompromittierung oder vermuteten Kompromittierung von privaten Schlüsseln der Vertrauensdienste wird das jeweilige Zertifikat sofort gesperrt (ausgenommen natürlich ein Wurzelzertifikat).

Sofern der Verdacht besteht, dass die für die Erzeugung und Anwendung des privaten Schlüssels eingesetzten Algorithmen, Parameter oder Geräte unsicher sind, wird eine entsprechende Untersuchung durchgeführt.

Der VDA der BA stellt Informationen für betroffene Antragsteller nach 1.3.3 und Vertrauende Dritte nach 1.3.4 bereit. Die Meldepflichten des VDA der BA gemäß [eIDAS] bleiben davon unberührt.

5.7.4. Aufrechterhaltung des Betriebs im Notfall

Im Notfall wird durch die Infrastruktur am zweiten Standort (siehe Abschnitt 5.1.1) ein Notbetrieb sichergestellt. Die Maßnahmen zur Wiederherstellung des Normalbetriebes sind in einem Notfallkonzept geregelt.

Das Notfallkonzept wird stets aktuell gehalten und durch regelmäßige Notfallübungen überprüft.

5.8. Einstellung der Tätigkeit

Der VDA der BA verfügt über einen fortlaufend aktualisierten Beendigungsplan. Im Falle der endgültigen Einstellung einzelner oder aller Zeitstempeldienste werden im Rahmen eines Beendigungsplanes u. a. folgende Maßnahmen ergriffen:

- Die Antragsteller nach Abschnitt 1.3.3 und Vertrauende Dritte nach Abschnitt 1.3.4 werden von der Einstellung der Zeitstempeldienste, soweit möglich, mindestens zwei Monate im Voraus informiert.
- Die Aufsichtsstelle nach [eIDAS] wird informiert.
- Alle noch gültigen Dienstezertifikate der Zeitstempeldienste werden gesperrt.
- Alle nicht mehr benötigten privaten Schlüssel der Vertrauensdienste werden vernichtet (siehe Abschnitt 6.2.10).

6 Technische Sicherheitsmaßnahmen

6.1. Erzeugung und Installation von Schlüsselpaaren

6.1.1. Erzeugung von Schlüsselpaaren

Das Signaturschlüsselpaar für die Erstellung und Prüfung einer qualifizierten elektronischen Signatur wird innerhalb der sicheren Umgebung des VDA der BA von der jeweiligen QSCD generiert.

Schlüsselpaare für die qualifizierten Dienste des VDA der BA werden innerhalb der sicheren Umgebung des VDA der BA von der jeweiligen QSCD generiert.

6.1.2. Übergabe privater Schlüssel an den Zertifikatsinhaber

Private Schlüssel der qualifizierten Dienste des VDA der BA werden nicht übergeben, sondern verbleiben innerhalb der sicheren Umgebung des VDA der BA, vgl. 6.2.2.

6.1.3. Übergabe öffentlicher Schlüssel an den VDA der BA

Wird vom VDA der BA nicht unterstützt.

6.1.4. Übergabe öffentlicher Schlüssel an Dritte (Relying Parties)

Öffentliche Schlüssel werden als Teil des zugehörigen Zertifikates veröffentlicht, vgl. Abschnitt 2.

6.1.5. Schlüssellängen

Durch den VDA der BA neu ausgestellte Zertifikate nutzen RSA mit mindestens 3072 Bit Moduluslänge.

6.1.6. Erzeugung und Prüfung der Schlüsselparameter

Die Eignung der kryptographischen Algorithmen und Parameter werden vom Management ständig überwacht. Wenn notwendig, werden die Schlüssellängen rechtzeitig angepasst, um die Sicherheit der Vertrauensdienste, der Zertifikate und der dafür zulässigen Anwendungen (siehe Abschnitt 1.4.1) zu gewährleisten.

Basis für geeignete Algorithmen und Parameter der qualifizierten Zertifikate und Schlüssel sind die Empfehlungen der Aufsichtsstelle nach [eIDAS].

6.1.7. Verwendungszweck der Schlüssel

Die genaue Bezeichnung des Verwendungszweckes des Schlüssels ist schlüsselabhängig und wird in der Zertifikatserweiterung KeyUsage bzw. ExtendedKeyUsage vermerkt (siehe Abschnitt 7.1.2). Es gilt:

- Die privaten Schlüssel des Zeitstempeldienstes werden ausschließlich im Zuge der Erstellung von Zeitstempeln verwendet.

6.2. Schutz der privaten Schlüssel und der kryptographischen Module

6.2.1. Standards für Schutzmechanismen und Bewertung der kryptographischen Module

Bei den Signaturkarten handelt es sich um eine qualifizierte elektronische Signaturerstellungseinheiten (QSCD) im Sinne der [eIDAS]. In der Standard-Hierarchie werden für die qualifizierten Dienste (qualifizierte Signatur-CA, TSP-R, OCSP-R) qualifizierte elektronische Siegelerstellungseinheiten im Sinne der [eIDAS] in Form von Hardware-Sicherheitsmodulen (HSM) verwendet.

6.2.2. Aufteilung der Kontrolle privater Schlüssel auf mehrere Personen

Die privaten Schlüssel der qualifizierten Vertrauensdienste stehen unter Kontrolle der Sicherheitsoffiziere des VDA der BA.

6.2.3. Treuhänderische Hinterlegung privater Schlüssel

Eine Hinterlegung der privaten Schlüssel der Zeitstempeldienste findet nicht statt.

6.2.4. Sicherung und Wiederherstellung privater Schlüssel

Sicherung und Wiederherstellung der privaten Schlüssel in Signaturkarten finden nicht statt.

Private Schlüssel der qualifizierten Dienste, wenn diese in einem HSM gespeichert sind, werden gesichert.

6.2.5. Archivierung privater Schlüssel

Eine Archivierung der privaten Schlüssel der Zeitstempeldienste wird nicht durchgeführt.

6.2.6. Transfer privater Schlüssel

Ein Transfer der privaten Schlüssel der Zeitstempeldienste wird nicht durchgeführt. Diese privaten Schlüssel werden durch die Smartcard innerhalb der sicheren Umgebung des VDA der BA erzeugt und nur dort genutzt.

6.2.7. Speicherung privater Schlüssel

Die privaten Schlüssel sind innerhalb der qualifizierten elektronischen Signaturerstellungseinheit so gespeichert, dass sie nicht ausgelesen werden können.

6.2.8. Methoden zur Aktivierung privater Schlüssel

Die Anwendung eines privaten Schlüssels einer Smartcard erfordert die Eingabe einer durch den Zertifikatsinhaber selber vergebenen PIN.

Die Aktivierung privater Schlüssel der qualifizierten Dienste erfolgt ausschließlich unter Mitwirkung mehrerer berechtigter Mitarbeiter, ausschließlich im Rahmen festgelegter Prozeduren und in der vorgesehenen sicheren Umgebung.

6.2.9. Methoden zur Deaktivierung privater Schlüssel

Private Schlüssel in HSM sind deaktiviert, solange keine Aktivierung über den Sicherheitsmechanismus des HSM erfolgt ist. Diese erfolgt ausschließlich unter Mitwirkung von mindestens zwei berechtigten Mitarbeitern.

6.2.10. Methoden zur Vernichtung privater Schlüssel

Private Schlüssel der qualifizierten Dienste werden entweder durch einen sicheren Löschmechanismus des Hardware-Sicherheitsmoduls oder durch physikalische Zerstörung der Dienstekarte vernichtet.

6.2.11. Bewertung kryptographischer Module

Siehe Abschnitt 6.2.1.

6.3. Weitere Aspekte des Schlüsselmanagements

6.3.1. Archivierung öffentlicher Schlüssel

Öffentliche Schlüssel werden mit den qualifizierten Zertifikaten vom VDA der BA entsprechend §16 Abs. 4 [VDG] für die gesamte Zeit seines Betriebs aufbewahrt.

6.3.2. Verwendungsdauern von Zertifikaten und Schlüsselpaaren

Die Dienstezertifikate des VDA der BA waren in der Legacy-Hierarchie fünf Jahre gültig. In der Standard-Hierarchie gelten Zertifikate der Signatur-CA für acht Jahre, Zertifikate der OCSP- und TSP-Responder sieben Jahre.

Private Schlüssel der qualifizierten Dienste werden nach Ablauf ihres Zertifikates nicht mehr verwendet (siehe Abschnitt 6.2.10).

Die Eignung der kryptographischen Algorithmen und Parameter werden vom Management ständig überwacht. Wenn sich herausstellt, dass ein Algorithmus oder die entsprechende Schlüssellänge über die Gültigkeitsdauer des Zertifikates hinweg keine ausreichende Sicherheit mehr bieten, wird rechtzeitig der Wechsel der betroffenen Schlüsselpaare veranlasst.

6.4. Aktivierungsdaten

Die Nutzung des privaten Schlüssels ist durch die zugehörige PIN geschützt.

6.4.1. Erzeugung und Installation von Aktivierungsdaten

Im Trustcenter wird die PIN einer Smartcard, die zur Aktivierung des eingesetzten HSM genutzt wird, im Rahmen des Initialisierungsprozesses durch den Inhaber der Smartcard vergeben.

6.4.2. Schutzmaßnahmen für Aktivierungsdaten

Die PINs zum Aktivieren der privaten Schlüssel der qualifizierten Dienste werden durch die folgenden organisatorischen Maßnahmen geschützt:

- Die Mitarbeiter sind verpflichtet, PINs vertraulich zu behandeln.
- Falls einem Mitarbeiter seine Rolle entzogen wird, wird ihm auch der Zugriff auf die ihm zugeordneten Smartcards entzogen.

6.4.3. Weitere Aspekte zu Aktivierungsdaten

Bei Smartcards ist der Wert für die maximale Anzahl der Fehlbedienungen sowie die Länge von PIN und PUK fest vorgegeben.

6.5. Sicherheitsbestimmungen für Computer

6.5.1. Spezifische Sicherheitsanforderungen für Computer

Auf den für die Erbringung der qualifizierten Dienste notwendigen Systemen, sowie auf den Systemen, die dem Schutz der Einrichtungen der qualifizierten Dienste dienen, sind alle notwendigen und anwendbaren Sicherheitsmaßnahmen der IT-Grundschutzkataloge umgesetzt. Zusätzlich werden die folgenden Maßnahmen zur Computersicherheit umgesetzt:

- Die zentralen IT-Systeme sind in verschlossenen Technikschränken untergebracht, die nur im 4-Augen-Prinzip geöffnet werden können.
- Die Vergabe und Kontrolle von Zugriffs- und Zutrittsrechten erfolgt rollenbasiert.
- Die sicherheitskritischen Systeme sind mit Siegeln versehen.
- Die Administration der zentralen Systeme wird protokolliert.
- Die Sicherheit der zentralen Systeme und die dafür eingesetzten Maßnahmen werden durch ein Monitoringsystem automatisch überwacht (siehe Abschnitt 5.4).
- Die Sicherheit der Systeme und die dafür eingesetzten Maßnahmen sind Gegenstand der regelmäßigen Audits (siehe Kapitel 8).
- In dem Rechenzentrum (RZ) befinden sich nur Systeme, welche durch den VDA der BA betrieben werden.
- Nicht benötigte Dienste sind deaktiviert

6.5.2. Bewertung der Computersicherheit

Für die QSCD wurde eine formale Evaluierung der Systemsicherheit nach den Common Criteria for Information Technology Security Evaluation (CC) durchgeführt.

Darüber hinaus wurde im Sicherheitskonzept des VDA der BA eine Bedrohungs- und Risikoanalyse durchgeführt, die die Wirksamkeit aller getroffenen Maßnahmen untersucht.

6.6. Technische Kontrollen des Software-Lebenszyklus

6.6.1. Systementwicklungsmaßnahmen

Änderungen an Software oder Konfiguration werden in einem Versionskontrollsystem mit persönlichem Login nachgehalten. Programmpakete werden vom Releasemanagement kryptographisch signiert. Änderungen an Software oder Konfiguration werden zunächst in einer Testumgebung und im Erfolgsfall anschließend in einer Referenzumgebung der Produktion erprobt. Softwareänderungen in der Produktion sind nur unter Verwendung des PIN-gesicherten Installationsmediums und nach Freigabe durch die TC-Leitung möglich.

6.6.2. Sicherheitsmanagement

Im Sicherheitskonzept des VDA der BA sind die Verantwortlichkeiten und Prozesse des Sicherheitsmanagements definiert.

6.6.3. Bewertung der Maßnahmen zur Kontrolle des Lebenszyklus

Im Sicherheitskonzept des VDA der BA wurde eine Bedrohungs- und Risikoanalyse durchgeführt, welche die Wirksamkeit aller getroffenen Maßnahmen untersucht.

6.7. Maßnahmen zur Netzwerksicherheit

In den für die Erbringung der Vertrauensdienste notwendigen Netzwerken sind alle erforderlichen Sicherheitsmaßnahmen implementiert. Dazu zählen:

- Die Aufteilung in verschiedene Netzwerksegmente und die Beschränkung und Überwachung der Kommunikation durch Firewalls.
- Sämtliche Kommunikationsverbindungen zwischen Systemen unterschiedlicher Netzwerksegmente sind durch kryptographische Mechanismen gesichert.
- Die Sicherheit der Netzwerke und die dafür eingesetzten Maßnahmen sind Gegenstand der regelmäßigen Audits (siehe Kapitel 8).

6.8. Zeitstempel[7]

Die von den Systemen der Vertrauensdienste protokollierten Daten (siehe Abschnitt 5.4.1) werden mit Zeitangaben versehen. Die Systemzeiten sind synchronisiert. Eine kryptographische Sicherung der Zeitangaben in den Protokolldaten findet nicht statt.

[7] Diese Zeitstempel sind *nicht* Gegenstand dieses TSAPS.

7 Profile

7.1. Zertifikatsprofile

7.1.1. Versionsnummer(n)

Die qualifizierten Zertifikate und Dienstezertifikate des Zeitstempeldienstes entsprechen dem Standard [X509] Version 3 bzw. seiner Profilierung in [RFC5280]. Sie erfüllen zudem die Anforderungen von [eIDAS]. Qualifizierte Zertifikate genügen zudem dem SigG-Profile von Common PKI.

7.1.2. Zertifikatserweiterungen

Zertifikate des Zeitstempeldienstes aus der Standard- oder Legacy-Hierarchie, vgl. Abschnitt 1.1, enthalten folgende nicht-kritische Erweiterungen:

- AuthorityKeyIdentifier (nicht im Zertifikat der qualifizierte Wurzel-CA)
- SubjectKeyIdentifier
- CertificatePolicies
- AuthorityInfoAccess (nicht in selbstsignierten CA-Zertifikaten)
- QCStatement: Abweichend von [ETSI-POLQ], clause 6.6.1 a) werden in qualifizierten Zertifikaten für elektronische Signaturen nur esi4-qcStatement-1 und esi4-qcStatement-4 aus [ETSI-QCST] eingetragen. Ein PKI Disclosure Statement ist nach [eIDAS] nicht notwendig und wird nicht eingetragen. Handelt es sich bei einem Dienstezertifikat um ein Zertifikat für elektronische Siegel, wird nur esi4-qcStatement-6 mit dem QC type identifier id-etsi-qct-eseal eingetragen. Diese Siegelzertifikate sind *nicht* qualifiziert

und folgende kritische Erweiterungen:

- KeyUsage
  - selbstsignierte CA-Zertifikate: `keyCertSign, CRLSign.`
  - Signatur- und Massensignaturzertifikate: `nonRepudiation`
- BasicConstraints
- ExtendedKeyUsage (nur TSP).

7.1.3. Algorithmenbezeichner (OID)

Die verwendeten Algorithmenbezeichner entsprechen den gängigen Standards.

7.1.4. Namensformen

Es gelten die Regelungen des Standard [X509] bzw. seiner Profilierung in [RFC5280] bzw. für qualifizierte Zertifikate dessen Profilierung in [COMPKI].

Für das Feld `Issuer` gelten zusätzlich folgende Festlegungen:

- Attribut `CountryName`: <DE>
- Attribut `Organization`: <Bundesagentur fuer Arbeit>
- Attribut `CommonName` (CN): Der Common Name der CA-Zertifikate ist nach dem folgenden Schema aufgebaut: <Präfix>-<Bezeichner>-CA-<lfd Nummer>:PN
  - Dienstezertifikate der qualifizierten Dienste nutzen das Präfix BA-QC, andernfalls ist das Präfix BA.
  - Der Bezeichner ist ein eindeutiger Namensbestandteil, der die Nutzung der CA andeuten soll.
  - Allen CA folgt danach der Kennzeichner „CA“.

- Die laufende Nummer wird für jeden Namen beginnend mit „1“ fortlaufend ganzzahlig geführt. Abschließend erfolgt die Kennzeichnung des CN als Pseudonym gemäß [COMPKI].

Beispiel: CN=BA-QC-Wurzel-CA-1:PN; Es handelt sich um den Common Name des Dienstezertifikats eines qualifizierten Dienstes (BA-QC), genauer der Wurzel (Bezeichner)-CA (Bezeichner), mit der laufenden Nummer 1.

7.1.5. Nutzung von Erweiterungen zu Namensbeschränkungen

Erweiterungen zur Namensbeschränkung werden nicht verwendet.

7.1.6. Bezeichner für Zertifizierungsrichtlinien (OID)

Die folgende OID wird in der Erweiterung certificatePolicy für die Referenzierung der CP für qualifizierte Zertifikate verwendet:

- CP der qualifizierten Zertifikate: 1.3.6.1.4.1.21679.1.1.5

Vgl. Abschnitt 1.2.

7.1.7. Nutzung von Erweiterungen zur Richtlinienbeschränkungen (Policy-Constraints)

Erweiterungen zur Richtlinienbeschränkungen werden nicht verwendet.

7.1.8. Syntax und Semantik von Policy Qualifiern

Richtlinien-Qualifier in der Erweiterung Certificate Policies werden nicht verwendet.

7.1.9. Verarbeitung von kritischen Erweiterungen für Zertifizierungsrichtlinien (Certificate Policies)

Die Erweiterungen für Zertifizierungsrichtlinien in den Zertifikaten sind nicht kritisch.

7.2. TSP-Profile

7.2.1. Versionsnummer(n)

Der Zeitstempeldienst der BA unterstützt TSP nach [RFC5816].

7.2.2. TSP-Datenstrukturen

Der Zeitstempeldienst unterstützt bei Anfragen die in der folgenden Tabelle angegebenen Daten:

Feld	**optional gemäß [RFC3161]**	**Kommentar**
TimeStampReq		
version	-	Muss v1 sein
messageImprint	-	
reqPolicy	X	Muss, falls vorhanden, mit konfigurierter Policy BTSP, Object Identifier 0.4.0.2023.1.1, aus [ETSI-POLTS] übereinstimmen.
nonce	X	Wird direkt in die TSP-Response übernommen.

Feld	optional gemäß [RFC3161]	Kommentar
certReq	X	Darf fehlen. Wenn nicht vorhanden, wird Wert FALSE angenommen. Wenn Wert FALSE, dann ist SignedData.certificates (siehe TSP-Response) in der TSP-Response nicht vorhanden. Wenn Wert TRUE, dann enthält SignedData.certificates (siehe TSP-Response) in der TSP-Response die Zertifikatskette des Signaturschlüssels, mit dem der TSP-Response signiert wurde.
Extensions	X	Muss fehlen, es werden keine unterstützt. Enthält der Request doch welche, wird eine Fehlerantwort (rejection/unacceptedExtension) erzeugt. Dies ist unabhängig davon, ob die jew. Extension critical markiert ist oder nicht.
MessageImprint		
hashAlgorithm	-	Muss SHA256 (2.16.840.1.101.3.4.2.1) oder SHA512 (2.16.840.1.101.3.4.2.3) sein. Wenn anderer Wert, wird eine Fehlerantwort (rejection/badAlg) erzeugt.
hashedMessage	-	Länge muss zu hashAlgorithm passen. Wenn nicht passend, wird eine Fehlerantwort (rejection/badDataFormat) erzeugt.

Tabelle 4 - Zulässige Daten der TSP-Anfragen

Der Zeitstempeldienst unterstützt bei Antworten die in der folgenden Tabelle angegebenen Daten:

Feld	optional gemäß [RFC3161]	TSP-R generiert	Kommentar
TimeStampResp			
Status	-	X	
timeStampToken	X	(X)	Nur vorhanden bei status = granted
ContentInfo			
contentType	-	X	id-signedData (1.2.840.113.1.7.2)
content	-	X	s. u.
SignedData			
version	-	X	INT(1)

Feld	optional gemäß [RFC3161]	TSP-R gene-riert	Kommentar
digestAlgorithms	-	X	SHA256 (2.16.840.1.101.3.4.2.1), inkl. ASN-NULL-Parameter
encapContentInfo	-	X	s. u.
certificates	X	(X)	Nur vorhanden, wenn Wert (Request.certReq) = TRUE Enthält kompletten Zertifikatspfad des TSP-Responders.
crls	X	-	nicht benutzt
signerInfos	-	X	s. u.
EncapsulatedContentInfo			
eContentType	-	X	id-ct-TSTInfo (1.2.840.113549.1.9.16.1.4)
eContent	X	X	OCTET STRING enthält TSTInfo
SignerInfo			
version	-	X	INT(1)
sid	-	X	issuerAndSerialNumber
digestAlgorithm	-	X	SHA256 (2.16.840.1.101.3.4.2.1) inkl. ASN-NULL-Parameter
signedAttrs	X	X	erzeugt werden folgende Attribute: contentType messageImprint signingCertificate
signatureAlgorithm	-	X	RSASSA-PSS mit hashAlgorithm=SHA256, maskGenAlgorithm=SHA-256, saltLength=32
signature	-	X	
TSTInfo			
version	-	X	INT(1)
policy	-	X	BTSP, Object Identifier 0.4.0.2023.1.1, aus [ETSI-POLTS].
messageImprint	-	X	Entspricht genau dem messageImprint aus dem Request.
serialNumber	-	X	Ein eindeutiger INTEGER mit einer Maximallänge von 160 bit (20 byte).

Feld	optional gemäß [RFC3161]	TSP-R gene-riert	Kommentar
genTime	-	X	Die eigentliche Zeit des Zeitstem-pels.
accuracy	X	X	Genauigkeit mindestens 1 Sekunde, s. u.
nonce	X	(X)	Nur vorhanden, wenn im Request vorhanden gewesen. Wert wird dann aus dem Request übernommen.
Tsa	X	X	subject(signerCertificate) ist kodiert als ASN1-Type "Name", daher wird hier der tsa dazu passend kodiert als directoryName ([4]).
extensions	X	-	`esi4-qtstStatement-1` nach [ETSI-PROFTS] clause 9
Accuracy			
seconds	X	X	INT(1)

Tabelle 5 - Zulässige Daten der TSP-Antworten

7.3. OCSP-Profile

7.3.1. Versionsnummer(n)

Der OCSP-Verzeichnisdienst der BA unterstützt OCSP nach [RFC2560]. Zusätzlich werden Erweiterungen von Common PKI [COMPKI] verwendet.

7.3.2. OCSP-Erweiterungen

Der OCSP-Verzeichnisdienst unterstützt bei Anfragen die in der folgenden Tabelle angegebenen Erweiterungen:

Erweiterungen	Inhalt
Nonce	Wert, der die Antwort kryptographisch an die Anfrage bindet (optional).
AcceptableResponses	id-pkix-ocsp-basic
ServiceLocator	Wird vom OCSP-Responder nicht ausgewertet.

Tabelle 6 - Zulässige Erweiterungen der OCSP-Anfragen

In den Antworten verwendet der OCSP-Verzeichnisdienst die in der folgenden Tabelle angegebenen Erweiterungen:

Erweiterungen	Inhalt
Nonce	Gleicher Wert wie in der Anfrage. Nicht existent, falls in Anfrage nicht vorhanden.
ArchiveCutoff	Wie in [RFC2560] beschrieben. Das Aufbewahrungsin-tervall beträgt 10950 Tage.

Erweiterungen	Inhalt
CertHash	Bei Status good oder revoked wird der SHA-1 Hash-Wert des Zertifikats eingetragen.
RequestedCertificate	Enthält das Zertifikat, falls RetrieveIfAllowed bei der Anfrage gesetzt war.

Tabelle 7 - Erweiterungen der OCSP-Antworten

8 Revisionen und andere Bewertungen

Die BA führt selbst regelmäßig interne Audits durch, um die Einhaltung der Sicherheitsmaßnahmen sicherzustellen. Neben internen, selbst durchgeführten Audits werden auch externe Prüfungen gemäß [eIDAS] Artikel 20 von einer Konformitätsbewertungsstelle durchgeführt.

8.1. Häufigkeiten von Revisionen

Interne Revisionen bzw. Audits werden regelmäßig nach einem Auditplan sowie bei Bedarf nach sicherheitskritischen Vorfällen durchgeführt. Dazu gehören insbesondere monatliche Schwachstellenscans aus dem Netz der BA sowie mindestens jährliche PEN-Tests.

Mindestens alle 24 Monate werden Prüfungen gemäß [eIDAS] Artikel 20 von einer Konformitätsbewertungsstelle durchgeführt.

Die Aufsichtsstelle nach [eIDAS] kann jederzeit eine Überprüfung vornehmen oder durch eine Konformitätsbewertungsstelle vornehmen lassen.

8.2. Identität und Qualifikation des Auditors

Der Beauftragte für IT-Sicherheit ist verantwortlich für die Prüfung der IT-Sicherheit innerhalb des VDA der BA. Zu seinen Aufgaben gehören:

- Initiierung regelmäßiger Prüfungen durch den Beauftragten für IT-Sicherheit,
- Überprüfung, ob das interne Kontrollsystem wirksam ist.

Der Beauftragte für IT-Sicherheit des IT-Systemhauses ist verantwortlich für die Überprüfung der Sicherheit des Vertrauensdienstes im laufenden Betrieb. Der Beauftragte für IT-Sicherheit im IT-Systemhaus besitzt umfangreiche Kompetenz und Erfahrung im Bereich Informationssicherheit, PKI und bezüglich der relevanten Gesetzgebung (vor allem zur elektronischen Signatur und zum Datenschutz).

Der Schwachstellenscan wird durch den Bereich Cert-BA im IT-Systemhaus durchgeführt, der über eine angemessene Expertise verfügt.

Die Durchführung des PEN-Testes wird von der BA bei einem externen Dienstleister eingekauft.

Konformitätsbewertungsstellen sind gemäß [eIDAS] Artikel 3 Satz 1 Nr. 18 akkreditiert.

8.3. Beziehungen zwischen Auditor und zu untersuchender Partei

Der interne Auditor ist ein Mitarbeiter der BA. Das Rollenkonzept des VDA der BA stellt sicher, dass der Auditor in keiner Weise an der Administration oder dem Betrieb der Vertrauensdienste beteiligt ist. Außerdem ist der Auditor weder direkt noch indirekt vom VDA der BA oder seinen Mitarbeitern abhängig.

Der beauftragte PEN-Tester und die Konformitätsbewertungsstelle stehen in vertraglicher Beziehung zur BA, haben aber keine Berührungspunkte mit Aufbau oder Betrieb der Vertrauensdienste.

8.4. Umfang der Prüfungen

Das Ziel der Audits ist die Überprüfung der Umsetzung der definierten Sicherheitsmaßnahmen. Die Prüfungen werden nach Kontrollplänen durchgeführt und umfassen insbesondere die folgenden Bereiche:

- Konfiguration der sicherheitskritischen Systeme,
- Log-Daten sicherheitskritischer Systeme,
- Protokolle sicherheitskritischer Prozeduren (z. B. Prozeduren der Schlüsselerzeugung, Notfallprozeduren, Updaten der Systeme),
- Dokumentation der personellen Sicherheitsmaßnahmen (z. B. Schulungsnachweise, Dienstpläne, Rollennachweise),
- Dokumentation zu Prozeduren und Systemen (z. B. Notfallpläne, Systemhandbücher),

- Schlüssel sowie Authentisierungs-Chipkarten (z. B. für die Zugangskontrolle oder den Zugriff auf Signaturkarten und Hardware Sicherheitsmodule),
- Archivdaten,
- Einrichtungen zur baulichen und physikalischen Sicherheit (z. B. Zutrittskontrolle, Brandschutz, Klimatisierung).

Die Grundlage für die externen Prüfungen bildet das Sicherheitskonzept des VDA der BA.

8.5. Maßnahmen bei Mängeln

Festgestellte Mängel werden je nach Schwere und Dringlichkeit im Rahmen des definierten Schwachstellenmanagements betrachtet und entsprechend behandelt. Schwerwiegende Mängel werden an das Security-Management der BA gemeldet.

Die Meldepflichten und Maßnahmen der [eIDAS] bleiben davon unberührt.

8.6. Veröffentlichung der Ergebnisse

Die Ergebnisse werden in einem Audit-Bericht dokumentiert. Sie werden nicht veröffentlicht.

Das Ergebnis einer regelmäßigen ([eIDAS] Artikel 20) oder von der Aufsichtsstelle nach [eIDAS] angeordneten Prüfung wird der Aufsichtsstelle zur Verfügung gestellt.

Meldepflichten des VDA der BA gemäß [eIDAS] bleiben davon unberührt.

9 Weitere geschäftliche und rechtliche Regelungen

9.1. Gebühren

Die Dienstleistungen des Zeitstempeldienstes sind für Mitarbeiter oder Fachverfahren der Rechtskreise SGB II oder SGB III gebührenfrei.

Werden die Dienstleistungen von einem anderen als dem in Satz 1 genannten Antragsteller, vgl. Abschnitt 1.3.3, in Anspruch genommen, gelten die Regelungen der folgenden Absätze.

9.1.1. Gebühren für die Ausstellung von Zeitstempeln

Mandanten müssen für die Ausstellung von Zeitstempeln die vertraglich vereinbarten Gebühren entrichten.

9.1.2. Gebühren für den Abruf von Zertifikaten

Derzeit erhebt die BA für den Abruf von Zertifikaten über die in 2.1 genannten Verzeichnisdienste keine Gebühren.

9.1.3. Gebühren für die Abfrage von Zertifikatsstatusinformationen

Die BA erhebt für den Abruf von Zertifikatsstatusinformationen über OCSP keine Gebühren.

9.1.4. Gebühren für andere Dienstleistungen

Keine.

9.1.5. Rückerstattungen

Eine Rückerstattung rechtmäßig erhobener Gebühren erfolgt nicht. Eine Rückerstattung ist nur bei vertraglicher Vereinbarung möglich.

9.2. Finanzielle Verantwortung

9.2.1. Deckungsvorsorge

Der VDA der BA verfügt über die erforderliche Deckungsvorsorge in Form einer Versicherung gemäß §2 [VDV].

9.2.2. Weitere Vermögenswerte

Keine weiteren Vermögenswerte.

9.2.3. Erweiterte Versicherung oder Garantie

Aufgrund der Zuschusspflicht des Bundes aus § 365 SGB III kann eine Insolvenz des VDA der BA nicht eintreten.

9.3. Vertraulichkeit betrieblicher Informationen

9.3.1. Art der geheimzuhaltenden Information

Als vertraulich gelten alle betrieblichen Informationen, die nicht von der BA über die Verzeichnisdienste oder über ihre Web-Seiten veröffentlicht werden.

9.3.2. Öffentliche Informationen

Als öffentlich gelten alle Informationen in den ausgestellten und veröffentlichten Zertifikaten sowie alle veröffentlichten TSAPS Versionen.

9.3.3. Verantwortlichkeit für den Schutz von geheimzuhaltenden Information

Der Vertrauensdienst der BA sichert die in Abschnitt 9.3.1 genannten vertraulichen Informationen vor Manipulation und unbefugter Kenntnisnahme durch Dritte.

9.4. Schutz personenbezogener Daten

9.4.1. Geheimhaltung

Der Vertrauensdienst der BA beachtet die gesetzlichen Anforderungen zur Geheimhaltung von vertraulichen Daten, insbesondere die des Bundesdatenschutzgesetzes sowie weitere Datenschutzvorschriften, u.a. der EU-Datenschutz Grundverordnung. Die BA trägt die Verantwortung für Maßnahmen zum Schutz vertraulicher Informationen. Daten dürfen im Rahmen der Diensterbringung an Dritte nur im Rahmen vertraglicher Regelungen weitergegeben werden, wenn vom Dritten zuvor eine Vertraulichkeitserklärung unterzeichnet wurde, in der dieser die mit der Aufgabe betrauten Mitarbeiter zur Einhaltung der gesetzlichen Bestimmungen über den Datenschutz verpflichtet hat.

9.4.2. Vertraulich zu behandelnde Daten

Als vertraulich gelten alle personenbezogenen Daten, die nicht Bestandteil eines Zertifikats oder einer Sperrliste sind.

9.4.3. Nicht vertraulich zu behandelnde Daten

Alle im Zertifikat enthaltenen Informationen gelten als nicht vertraulich.

9.4.4. Verantwortlichkeit für den Schutz privater Informationen

Der VDA der BA wird Daten des Zertifikatsinhabers, soweit sie in personenbezogener Form vorliegen, unter Einhaltung der einschlägigen Bestimmungen der Datenschutzvorschriften behandeln (siehe auch 9.4.1).

9.4.5. Einverständniserklärung zur Nutzung privater Informationen

Soweit erforderlich, erteilt der Antragsteller sein Einverständnis, dass seine personenbezogenen Daten zum Zweck der Diensterbringung auf Basis der geltenden Gesetze verarbeitet werden dürfen.

9.4.6. Weitergabe von Informationen an Ermittlungsinstanzen oder Behörden

Es gelten die Vorschriften des §8 [VDG], insbesondere die Absätze

(2) Der Vertrauensdiensteanbieter darf personenbezogene Daten einer Person, die Vertrauensdienste nutzt, den zuständigen Stellen übermitteln,

1. soweit die zuständigen Stellen die Übermittlung nach Maßgabe der hierfür geltenden Bestimmungen verlangen, da die Übermittlung erforderlich ist,

a) für die Verfolgung von Straftaten oder Ordnungswidrigkeiten,

b) zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung oder

c) für die Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes, des Militärischen Abschirmdienstes oder der Finanzbehörden, oder

2. soweit Gerichte die Übermittlung im Rahmen anhängiger Verfahren nach Maßgabe der hierfür geltenden Bestimmungen anordnen.

Die Berechtigung zur Datenübermittlung nach Satz 1 Nummer 1 gilt nicht, soweit sie durch andere Gesetze ausdrücklich ausgeschlossen ist.

(3) Die Vertrauensdiensteanbieter haben die Übermittlung zu dokumentieren. Die Dokumentation ist zwölf Monate aufzubewahren.

(5) Die allgemeinen Datenschutzanforderungen bleiben unberührt.

9.4.7. Sonstige Offenlegungsgründe

Keine weiteren Offenlegungsgründe.

9.5. Geistiges Eigentum und dessen Rechte

Bestand und Inhalt von Urheber- und sonstigen Immaterialgüterrechten richten sich nach den allgemeinen gesetzlichen Vorschriften.

9.6. Gewährleistung, Sorgfalts- und Mitwirkungspflichten

9.6.1. Verpflichtung des Zeitstempelgebers

Der VDA der BA sichert zu, dass die von ihm erzeugten Zeitstempel alle Anforderungen des vorliegenden TSAPS erfüllen.

9.6.2. Verpflichtung der Registrierungsstelle

Nicht relevant.

9.6.3. Verpflichtung des Beziehers

Der Bezieher hat insbesondere folgende Pflichten:

- Die Zeitstempel sind nur bestimmungsgemäß und nicht missbräuchlich zu benutzen.
- Er hat sich über Aktualisierung des TSAPS zu informieren, siehe Abschnitt 9.12.2.

9.6.4. Verpflichtung vertrauender Dritte

Vertrauende Dritte sind dazu verpflichtet, gemäß den in Abschnitt 4.5.2 und Abschnitt 4.9.6 beschriebenen Regeln vorzugehen.

9.6.5. Verpflichtung weiterer Teilnehmer

Keine Verpflichtungen für andere Teilnehmer.

9.7. Haftungsausschluss

Der VDA der BA übernimmt trotz Umsetzung aller erforderlichen Sicherheitsmaßnahmen keine Gewähr dafür, dass die Datenverarbeitungssysteme ohne Unterbrechung betriebsbereit sind und fehlerfrei arbeiten.

Datenverluste in Folge technischer Störungen und die Kenntnisnahme vertraulicher Daten durch unberechtigte Eingriffe sind auch bei Beachtung der erforderlichen Sorgfalt nie völlig auszuschließen.

9.8. Haftungsbegrenzungen

Die Haftung des VDAs der BA richtet sich nach den jeweiligen gesetzlichen Bestimmungen, insbesondere § 10 Vertrauensdienstegesetz [VDG] und §2 Vertrauensdiensteverordnung [VDV], sowie den allgemeinen Schadensersatzregelungen des Bürgerlichen Gesetzbuches.

9.9. Schadensersatz

Siehe 9.8

9.10. Gültigkeit des TSAPS

9.10.1. Gültigkeitszeitraum

Das vorliegende TSAPS ist ab dem 08.11.2023 gültig. Die Gültigkeit endet spätestens mit der Einstellung der Tätigkeit des VDA der BA (siehe Abschnitt 5.8).

9.10.2. Vorzeitiger Ablauf der Gültigkeit

Die Gültigkeit dieses TSAPS endet vorzeitig mit der Veröffentlichung einer neuen Version.

9.10.3. Konsequenzen des Ablaufs dieses Dokumentes

Die Teilnehmer sind bis zum Ende der Nutzung (End of subscription) siehe 4.11, oder der Einstellung der Tätigkeit, siehe 5.8, an die Bestimmungen der dann gültigen Version des TSAPS gebunden.

9.11. Individuelle Mitteilungen und Absprachen mit den Teilnehmern

Für individuelle Mitteilungen und Absprachen mit den Teilnehmern werden die jeweils gültigen Kontaktinformationen und Kommunikationswege (E-Mail, Telefon, Post, etc.) genutzt.

9.12. Änderungen der Richtlinie

9.12.1. Verfahren für die Änderung

Für die Pflege des TSAPS ist ein interner Prozess mit einer entsprechenden Rolle auf Managementebene definiert. Durch diesen wird sichergestellt, dass das TSAPS stets die aktuellen Praktiken der Vertrauensdienste der BA wiedergibt.

Bei einer Aktualisierung des TSAPS wird nur dann die volle Versionsnummer erhöht, wenn sicherheitsrelevante Veränderungen der beschriebenen Praktiken vorgenommen wurden. Die Entscheidung über die Erhöhung der vollen Versionsnummer ist Teil des Prozesses zur Aktualisierung des TSAPS.

9.12.2. Benachrichtigungsverfahren und Veröffentlichungsperioden

Eine Aktualisierung des TSAPS wird auf der Webseite des VDA der BA, siehe Abschnitt 2.1, bekanntgegeben.

9.12.3. Bedingungen für Änderungen der Objekt-Kennung (OID)

Die Entscheidung über die Zuweisung einer neuen OID ist Teil des Prozesses zur Aktualisierung des TSAPS. Bei Ergänzungen oder Modifikationen des TSAPS entscheidet der VDA der BA, ob sich daraus signifikante Änderungen der Sicherheit des Vertrauensdienstes, der Rechte und Pflichten der Teilnehmer oder der Anwendbarkeit der Zertifikate ergeben, die eine Änderung der OID bedingen.

9.13. Schiedsverfahren

Die Aufsichtsstelle nach [eIDAS], derzeit Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, kann zur Beilegung telekommunikationsrechtlicher Streitigkeiten einen einvernehmlichen Einigungsversuch vor einer Gütestelle (Mediationsverfahren) gemäß § 124 TKG vorschlagen.

9.14. Geltende Gesetze

Es gilt deutsches Recht.

9.15. Konformität mit anwendbarem Recht

Für Streitigkeiten aus diesem TSAPS gilt – soweit gesetzlich zulässig – als Gerichtsstand Nürnberg.

9.16. Sonstige Bestimmungen

9.16.1. Vollständigkeitsklausel

Alle im vorliegenden TSAPS enthaltenen Regelungen gelten zwischen dem VDA der BA und den Teilnehmern. Mündliche Vereinbarungen bzw. Nebenabreden bestehen nicht.

9.16.2. Abtretung der Rechte

Entfällt.

9.16.3. Salvatorische Klausel

Sollten einzelne Bestimmungen dieses TSAPS unwirksam sein oder Lücken enthalten, wird dadurch die Wirksamkeit der übrigen Bestimmungen nicht berührt.

Anstelle der unwirksamen Bestimmung gilt die wirksame Bestimmung als vereinbart, welche der ursprünglich gewollten am nächsten kommt.

9.16.4. Vollstreckung (Anwaltskosten und Rechtsverzicht)

Entfällt.

9.16.5. Höhere Gewalt (Force Majeure)

Entfällt.

9.17. Andere Regelungen

9.17.1. Organisatorisch

Keine.

9.17.2. Testmöglichkeiten

Der VDA der BA stellt Antragstellern im Sinne von Abschnitt 1.3.3 Zugriff auf einen Test TSP-R zur Verfügung.

Die Dienstezertifikate der Testsysteme sind am Namensschema des Common Name (CN) erkennbar:

EDST-Test-BA-QC-<Bezeichner>-<lfd Nummer>:PN

<Bezeichner> ist ein eindeutiger Namensbestandteil, der die Nutzung des Dienstezertifikates andeuten soll. Die laufende Nummer wird für jeden Namen beginnend mit „1“ fortlaufend ganzzahlig geführt. Abschließend erfolgt die Kennzeichnung des CN als Pseudonym gemäß Common PKI [COMPKI].

Das Präfix „EDST-Test-BA-QC“ wird verwendet, um durch den Namen den nicht qualifizierten Charakter des entsprechenden Dienstes hervorzuheben.

Beispiele:

CN=EDST-Test-BA-QC-Signatur-CA-5:PN

CN=EDST-Test-BA-QC-TSP-51:PN

CN=EDST-Test-BA-QC-OCSP-44:PN

9.17.3. Menschen mit Behinderung

Der VDA der BA beachtet die gesetzlichen Anforderungen zur Barrierefreiheit, insbesondere das Behindertengleichstellungsgesetz und die barrierefreie Informationstechnikverordnung.

Abbildungsverzeichnis

Tabellenverzeichnis

Referenzen

Bezeichner	Dokument
[RFC5280]	RFC 5280: Internet X.509 Public Key Infrastructure - Certificate and CRL Profile
[eIDAS]	VERORDNUNG (EU) Nr. 910/2014 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG
[ETSI-TSP]	ETSI TS 101 861: Time stamping profile, European Telecommunications Standards Institute, Version 1.2.1, März 2003
[ETSI-POLQ]	ETSI EN 319 411-2: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates. Version 2.1.1, Februar 2016
[ETSI-QCST]	ETSI EN 319 412-5: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements V2.1.1, Februar 2016
[ETSI-POLTS]	ETSI EN 319 421: Electronic Signatures and Infrastructures (ESI): Policy and Security Requirements for Trust Service Providers issuing Time-Stamps. V1.1.1, März 2016
[ETSI-PROFTS]	ETSI EN 319 422: Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles V1.1.1, März 2016
[QCP-n-qscd]	Certificate policy for EU qualified certificates issued to natural persons with private key related to the certified public key in a QSCD; OID 0.4.0.194112.1.2 Definiert in [ETSI-POLQ]
[RFC3647]	RFC 3647: Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework, IETF Network Working Group, November 2003
[RFC2560]	RFC 2560: X.509 Internet Public Key Infrastructure - Online Certificate Status Protocol – OCSP, IETF Network Working Group, Juni 1999
[RFC2251]	RFC 2251: Lightweight Directory Access Protocol (v3), IETF Network Working Group, Dezember 1997
[RFC3161]	RFC 3161: Internet X.509 Public Key Infrastructure - Time-Stamp Protocol (TSP), IETF Network Working Group, August 2001
[RFC5816]	RFC 5816: ESSCertIDv2 Update for RFC 3161, IETF Network Working Group, März 2010
[COMPKI]	Common PKI Specifications for Interoperable PKI Applications from T7 and Teletrust V2.0, January20th, 2009, http://www.t7ev.org/common-pki.html.
[CPS]	Certification Practice Statement der BA, Version: 3.1, Datum 01.10.2017; OID 1.3.6.1.4.1.21679.1.1.4.
[ISISMTT1]	Common ISIS-MTT Specifications for Interoperable PKI Applications - Core Parts, T7 e. V. i. G. and TeleTrusT e. V., Version 1.1, März 2004
[ISISMTTb]	Common ISIS-MTT Specifications for Interoperable PKI Applications - Optional Profile: SigG-Profile, T7 e. V. i. G. and TeleTrusT e. V., Version 1.1, März 2004

Bezeichner	Dokument
[X509]	ITU-T Recommendation X.509: Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, International Telecommunication Union, August 2005 (äquivalent zu ISO/IEC 9594-8)
[FIPS140]	FIPS PUB 140-1: Security Requirements for Cryptographic Modules, National Institute of Standards and Technology (NIST), Januar 1994
[PKCS1]	PKCS#1: RSA Cryptography Standard, RSA Laboratories, Version 2.1, Juni 2002
[SÜG]	Gesetz über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes (Sicherheitsüberprüfungsgesetz – SÜG) vom 20. April 1994 (BGBl. I S. 867), zuletzt geändert durch Art. 20 V v. 19.06.2020 I 1328
[VDG]	Vertrauensdienstegesetz vom 18. Juli 2017 (BGBl. I S. 2745), das durch Artikel 2 des Gesetzes vom 18. Juli 2017 (BGBl. I S. 2745) geändert worden ist In Kraft getreten am 29.7.2017.
[VDV]	Vertrauensdiensteverordnung vom 15. Februar 2019 BGBl. I 2019 S. 114 ausgegeben am 27. Februar 2019. In Kraft getreten am 28.2.2019.

Definitionen und Abkürzungen

Begriff	Erläuterung
Aktivierungsdaten	Vertrauliche Daten, mit denen sich ein legitimierter Nutzer eines privaten Schlüssels gegenüber dem System, das den Schlüssel speichert, (z. B. einer Chipkarte) authentisiert und somit den Schlüssel aktiviert. Üblicherweise werden PINs und Passwörter als Aktivierungsdaten verwendet.
ARL	Authority Revocation List Sperrliste für CA-Zertifikate.
ASCII	American Standard Code for Information Interchange Standard für einen Zeichensatz.
ASN.1	Abstract Syntax Notation Beschreibungssprache für Daten, wird z. B. von X.509 verwendet.
Asymmetrische Kryptoverfahren	Kryptografische Verfahren, die auf zwei verschiedenen Schlüsseln basieren, wobei einer öffentlich und einer privat (geheim) ist. Dadurch ist es möglich, dass jemand mit dem öffentlichen Schlüssel eine Nachricht verschlüsselt, die nur der Besitzer des geheimen Schlüssels wieder entschlüsseln kann. Damit ist das Problem des Austausches und des Verteilens von geheimen symmetrischen Schlüsseln beseitigt, und es sind Verfahren wie die digitale Signatur möglich.
Authentisierung, Authentifizierung	Vorgang des Nachweises der Authentizität durch kryptografische Verfahren. Durch ein festgelegtes Verfahren wird festgestellt, ob jemand wirklich derjenige ist, der er vorgibt zu sein, bzw. dass die Daten wirklich von einer bestimmten Person stammen. Authentisierung bezeichnet dabei den Nachweis, Authentifizierung die Prüfung dieses Nachweises.
Authentisierungszertifikat	Zertifikat zu einem Schlüsselpaar (z. B. auf einer digitalen Dienstkarte oder Gästekarte), mit dem eine sichere Authentisierung (z. B. für einen Smartcard-Logon oder an einem Web-Portal) durchgeführt werden kann.
BNetzA	Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen. Die BNetzA ist nach dem [VDG] die zuständige Aufsichtsbehörde.
Certification Authority (CA)	Englischer Begriff für eine Zertifizierungsinstanz.
Certificate Policy (CP)	Gesamtheit der Regeln und Vorgaben, die die Anwendbarkeit eines Zertifikatstyps festlegen.
Certification Practice Statement (CPS)	Darlegung der Praktiken, die ein Zertifizierungsdienst bei der Ausgabe der Zertifikate anwendet.
Certficate Revocation List (CRL)	Englischer Begriff für Zertifikats-Sperrliste.

Begriff	Erläuterung
Common Criteria (CC)	Internationaler Standard zur Bewertung der Informationssicherheit von Produkten und Systemen. CC unterscheidet verschiedene Evaluation Assurance Levels (EAL), die festlegen, was und wie geprüft wird. Die Prüfung erfolgt immer gegen die Sicherheitsvorgaben oder ein Schutzprofil (Protection Profile).
DCF77	Von der Physikalisch-Technische Bundesanstalt auf 77,5 kHz ausgestrahltes Funksignal, das in Deutschland die „gesetzliche Zeit“ verbreitet.
Delta-CRL	Inkrementelle Sperrliste, d. h. Sperrliste, die nur jene Sperrinformationen enthält, die sich seit der Veröffentlichung der letzten vollständigen Sperrliste geändert haben.
Dienstekarte	Bei den Dienstekarten handelt es sich um Signaturkarten, mit denen Signatur-CA, OCSP-Responder oder TSP-Responder signieren.
digitale Dienstkarte (dDk)	Als Chipkarte realisierter Ausweis für interne Mitarbeiter der BA. Die dDk enthält Schlüsselpaare zur Erzeugung von Signaturen, zur Authentisierung und zur Verschlüsselung. Die digitalen Dienstkarten sind sichere Signaturerstellungseinheiten.
digitale Signatur	Mit asymmetrischen Kryptoverfahren berechnete Daten, die mit anderen elektronischen Daten logisch verknüpft sind, und mit denen sich deren Authentizität und Integrität prüfen lassen. Die Sicherheit einer digitalen Signatur hängt dabei von den verwendeten Parametern des Kryptoverfahrens, der Geheimhaltung des privaten Schlüssels und der Zuordnung des öffentlichen Schlüssels zum Signator (z. B. durch ein Zertifikat) ab.
DistinguishedName (DN)	Namensform nach X.501. Ein DN besteht aus verschiedenen Attributen und entsprechenden Werten und soll eine Entität eindeutig kennzeichnen. Die wichtigsten Attribute in dieser CPS sind CommonName (cn), Organization (o) und Country (c).
DNS-Name	Eindeutiger Name eines Systems, über das dieses in einem Netzwerk adressiert werden kann.
Elektronische Signatur	Daten, die mit anderen elektronischen Daten logisch verknüpft sind, und mit denen sich deren Authentizität und Integrität prüfen lassen. D. h., mittels einer elektronischen Signatur kann sowohl die Unverfälschtheit einer Nachricht als auch der Unterzeichner eines elektronischen Dokumentes verifiziert werden. Die sicherste bekannte Ausprägung einer elektronischen Signatur ist die qualifizierte digitale Signatur.
Gästekarte	Als Smartcard realisierter Ausweis für externe Mitarbeiter der BA. Die Gästekarte enthält Schlüsselpaare zur Authentisierung und zur Verschlüsselung.
Hardware Sicherheitsmodul (HSM)	Gerät zur sicheren Speicherung und Anwendung kryptographischer Schlüssel. Im Unterschied zu Smartcards besitzen HSMs meist eine eigene Stromversorgung und implementieren oft aufwendige Sicherheitsmechanismen wie ein sicheres Key Backup von Schlüsseln, die Protokollierung sicherheitsrelevanter Ereignisse oder ein rollenbasiertes Zugriffskonzept.

Begriff	Erläuterung
HTTP	Hypertext Transfer Protocol Besonders im Internet verbreitetes Kommunikationsprotokoll.
Kartenausgeber (LRA-Kartenausgeber)	Rolle im VDA der BA, der u.a. die dDk oder Gästekarte an die Mitarbeiter ausgibt.
Karteninhaber	Person, für die eine dDk oder Gästekarte ausgestellt wurde.
Kartenpersonalisierung	Dienst innerhalb der VDA der BA, der die dDk oder Gästekarte personalisiert.
LDAP	Lightweight Directory Access Protocol Von der IETF standardisiertes Protokoll zum Zugriff auf Verzeichnisse.
Local Registration Authority (LRA) = Lokale Registrierungsstelle	Lokale Registrierungsstelle In den Dienststellen der BA eingerichtete lokale Registrierungsstellen. Diese sind u.a. für die Ausgabe der Mitarbeiterzertifikate zuständig.
Mandanten-Signaturkarte	Signaturkarten, die an Mitarbeiter des Mandanten ausgegeben werden. Sie enthalten ein Schlüsselpaar sowie ein zugehöriges Zertifikat (Signaturschlüsselzertifikat) für die Erzeugung bzw. Verifizierung qualifizierter elektronischer Signaturen.
Mandanten-Zertifikat	Qualifiziertes Zertifikat auf der Mandanten-Signaturkarte.
Massensignatur	Eine Massensignatur beschreibt hier eine Betriebsart von Chipkarten mit einmaliger PIN-Eingabe mehrere Signaturen durchzuführen. Eine erneute PIN-Eingabe wird erst nach Beendigung der logischen Verbindung zwischen Karte und System notwendig. Massensignaturen werden in speziell dafür vorgesehenen Anwendungen durch Massensignaturkarten durchgeführt.
Massensignaturkarte (MSK)	Chipkarte zum Durchführen von Massensignaturen in einer entsprechenden Anwendung. Die MSK hat Signatur- und Authentisierungsschlüssel, ist einer Person zugeordnet, trägt aber im Gegensatz zu einer dDk ein Pseudonym im Zertifikatsnamen.
Object Identifier (OID)	Weltweit eindeutiger, hierarchisch ausgebauter, numerischer Bezeichner.
OCSP	Online Certificate Status Protocol Von der IETF standardisiertes Protokoll zur Online-Abfrage von Statusinformationen von Zertifikaten.
OCSP-Responder	Server, der einen OCSP-Verzeichnisdienst implementiert.
OCSP-Verzeichnisdienst	Verzeichnisdienst, der Zertifikate und ihren aktuellen Sperrstatus über das OCSP-Protokoll bereitstellt.
Öffentlicher Schlüssel	Nicht-geheimer Teil eines Schlüsselpaares bei asymmetrischen Schlüsselpaaren.
OID	Object Identifier.

Begriff	Erläuterung
Personalisierung	Vorgang der Zuordnung einer Karte zu einer Person. Dies kann einerseits durch die physikalische Personalisierung (z. B. Hochprägung, Lasergravur) oder auch durch die elektrische Personalisierung (d. h. Laden der personenbezogenen Daten in den Speicher der Chipkarte) geschehen.
PIN	Personal Identification Number Geheimzahl zur Authentisierung eines Individuums z. B. gegenüber einer Chipkarte.
PKI	Public Key-Infrastruktur Technisches Umfeld für den Einsatz asymmetrischer Kryptoverfahren. Eine PKI basiert üblicherweise auf Zertifikaten und einer Zertifizierungshierarchie. Wichtige Komponenten einer PKI sind daher die Zertifizierungsinstanzen, Registrierungsinstanzen und Verzeichnisdienste. Darüber hinaus umfasst die PKI aber auch die Teilnehmer (Anwender), dezentrale Komponenten wie z. B. Client-Komponenten zur Speicherung und Anwendung der Schlüssel und Zertifikate sowie umfassende technische und organisatorische Prozesse.
Privater Schlüssel	Geheimer Teil eines Schlüsselpaares bei asymmetrischen Schlüsselpaaren.
PSE	Personal Security Environment Speicher für kryptographische Schlüssel. Ein PSE kann als Hardware (z. B. Smartcard) oder als verschlüsselte Datei (Soft-PSE) realisiert sein.
PUK	PIN Unblocking Key Code zur Re-Aktivierung einer gesperrten PIN, dabei wird der Fehlbedienungszähler der PIN wieder zurückgesetzt.
QSCD	Qualified Signature Creation Device Eine qualifizierte elektronische Signaturerstellungseinheit im Sinne der [eIDAS].
Registrar (LRA-Registrar)	Rolle im VDA der BA, der die Registrierung der Mitarbeiter durchführt.
Registrierungsinstanz (engl. Registration Authority, RA)	Stelle eines Zertifizierungsdienstes, die die Anträge zur Ausstellung oder Sperrung von Zertifikaten erfasst und die Antragsteller identifiziert.
RFC	Request for Comment Dokumententyp der Internet Engineering Task Force (IETF), in der diese Standards vorschlägt und veröffentlicht.
RSA	Asymmetrisches Kryptoverfahren für Verschlüsselung und digitale Signatur, benannt nach Rivest, Shamir, Adleman.
SGB	Sozialgesetzbuch
SHA-1	Vom US-amerikanischen Standardisierungsinstitut normierte Hashfunktion mit 160 Bit langen Ausgabewerten.

Begriff	Erläuterung
SigG-Profile	Bezeichnung des Part 9 der Spezifikation [COMPKI]. Der Terminus SigG ist fester Bestandteil des Dokumentennamens. Das SigG (deutsches Signaturgesetz) ist seit dem 29.07.2017 außer Kraft.
Smartcard	Einzelsignaturkarte, MSK, Gästekarte werden unter dem Begriff Smartcard zusammengefasst.
Sperrliste	Liste, in der ein Anbieter eines Zertifizierungsdienstes die Sperrinformation der von ihm ausgestellten und noch nicht abgelaufenen Zertifikate veröffentlicht.
Sperroperator (LRA-Sperroperator)	Rolle im Zertifizierungsdienst der BA, der die Sperrung von Mitarbeiterzertifikaten in einer LRA durchführt.
Sperrstatus	Status eines Zertifikates bzgl. Sperrung.
TS	Technical Standard Bezeichnung für technische Standards bei ETSI.
TSP	Time Stamp Protokoll Protokoll zur Anforderung und Ausgabe eines Zeitstempels.
Verschlüsselungszertifikat	Zertifikat zu einem Schlüsselpaar (z. B. auf einer digitalen Dienstkarte oder Gästekarte), dass eine verschlüsselte Kommunikation ermöglicht.
Verzeichnisdienst	In einer PKI: Dienst über den Zertifikaten oder Informationen zu Zertifikaten (z. B. Sperrinformationen) oder der PKI abgerufen werden können.
Wurzel-CA	Oberste Zertifizierungsinstanz einer Zertifizierungshierarchie. Das Zertifikat der Wurzel-CA wird von ihr selbst signiert und muss den Teilnehmern der PKI auf eine vertrauenswürdige Weise (z. B. Offline) zugänglich gemacht werden.
X.509	Von der ITU definierter Standard, der unter anderem die heute überwiegend verwendeten Datenformate für Zertifikate und Sperrlisten definiert.
Zeitstempel	Elektronische Bestätigung, dass gewisse Daten zu einem bestimmten Zeitpunkt vorgelegen haben. Ein Zeitstempel enthält üblicherweise eine digitale Signatur über die mit der aktuellen Zeitinformation versehenen vorgelegten Daten.
Zeitstempeldienst	Dienst der Zeitstempel ausstellt.
Zertifikat	Eine elektronische Bescheinigung, mit der ein öffentlicher Schlüssel dem Zertifikatsinhaber zugeordnet wird und dessen Identität bestätigt wird. Ein Zertifikat enthält Angaben zum Inhaber, zum Aussteller und zur Nutzung des Zertifikates sowie den öffentlichen Schlüssel des Inhabers. Außerdem enthält das Zertifikat eine digitale Signatur, welche die Authentizität und Integrität der im Zertifikat enthaltenen Daten sicherstellt.
Zertifikatsinhaber/Zertifikatsnehmer	Entität, für die das Zertifikat ausgestellt wird.
Zertifizierungsdienst	Dienst, der Zertifikate ausstellt oder andere Dienstleistungen im Zusammenhang mit Zertifikaten erbringt, beispielsweise Verzeichnisdienste, Schlüsselhinterlegungsdienste.

Begriff	Erläuterung
Zertifizierungshierarchie	Hierarchisch geordnete Struktur bestehend aus den Zertifizierungsinstanzen und den von ihnen ausgestellten Zertifikaten. Auf der untersten Hierarchie-Ebene stehen die Zertifikate der Endanwender. Unter jeder Zertifizierungsinstanz hängen an entsprechenden Ästen die Entitäten, für die sie Zertifikate ausstellen. Die oberste(n) Zertifizierungsinstanz(en) nennt man Wurzel-CA(s).
Zertifizierungsinstanz	Logische Einheit eines Zertifizierungsdienstes zur Ausstellung (Signierung) von Zertifikaten. Jeder Zertifizierungsinstanz sind jeweils ein oder mehrere Schlüsselpaare zur Signierung der Zertifikate zugeordnet.
Zertifizierungsstelle	Zertifizierungsdienstleister, der Zertifikate ausstellt.