

Trustcenter der Deutschen Rentenversicherung

Vertrauensdiensteanbieter Deutsche Rentenversicherung Bund nach eIDAS-VO

TSA Policy des Zeitstempeldienstes DRV QC Root TSA

Dokument-OID: 1.3.6.1.4.1.22204.1.8.1.1.3

Version	06.00.00
Stand	21.04.17
Dateiname	TCDRV_TP_DRV-QC-Root-TSA_060000_20170421_DE.pdf
Produktzustand	Freigegeben
Vertraulichkeit	Keine Beschränkungen

Inhaltsverzeichnis

1	Einleitung	4
1.1	Überblick	4
1.2	Dokumentenname sowie Identifikation	6
1.3	Teilnehmer des Zeitstempeldienstes DRV QC Root TSA	6
1.4	Anwendungsbereich	7
1.5	Verwaltung der Richtlinie	7
1.6	Definitionen und Abkürzungen	7
2	Veröffentlichungen und Verzeichnisdienst	8
2.1	Verzeichnisdienste	8
2.2	Veröffentlichung von Informationen	8
2.3	Aktualisierung der Informationen (Zeitpunkt, Frequenz)	9
2.4	Zugangskontrolle zu Verzeichnisdiensten	9
3	Identifizierung und Authentifizierung	10
3.1	Namen	10
3.2	Identitätsüberprüfung bei Neuantrag	10
3.3	Identitätsüberprüfung bei Erneuerung	10
3.4	Identifizierung und Authentifizierung von Sperranträgen	10
4	Ablauforganisation (Time Stamp Lifecycle)	11
4.1	Zeitstempel-Antrag	11
4.2	Bearbeitung von Zeitstempel-Anträgen	11
4.3	Erstellung von Zeitstempeln	11
4.4	Akzeptanz von Zeitstempeln	14
4.5	Verwendung von Zeitstempeln	14
4.6	Erneuerung von Zeitstempeln unter Beibehaltung des alten Schlüssels	15
4.7	Erneuerung von Zeitstempeln mit neuem Schlüssel	15
4.8	Modifizierung	15
4.9	Widerruf / Sperrung von Zeitstempeln	15
4.10	Dienst zur Statusabfrage von Zertifikaten (OCSP)	15
4.11	Beendigung des Vertragsverhältnisses	15
4.12	Schlüsselhinterlegung und -wiederherstellung	15
5	Infrastrukturelle, organisatorische und personelle Sicherheitsmaßnahmen	16
5.1	Infrastrukturelle Sicherheitsmaßnahmen	16
5.2	Organisatorische Sicherheitsmaßnahmen	16
5.3	Personelle Sicherheitsmaßnahmen	16
5.4	Überwachung / Protokollierung	16
5.5	Archivierung	16
5.6	Schlüsselwechsel	17
5.7	Kompromittierung und Wiederherstellung	17
5.8	Einstellung des Betriebs	17
6	Technische Sicherheitsmaßnahmen	19
6.1	Schlüsselerzeugung und Installation	19
6.2	Schutz privater Schlüssel und Einsatz kryptographischer Module	19
6.3	Weitere Aspekte des Schlüsselmanagements	19
6.4	Aktivierungsdaten	19
6.5	Sicherheitsmaßnahmen für Computer	19
6.6	Technische Maßnahmen im Lebenszyklus	19
6.7	Sicherheitsmaßnahmen für das Netzwerk	20
6.8	Zeitstempel	20
7	Profile für Zertifikate, Sperrlisten und Online-Abfragen	21

7.1	Zertifikatsprofil	21
7.2	Sperrlistenprofil.....	21
7.3	OCSP Profil	21
7.4	TSA Profil	21
8	Konformitätsprüfung (Compliance Audit, Assessments).....	22
8.1	Häufigkeit und Umstände der Überprüfung	22
8.2	Identität und Qualifikation des Überprüfers	22
8.3	Verhältnis von Prüfer zu Überprüfem	22
8.4	Überprüfte Bereiche.....	22
8.5	Mängelbeseitigung.....	22
8.6	Veröffentlichung der Ergebnisse	22
9	Weitere geschäftliche und rechtliche Angelegenheiten	23
9.1	Gebühren.....	23
9.2	Finanzielle Verantwortung	23
9.3	Vertraulichkeit von Geschäftsinformationen	23
9.4	Schutz personenbezogener Daten.....	24
9.5	Urheberrechte.....	24
9.6	Pflichten.....	24
9.7	Haftung.....	25
9.8	Haftungsbeschränkung	25
9.9	Haftungsfreistellung	25
9.10	Inkrafttreten und Aufhebung.....	25
9.11	Individuelle Benachrichtigungen und Kommunikation mit Teilnehmern	25
9.12	Änderungen der Richtlinie.....	26
9.13	Konfliktbeilegung	26
9.14	Geltendes Recht.....	26
9.15	Konformität mit geltendem Recht.....	26
9.16	Weitere Regelungen	27
9.17	Andere Regelungen.....	27
10	Abkürzungen und Begriffe	28
10.1	Abkürzungen	28
10.2	Begriffe	31
11	Informationen zum Dokument.....	33
11.1	Änderungsverzeichnis.....	33
11.2	Abbildungsverzeichnis	33
11.3	Tabellenverzeichnis	33
11.4	Referenzen	34

1 Einleitung

1.1 Überblick

Die Träger der Deutschen Rentenversicherung (DRV) betreiben ein gemeinschaftliches Trustcenter der DRV zur Bereitstellung von qualifizierten Vertrauensdiensten gemäß eIDAS-VO [1]. Im Trustcenter der DRV sind die folgenden Vertrauensdiensteanbieter tätig, welche qualifizierte Vertrauensdienste bereitstellen:

(1) VDA DRV Bund stellt bereit:

- Zertifikatsdienst DRV QC Root CA:
Qualifizierter Vertrauensdienst DRV QC Root CA für die Ausstellung von:
 - Ausstellerzertifikaten für DRV QC Root CA, DRV QC 70 MA CA, DRV QC 13 MA CA und DRV QC 11 MA CA,
 - Zertifikaten des Zeitstempeldienstes DRV QC Root TSA,
 - Zertifikaten des Validierungsdienstes DRV QC Root OCSP;
- Zeitstempeldienst DRV QC Root TSA:
Qualifizierter Vertrauensdienst DRV QC Root TSA für die Ausstellung:
 - qualifizierter elektronischer Zeitstempel;
- Zertifikatsdienst DRV QC 70 MA CA:
Qualifizierter Vertrauensdienst DRV QC 70 MA CA für die Ausstellung von:
 - qualifizierten EE-Zertifikaten,
 - Zertifikaten des Validierungsdienstes DRV QC 70 MA OCSP;

(2) VDA DRV Rheinland stellt bereit:

- Zertifikatsdienst DRV QC 13 MA CA:
Qualifizierter Vertrauensdienst DRV QC 13 MA CA für die Ausstellung von:
 - qualifizierten EE-Zertifikaten,
 - Zertifikaten des Validierungsdienstes DRV QC 13 MA OCSP;

(3) VDA DRV Westfalen stellt bereit:

- Zertifikatsdienst DRV QC 11 MA CA:
Qualifizierter Vertrauensdienst DRV QC 11 MA CA für die Ausstellung von:
 - qualifizierten EE-Zertifikaten,
 - Zertifikaten des Validierungsdienstes DRV QC 11 MA OCSP.

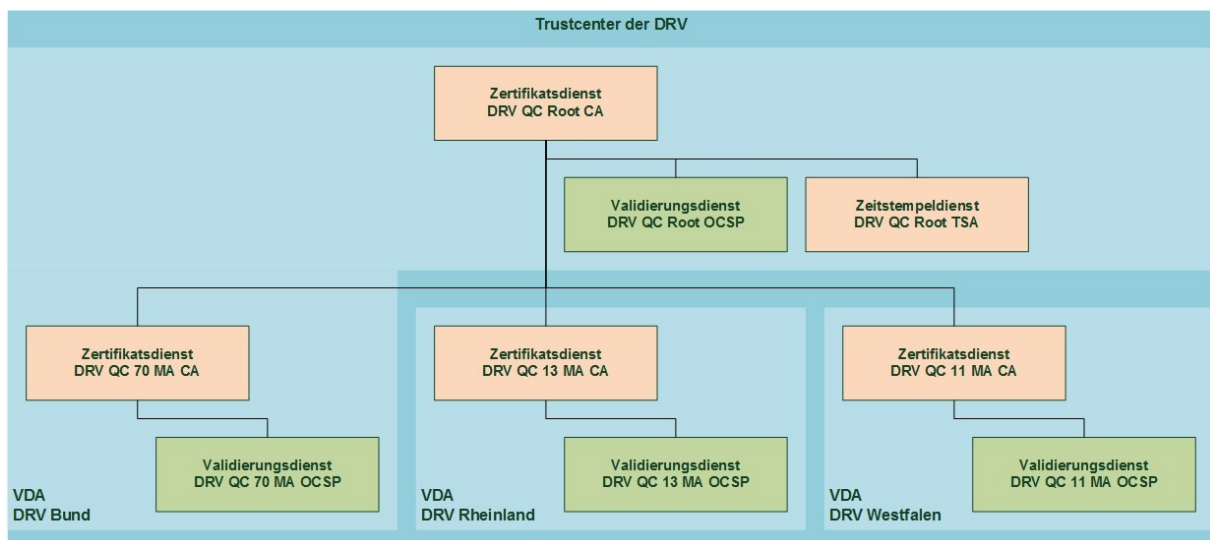


Abbildung 1 Qualifizierte Vertrauensdienste im Trustcenter der DRV

Die folgende Abbildung gibt einen Überblick über die Richtlinien Dokumente des Zeitstempeldienstes DRV QC Root TSA.

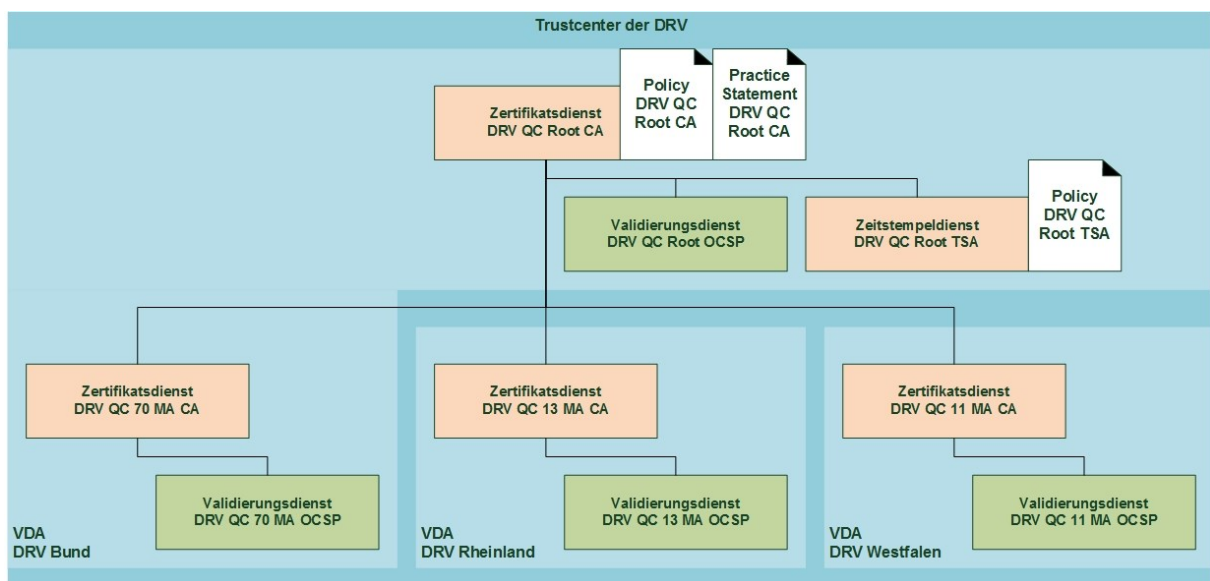


Abbildung 2 Richtlinien Dokumente des Zeitstempeldienstes DRV QC Root TSA

Diese Policy ist gemäß RFC 3647 (siehe [2]) strukturiert.

1.2 Dokumentenname sowie Identifikation

Dokumentname: Policy des Zeitstempeldienstes DRV QC Root TSA

OID: 1.3.6.1.4.1.22204.1.8.1.1.3

PEN-DRV-Bund (1.3.6.1.4.1.22204).Trustcenter (1). Policies (8).
QC-CP (1). Produktivsystem (1). QC-Root-TSA (3)

Diese Policy des Zeitstempeldienstes DRV QC Root TSA berücksichtigt die relevanten ETSI Normen:

- ETSI EN 319401: Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers [4];
- ETSI EN 319421: Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps [5];
- ETSI EN 319422: Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles [6].

Der Standard ETSI EN 319401 definiert die generellen Anforderungen an einen Vertrauensdiensteanbieter. Für Vertrauensdiensteanbieter von Zeitstempeldiensten sind die Anforderungen im Standard ETSI EN 319421 und die Protokolldaten im Standard ETSI EN 319422 detailliert beschrieben.

1.3 Teilnehmer des Zeitstempeldienstes DRV QC Root TSA

1.3.1 Zertifikatsdienste

Die Träger der Deutschen Rentenversicherung betreiben ein gemeinschaftliches Trustcenter der DRV. Zu den Leistungen des Trustcenters der DRV gehört u.a. der Zeitstempeldienst DRV QC Root TSA, der qualifizierte Zeitstempel gemäß Artikel 42 der eIDAS-VO ausstellt.

Der VDA DRV Bund betreibt einen qualifizierten Zertifikatsdienst, der u.a. qualifizierte Zertifikate für den Zeitstempeldienst DRV QC Root TSA ausstellt.

Der VDA DRV Bund betreibt weiterhin einen nicht-qualifizierten Zertifikatsdienst DRV NQ Root CA und darunter mehrere nicht-qualifizierte Zertifikatsdienste zur Erstellung von Authentisierungs- und Verschlüsselungs-Zertifikaten. Im Zusammenhang mit dem Zeitstempeldienst DRV QC Root TSA erstellt ein nicht-qualifizierter Zertifikatsdienst Authentisierungs-Zertifikate für die Benutzer des Zeitstempeldienstes.

Die Anwendungen des VDA DRV Bund für Nutzer des qualifizierten Zeitstempeldienstes sind barrierefrei. Es gibt keine Einschränkungen für Anwender mit Behinderungen.

1.3.2 Zeitstempeldienst

Der VDA DRV Bund betreibt den qualifizierten Vertrauensdienst DRV QC Root TSA zur Erstellung qualifizierter Zeitstempel gemäß Artikel 42 eIDAS-VO.

1.3.3 Anwender (Subscriber)

Die Benutzer des Zeitstempeldienstes DRV QC Root TSA sind Personen bzw. Verantwortliche von Systemen, die qualifizierte Zeitstempel anfordern können.

Die Benutzung des Zeitstempeldienstes DRV QC Root TSA erfolgt auf der Grundlage einer Verwaltungsvereinbarung zwischen dem VDA DRV Bund und den nutzenden Institutionen.

1.3.4 Vertrauende Parteien (Relying Parties)

Der Kreis der vertrauenden Parteien ist nicht beschränkt. Der Status der qualifizierten Zertifikate, die zur Erstellung eines qualifizierten Zeitstempels genutzt wurden, können über das Internet und das DRV-Netz geprüft werden.

1.3.5 Weitere Teilnehmer

Keine Angaben.

1.4 Anwendungsbereich

1.4.1 Geeignete Nutzung

Der Zeitstempeldienst DRV QC Root TSA erstellt qualifizierte Zeitstempel gemäß Artikel 42 eIDAS-VO. Berechtigte Benutzer können qualifizierte Zeitstempel abrufen. Die qualifizierten Zeitstempel dürfen in den Anwendungen der berechtigten Benutzer verwendet werden.

1.4.2 Untersagte Nutzung

Die Verwendung der qualifizierten Zeitstempel für andere als die in diesem Dokument in Kapitel 1.4.1 genannten Zwecke ist nicht erlaubt.

1.5 Verwaltung der Richtlinie

1.5.1 Änderungsmanagement

Für die Verwaltung dieses Dokumentes ist die Deutsche Rentenversicherung Bund zuständig.

1.5.2 Ansprechpartner

Folgende Ansprechewege hinsichtlich dieser Policy bestehen:

Postadresse: Deutsche Rentenversicherung Bund
Abteilung Organisation und IT-Services
Trustcenter der Deutschen Rentenversicherung
10704 Berlin

Das Dokument "Policy des Zeitstempeldienstes DRV QC Root TSA" wird gemäß Kapitel 2.2 nach seiner Freigabe veröffentlicht.

1.5.3 Verantwortliche Stelle zur Prüfung der Regelungen zum Betrieb

Für die Prüfung der Regelungen zum Betrieb des Zeitstempeldienstes im Dokument Certification Practice Statements ist die gleiche Stelle wie für diese TSA Policy zuständig (Siehe Kapitel 1.5.2).

1.5.4 Verfahren zur Genehmigung der Regelungen zum Betrieb

Ein Genehmigungsverfahren ist nicht festgelegt. Konsistenz zwischen TSA Policy und Certification Practice Statements wird dadurch erreicht, dass beide Dokumente in der Verantwortung einer organisatorischen Einheit liegen.

1.6 Definitionen und Abkürzungen

Die Begriffe und Abkürzungen sind in Kapitel 10 definiert.

2 Veröffentlichungen und Verzeichnisdienst

2.1 Verzeichnisdienste

Die vom Zertifikatsdienst DRV QC Root CA ausgestellten Zertifikate (CA-, TSA- und OCSP-Zertifikate) werden im Verzeichnisdienst des Trustcenters der DRV veröffentlicht und zum Abruf bereitgestellt.

OCSP-Auskünfte werden für die ausgestellten Zertifikate durch den jeweiligen OCSP-Responder erteilt.

Die ausgestellten Zertifikate enthalten die Dienstadressen des Verzeichnisdienstes zum öffentlichen Abruf von CA-Zertifikaten und des Validierungsdienstes zum öffentlichen Abruf von OCSP-Statusauskünften.

2.1.1 Verzeichnisdienst

Im Verzeichnisdienst werden die von den qualifizierten Zertifikatsdiensten ausgestellten Systemzertifikate veröffentlicht (CA-, OCSP- und TSA-Zertifikate). Diese Zertifikate sind öffentlich abrufbar.

Die veröffentlichten Informationen können vom Verzeichnisdienst über die Protokolle HTTP und LDAP aus dem Internet und dem DRV-Netz anonym abgerufen werden. Die Adressen der LDAP- und HTTP-Dienste zum Download für Herausgeber CA-Zertifikate sind in den ausgestellten Zertifikaten in der Extension „IssuerAltName (IAN)“ enthalten.

Der Verzeichnisdienst wird hochverfügbar 24 Stunden am Tag, 7 Tage die Woche betrieben.

2.1.2 Validierungsdienst

Der Status der ausgestellten Zertifikate kann über den jeweiligen Validierungsdienst (OCSP-Responder) abgefragt werden. Der OCSP-Responder erteilt Vorhandenseins- und Sperrauskünfte. Die notwendigen Informationen für den Zugriff auf den Validierungsdienst sind in ausgestellten Zertifikaten in der Extension „AuthorityInfoAccess (AIA)“ enthalten.

Der Validierungsdienst wird hochverfügbar 24 Stunden am Tag, 7 Tage die Woche betrieben.

2.1.3 Vertrauensliste der Bundesnetzagentur

Die vom qualifizierten Zertifikatsdienst DRV QC Root CA ausgestellten Systemzertifikate für qualifizierte Vertrauensdienste (CA- und TSA-Zertifikate) werden an die nationale Aufsichtsstelle gemäß Artikel 17 eIDAS-VO [1] übermittelt. Die Aufsichtsstelle veröffentlicht diese Zertifikate bei Vorliegen eines gültigen Konformitätsbewertungsberichtes (Siehe Kapitel 8) gemäß Artikel 22 eIDAS-VO in der nationalen Vertrauensliste [13].

2.2 Veröffentlichung von Informationen

Das vorliegende Dokument " Policy des Zeitstempeldienstes DRV QC Root TSA " wird auf der Web-Seite des VDA DRV Bund [11] veröffentlicht:

Die Nutzungsbedingungen des Zeitstempeldienstes DRV QC Root TSA werden in Form eines "TSA Disclosure Statements" auf der Web-Seite des VDA DRV Bund veröffentlicht.

Dokumentname: TSA Disclosure Statements des Zeitstempeldienstes DRV QC Root TSA

Dokument-OID: 1.3.6.1.4.1.22204.1.8.6.1.3

Für den Zeitstempeldienstes DRV QC Root TSA wird kein separates Dokument "TSA Practice Statements" erstellt. Sofern erforderlich werden Festlegungen im Dokument Certification Practice Statements des Zertifikatsdienstes DRV QC Root CA [8] übernommen. Das betrifft insbesondere die Kapitel 5 und 6 bzgl. der Sicherheitsmaßnahmen im Trustcenter der DRV.

Die Webseite des VDA DRV Bund wird hochverfügbar 24 Stunden am Tag, 7 Tage die Woche betrieben.

2.3 Aktualisierung der Informationen (Zeitpunkt, Frequenz)

Die Aktualisierung der Informationen hängt von ihrem Typ ab. Die folgende Tabelle fasst die relevanten Informationen zusammen:

Tabelle 1: Veröffentlichte Informationen

Information	Frequenz der Aktualisierung	Zeitpunkt der Veröffentlichung	Ziel der Veröffentlichung
Dokument TSA Policy	Aktualisierung bei Bedarf	Nach Freigabe des Dokumentes	• Web-Seite des VDA DRV Bund
Dokument TSA Disclosure Statements	Aktualisierung bei Bedarf	Nach Freigabe des Dokumentes	• Web-Seite des VDA DRV Bund

2.4 Zugangskontrolle zu Verzeichnisdiensten

Die Zugangskontrolle zu den Veröffentlichungspunkten im Trustcenter der DRV ist wie folgt vorgesehen:

Tabelle 2: Zugangskontrolle zu Veröffentlichungspunkten

Veröffentlichungspunkt	Zugriffsart	Zugriff durch	Zugriffsschutz
Web-Seite VDA DRV Bund	Erstellen, Ändern, Löschen	Web-Admin	Authentisierung erforderlich
	Lesen	Unbeschränkt	Anonym

3 Identifizierung und Authentifizierung

In diesem Kapitel werden die Identifizierung und Authentifizierung der Anwender des qualifizierten Zeitstempeldienstes behandelt.

3.1 Namen

Nicht relevant.

3.2 Identitätsüberprüfung bei Neuantrag

3.2.1 Nachweis des Besitzes des privaten Schlüssels

Nicht relevant.

3.2.2 Identifizierung einer Organisation

Die Benutzer des Zeitstempeldienstes DRV QC Root TSA authentisieren sich an einem vor den Zeitstempeldienst DRV QC Root TSA geschalteten TLS-Proxy-Server mittels TLS-Client-Authentisierung. Die Client-Zertifikate zur Authentisierung werden vom VDA DRV Bund für die Organisation des Benutzers ausgestellt.

Vor der Nutzung des Zeitstempeldienstes DRV QC Root TSA muss die nutzende Institution eine Verwaltungsvereinbarung mit dem Trustcenter der Deutschen Rentenversicherung abschließen.

3.2.3 Identifizierung natürlicher Personen

Nicht relevant.

3.2.4 Nicht überprüfte Teilnehmerangaben

Keine Angaben.

3.2.5 Überprüfung der Berechtigung

Keine Angaben.

3.2.6 Kriterien für Zusammenarbeit

Keine Angaben.

3.3 Identitätsüberprüfung bei Erneuerung

Die Nutzung des Zeitstempeldienstes DRV QC Root TSA erfolgt i.d.R. für ein Jahr mit jährlicher Verlängerung, sofern keine Kündigung durch einen Partner erfolgt.

3.4 Identifizierung und Authentifizierung von Sperranträgen

Zeitstempel können nicht gesperrt werden.

4 Ablauforganisation (Time Stamp Lifecycle)

4.1 Zeitstempel-Antrag

Von berechtigten Personen und Systemen können Zeitstempel über folgende URL angefordert werden:

<https://tsp.tc.deutsche-rentenversicherung.de>

Das Format der Anfrage sowie der Antwort sind konform zu den Standards RFC 3161 [2] und ETSI 319422 [6]. Die im Antrag gelieferten Daten sind das Ergebnis einer Hashwert-Bildung auf Seite des Antragstellers. Unterstützte Hash-Algorithmen sind SHA-256 und SHA-512.

4.2 Bearbeitung von Zeitstempel-Anträgen

Qualifizierte Zeitstempel können nur von Personen bzw. Systemen angefordert werden, die über ein Authentifizierungszertifikat vom VDA DRV Bund verfügen. Die Authentifizierung des Benutzers erfolgt bei Anforderung eines Zeitstempels über einen TLS-Proxy-Server mit Client-Authentisierung vor dem eigentlichen Zeitstempeldienst.

Das Authentisierungszertifikat wird im Zeitstempeldienst DRV QC Root TSA hinterlegt und als berechtigt konfiguriert. Ein solches Authentisierungszertifikat erhalten die berechtigten Benutzer (Siehe Kapitel 1.3.3) nach Abschluss der dort erwähnten Verwaltungsvereinbarung mit dem VDA DRV Bund.

Der Antrag auf einen Zeitstempel wird im "Request Format" gemäß RFC 3161 [3] erwartet. Es werden u.a. folgende Felder unterstützt:

- Version (Pflichtfeld);
- MessageImprint (Daten, für die ein Zeitstempel angefordert wird; Pflichtfeld);
- Nonce (Zufallszahl gegen Replay-Attacken; optional);
- CertReq (Anforderung der Zertifikatskette der Zeitstempeldiensteinheit; optional).

4.3 Erstellung von Zeitstempeln

4.3.1 Zeitstempeldienst-Instanzen

Im Trustcenter der DRV wird der Zeitstempeldienst DRV QC Root TSA betrieben. Der Begriff Zeitstempeldienst (TSA) bezeichnet den Dienst als Ganzes. Der Begriff Zeitstempeldienst-Instanz (TSU) bezeichnet eine einzelne TSA Instanz, welche Zeitstempel mit dedizierten Signaturerstellungseinheiten erstellt. Der Zeitstempeldienst DRV QC Root TSA umfasst 2 aktive Instanzen im Haupt-System und 2 stand-by Instanzen im Backup-System.

Eine Zeitstempel-Instanz ist logisch in Funktionsblöcke unterteilt, die für einzelne Aufgaben wie z.B. Monitoring der Signaturerstellungseinheiten, Zeitüberwachung, Zeitaktualisierung, Signaturerstellung zuständig sind.

4.3.2 Zeitstempel Signaturschlüssel

Der Zeitstempeldienst DRV QC Root TSA erstellt qualifizierte Zeitstempel, in dem die übergebenen Daten im Format eines Hashwertes zusammen mit einem Zeitstempel qualifiziert elektronisch signiert werden.

Die Anforderungen an die qualifizierte Signaturerstellungseinheit des Zeitstempeldienstes DRV QC Root TSA werden erfüllt.

- Vertraulichkeit: Die Signaturschlüssel werden in Chipkarten als qualifizierte Signaturerstellungseinheit erstellt und können nicht exportiert werden,
- Einmaligkeit: Die Signaturschlüssel werden in Chipkarten auf Basis des internen Zufallsgenerators generiert. Der Zufallsgenerator der eingesetzten Chipkarte sorgt dafür, dass generierte Schlüssel zufällig und damit weitest möglich einmalig sind.
- Nichtableitbarkeit: Für Signaturschlüssel wird ein RSA 2048 Bit Schlüsselpaar erstellt. Gemäß dem aktuellen nationalen Algorithmen-Katalog [12] ist die Nichtableitbarkeit bis Ende 2022 gegeben.
- Zweckbindung: Die Signaturschlüssel stehen nur dem Zeitstempeldienst DRV QC Root TSA zur Verfügung. Die Zweckbindung ist im qualifizierten Zertifikat angegeben.
- Die zum Erstellen des qualifizierten Zeitstempels übergebenen Daten werden durch die qualifizierte Signaturerstellungseinheit nicht geändert. Eine Anzeige dieser Daten ist im automatisierten Betrieb nicht vorgesehen.
- Die qualifizierten Signaturerstellungseinheiten für den Zeitstempeldienst DRV QC Root TSA werden vom Zertifikatsdienst DRV QC Root CA erstellt und verwaltet.
- Die Signaturschlüssel des Zeitstempeldienstes DRV QC Root TSA werden nicht gesichert oder archiviert. Dies ist mit den eingesetzten Chipkarten technisch nicht möglich.

Der Zeitstempeldienst DRV QC Root TSA hat zur Erstellung von Zeitstempeln mindestens sechs Signaturchipkarten als qualifizierte Signaturerstellungseinheiten (QSCD) zur Verfügung:

- jede der beiden Zeitstempeldienst-Instanzen im Haupt-System erhält mindestens eine QSCD,
- eine Ersatz QSCD für das Haupt-System,
- jede der beiden Zeitstempeldienst-Instanzen im Backup-System erhält mindestens eine QSCD,
- eine Ersatz QSCD für den Backupstandort.

Jede dieser Signaturchipkarten beinhaltet einen individuellen Signaturschlüssel. Die erzeugten qualifizierten Zeitstempel sind mit dem Signaturprüfchlüssel des Zeitstempeldienstes verifizierbar. Der Signaturprüfchlüssel ist im Zertifikat des Zeitstempeldienstes enthalten, es wird im erstellten Zeitstempel mitgeliefert.

4.3.3 Zeitstempel Signaturzertifikat

Die Anforderungen an die Zertifikate des Zeitstempeldienstes DRV QC Root TSA werden erfüllt.

- Die qualifizierten Zertifikate des Zeitstempeldienstes DRV QC Root TSA beinhalten ein QC Statement, das zur maschinellen Prüfung die Attribute QcsCompliance und QcsQcSSCD beinhaltet.
- Die qualifizierten Zertifikate des Zeitstempeldienstes DRV QC Root TSA beinhalten den Namen des Zertifikatsdienstes DRV QC Root CA als Herausgeber.
- Die qualifizierten Zertifikate des Zeitstempeldienstes DRV QC Root TSA beinhalten den öffentlichen Schlüssel des Zeitstempeldienstes, der zur Validierung der signierten Zeitstempel-Antwort erforderlich ist.
- Die qualifizierten Zertifikate des Zeitstempeldienstes DRV QC Root TSA beinhalten Angaben zu ihrer Gültigkeit.
- Die qualifizierten Zertifikate des Zeitstempeldienstes DRV QC Root TSA beinhalten eine Seriennummer, welche zusammen mit dem Herausgeber als eindeutiges Identifikationsmerkmal dient.
- Die qualifizierten Zertifikate des Zeitstempeldienstes DRV QC Root TSA beinhalten die URL, von der das Zertifikat des Herausgebers geladen werden kann.
- Die qualifizierten Zertifikate des Zeitstempeldienstes DRV QC Root TSA beinhalten die URL des Validierungsdienstes (OCSP-Responder), der zur Zertifikatsstatusprüfung genutzt werden soll.
- Die qualifizierten Zertifikate des Zeitstempeldienstes DRV QC Root TSA beinhalten die OID der zugehörigen Certificate Policy [7]. Diese Policy definiert die Nutzung von sicheren Signaturerstellungseinheiten zur Erstellung qualifizierter Signaturen.
- Die qualifizierten Zertifikate des Zeitstempeldienstes DRV QC Root TSA beinhalten eine qualifizierte elektronische Signatur des Zertifikatsdienstes DRV QC Root CA.

Die Zertifikate des Zeitstempeldienstes DRV QC Root TSA werden vom Zertifikatsdienst DRV QC Root CA ausgestellt. Sie beinhalten alle den gleichen Namen als Zertifikatsinhaber (Subject) und unterscheiden sich in der Zertifikatsseriennummer. Weitere Festlegungen zu den Zertifikaten sind in der Certificate Policy des Zertifikatsdienstes DRV QC Root CA definiert [7].

4.3.4 Zeitstempel

Der Zeitstempeldienst DRV QC Root TSA erstellt Zeitstempel konform zur Norm ETSI EN 319422 [6] und gemäß den Anforderungen der eIDAS-VO.

- Der aktuelle Zeitstempel wird mit den gelieferten Daten durch eine qualifizierte elektronische Signatur verbunden. Ein unbemerktes Verändern der verbundenen Daten ist nach heutigem Ermessen nicht möglich.
- Der Zeitstempel wird mittels Funkuhr vom Zeitzeichensender DCF77 abgeleitet. Die Genauigkeit des Zeitstempels ist mindestens 1 Sekunde.
- Die qualifizierte elektronische Signatur wird durch eine geprüfte (Common Criteria Prüfstärke EAL4+) qualifizierte Signaturerstellungseinheit erstellt. Das Trustcenter der DRV stellt für jede Signaturerstellungseinheit ein eigenes qualifiziertes Zertifikat durch seinen Zertifikatsdienst DRV QC Root CA aus.

Qualifizierte elektronische Zeitstempel werden im "Response Format" gemäß RFC 3161 [3] erstellt. Es werden u.a. folgende Felder unterstützt:

- Version (Pflichtfeld);
- Policy (BTSP; Pflichtfeld);
- MessageImprint (Daten, für die ein Zeitstempel angefordert wird; Pflichtfeld);
- SerialNumber (Hashwert gebildet aus PID und Uhrzeit; Pflichtfeld);
- GenTime (Zeitpunkt der Erstellung des Zeitstempels, Pflichtfeld);
- Accuracy (Genauigkeit des Zeitstempels, optional);
- Nonce (Zufallszahl, Kopie aus der Anfrage; optional);
- TSAName (Name des Zeitstempeldienstes, optional);
- Certificates (Zertifikatskette der Zeitstempeldiensteinheit auf Anforderung; optional).

4.3.5 Zeitsynchronisation

Der Zeitstempeldienst DRV QC Root TSA stellt die Zeitstempel mit der gesetzlichen deutschen Zeit mit einer Genauigkeit von mindestens 1 Sekunde aus. Die Synchronisation der Uhr des Zeitstempeldienstes mit der gesetzlichen deutschen Zeit erfolgt einmal am Tag.

Ein interner Vergleich der Systemuhr gegen die externe Zeitquelle erfolgt alle 10 Sekunden. Eine Plausibilitätsprüfung prüft auf sprunghafte Änderungen. Die maximale Differenz zwischen System-Zeit und DCF77-Zeit darf den Wert von 1 Sekunde im Normalfall nicht überschreiten. Bei Feststellung einer Gangabweichung größer als eine Sekunde stellt der Zeitstempeldienst seinen Dienst automatisch ein.

Der Sonderfall von Schaltsekunden wird durch die Zeitsynchronisation berücksichtigt und führt nicht zu einem Ausfall der Systeme. Die Erkennung von Schaltsekunden erfolgt über eine Kennung in den Zeitlegrammen des Zeitzeichensenders DCF77 (Siehe [15]). In der Logdatei des Zeitstempeldienstes werden Schaltsekunden eingetragen.

Als Quelle der gesetzlichen Zeit dient ein DCF77-Funkempfänger für das Zeitsignal des Zeitzeichensenders DCF77. Der Zeitzeichensender verwendet die Uhrzeit des deutschen Zeitlabors UTC(PTB) (Siehe [16]).

4.4 Akzeptanz von Zeitstempeln

Die erstellten qualifizierten Zeitstempel sind mit Auslieferung gültig. Zur Validierung eines Zeitstempels sind folgende Prüfungen erforderlich:

- Prüfung von Signatur des Zeitstempels;
- Prüfung des Signaturzertifikates der Zeitstempeldienstes DRV QC Root TSA (Zertifikat ist im Zeitstempel beinhaltet);
- Prüfung des Signaturzertifikates des Zertifikatsdienstes DRV QC Root CA (Zertifikat ist im Zeitstempel beinhaltet).

4.5 Verwendung von Zeitstempeln

Im Zeitstempel ist die Zertifikatskette des Zeitstempeldienstes DRV QC Root TSA enthalten. Die Zertifikate beinhalten u.a. die URL des Validierungsdienstes (OCSP-Responder) DRV QC Root OCSP, über den der Sperrstatus der Zertifikate geprüft werden kann.

4.6 Erneuerung von Zeitstempeln unter Beibehaltung des alten Schlüssels

Nicht relevant.

4.7 Erneuerung von Zeitstempeln mit neuem Schlüssel

Nicht relevant.

4.8 Modifizierung

Nicht relevant.

4.9 Widerruf / Sperrung von Zeitstempeln

Nicht relevant.

4.10 Dienst zur Statusabfrage von Zertifikaten (OCSP)

4.10.1 Betriebsbedingte Eigenschaften

Der Validierungsdienst (OCSP-Responder) ist mit jeweils zwei Instanzen im Haupt-System und im Backup-System implementiert. Es ist entweder das Haupt-System oder das Backup-System aktiv. Zwischen den beiden Instanzen eines Systems erfolgt eine Lastverteilung.

4.10.2 Verfügbarkeit des Dienstes

Der Validierungsdienst (OCSP-Responder) wird hochverfügbar betrieben und soll eine Verfügbarkeit von 99,5% pro Jahr erreichen.

4.10.3 Weitere Merkmale

Keine Angaben.

4.11 Beendigung des Vertragsverhältnisses

Wenn das Vertragsverhältnis zwischen dem VDA DRV Bund und dem Benutzer des Zeitstempeldienstes DRV QC Root TSA beendet werden soll, muss die Verwaltungsvereinbarung (Siehe Kapitel 1.3.3) von einer Partei gekündigt werden.

4.12 Schlüsselhinterlegung und -wiederherstellung

Eine Hinterlegung von privaten Schlüsseln für qualifizierte Zertifikate ist nicht vorgesehen.

5 Infrastrukturelle, organisatorische und personelle Sicherheitsmaßnahmen

5.1 Infrastrukturelle Sicherheitsmaßnahmen

Der Zeitstempeldienst DRV QC Root TSA wird auf dedizierten Servern betrieben. Diese Server sind im Rechenzentrum des Trustcenters der DRV aufgebaut. Sowohl das Rechenzentrum als auch die Racks sind physikalisch gesichert. Nur autorisierte Personen haben physikalischen Zugang zu diesen Systemen.

Der logische Zugang zu den Systemen ist per Firewall vom Netz der DRV bzw. vom Internet begrenzt auf die Erstellung von qualifizierten Zeitstempeln.

Die Sicherheitsmaßnahmen werden detailliert im Dokument Certification Practice Statements des Zertifikatsdienstes DRV QC Root CA [8] definiert.

5.2 Organisatorische Sicherheitsmaßnahmen

Der Zeitstempeldienst DRV QC Root TSA wird durch den VDA DRV Bund betrieben. Die Anforderungen an die Organisation sind im Sicherheitskonzept des Zertifikatsdienstes DRV QC Root CA beschrieben. Die konkrete Organisation ist im Organisationskonzept des Trustcenters der DRV definiert. Die Zuordnung von Mitarbeitern zu den definierten Rollen wird elektronisch als Liste in einer Datenbank dokumentiert.

Die Sicherheitsmaßnahmen werden detailliert im Dokument Certification Practice Statements des Zertifikatsdienstes DRV QC Root CA [8] definiert.

5.3 Personelle Sicherheitsmaßnahmen

Der VDA DRV Bund führt ein Verzeichnis der aktuellen Dokumentation (Asset Management):

- Die aktuelle Dokumentation inkl. Versionsstand wird in einer Trustcenter Datenbank gepflegt.

Die Sicherheitsmaßnahmen werden detailliert im Dokument Certification Practice Statements des Zertifikatsdienstes DRV QC Root CA [8] definiert.

5.4 Überwachung / Protokollierung

Alle Aktivitäten des Zeitstempeldienstes DRV QC Root TSA werden in Log-Dateien gespeichert und archiviert. Das beinhaltet u.a.

- Anforderung und Erstellung von qualifizierten Zeitstempeln,
- Zeitsynchronisation auf Basis des Zeitzeichensenders DCF77,
- Verlust des Zeitsignals vom Zeitzeichensender,
- Fehler in der Zeitüberwachung (Abweichung größer als 1s).

Die Log-Dateien werden gesichert und archiviert.

Die Sicherheitsmaßnahmen werden detailliert im Dokument Certification Practice Statements des Zertifikatsdienstes DRV QC Root CA [8] definiert.

5.5 Archivierung

Die erstellten Zeitstempel werden zur Beweissicherung in Logdateien gespeichert und archiviert. Die Benutzer des Zeitstempeldienstes DRV QC Root TSA authentisieren sich mittels TLS-Client-Authentisierung. Die Client-Zertifikate zur Authentisierung beinhalten den

Organisationsnamen des Anwenders. Die Client-Zertifikate zur Authentisierung werden zu Protokollierungs-, Abrechnungs- und Nachweiszwecken in Logdateien des TLS-Proxy-Servers gespeichert. Die archivierten Daten bzgl. der erstellten Zeitstempel werden für 5 Jahre aufbewahrt.

5.6 Schlüsselwechsel

Die Sicherheitsmaßnahmen werden detailliert im Dokument Certification Practice Statements des Zertifikatsdienstes DRV QC Root CA [8] definiert.

5.7 Kompromittierung und Wiederherstellung

Die Wiederherstellung einer Zeitstempeldienst-Instanz bzw. des gesamten Zeitstempeldienstes DRV QC Root TSA nach einem Ausfall ist im Notfallplan geregelt. Der Notfallplan ist Bestandteil des Betriebskonzeptes des Trustcenters der DRV.

Die Sicherheitsmaßnahmen werden detailliert im Dokument Certification Practice Statements des Zertifikatsdienstes DRV QC Root CA [8] definiert.

5.8 Einstellung des Betriebs

Die Nutzer des qualifizierten Zeitstempeldienstes DRV QC Root TSA sind:

- Institutionen mit einer Verwaltungsvereinbarung mit dem VDA DRV Bund zur Nutzung des qualifizierten Zeitstempeldienstes.

Über die Einstellung des Betriebes des qualifizierten Zeitstempeldienstes DRV QC Root TSA entscheidet die Leiter des VDA DRV Bund in Abstimmung mit der Geschäftsleitung der DRV Bund

Bei der Einstellung des qualifizierten Zeitstempeldienstes DRV QC Root TSA gelten insbesondere folgende Anforderungen:

- Übertragung der Pflichten, Aufgaben und Dokumentation:
Die Pflichten, Aufgaben und Dokumentationen werden nicht an einen anderen VDA übergeben. Der Dienst wird nicht fortgesetzt.
Die Zertifikate des Zeitstempeldienstes DRV QC Root TSA werden gesperrt. Die Sperrinformation wird online durch den DRV QC Root OCSP bereitgestellt.
Die Konzepte und die Dokumentation des qualifizierten Zeitstempeldienstes werden durch den VDA DRV Bund archiviert und für den rechtlich notwendigen Zeitraum vorgehalten. Eine Einsicht in die Dokumentation kann in berechtigten Fällen beim VDA DRV Bund erfolgen.
- Informationspflicht:
Die Anwender werden vorab über die Einstellung des Betriebes informiert. Grundlage ist die Verwaltungsvereinbarung mit dem VDA DRV Bund.
Die nationale Aufsichtsstelle gemäß eIDAS-VO wird vorab über die beabsichtigte Einstellung des Betriebes informiert.
Die vertrauenden Parteien werden über die Web-Seite des VDA DRV Bund über die Einstellung des Betriebes informiert.
- Geordneter Rückbau:
Nach Einstellung des Betriebes werden alle privaten Schlüssel des Zeitstempeldienstes zerstört. Es ist dadurch nicht möglich, weiterhin Zeitstempel zu erstellen.

Die Prozeduren zur Einstellung des Betriebes des qualifizierten Zertifikatsdienstes DRV QC Root CA sind im Beendigungsplan [10] definiert.

6 Technische Sicherheitsmaßnahmen

6.1 Schlüsselerzeugung und Installation

Die Schlüsselerzeugung wird detailliert im Dokument Certification Practice Statements des Zertifikatsdienstes DRV QC Root CA [8] beschrieben.

6.2 Schutz privater Schlüssel und Einsatz kryptographischer Module

Die Maßnahmen zum Schutz der privaten Schlüssel werden detailliert im Dokument Certification Practice Statements des Zertifikatsdienstes DRV QC Root CA [8] beschrieben.

6.3 Weitere Aspekte des Schlüsselmanagements

Weitere Aspekte des Schlüsselmanagements werden detailliert im Dokument Certification Practice Statements des Zertifikatsdienstes DRV QC Root CA [8] beschrieben.

6.4 Aktivierungsdaten

Die Aktivierungsdaten werden detailliert im Dokument Certification Practice Statements des Zertifikatsdienstes DRV QC Root CA [8] beschrieben.

6.5 Sicherheitsmaßnahmen für Computer

Die Sicherheitsmaßnahmen werden detailliert im Dokument Certification Practice Statements des Zertifikatsdienstes DRV QC Root CA [8] definiert.

6.6 Technische Maßnahmen im Lebenszyklus

Der Zeitstempeldienst DRV QC Root TSA basiert auf einem zertifizierten Software-Produkt gemäß ITSEC Prüfstärke E2. Änderungen an der Installation des Produktes erfolgen (a) regulär bei Software-Änderungen durch ein Change-Request-Verfahren oder (b) als Patch im Rahmen eines Incidents. Durchgeführte Änderungen werden dokumentiert. Änderungen an der Installation werden in der Installations- und Konfigurations-Dokumentation dokumentiert.

Der Betrieb des Trustcenters der DRV wird überwacht. Im Fehlerfall wird ein Incident geöffnet und mit der Fehlerbehebung begonnen. Die Fehlerbehebung wird durch das Personal des VDA DRV Bund überwacht und koordiniert. Relevante Patches werden zeitnah eingebracht.

Festlegungen zum Incident- und Patch-Management werden detailliert im Dokument Certification Practice Statements des Zertifikatsdienstes DRV QC Root CA [8] definiert.

Die Analyse und die Bewertung von betrieblichen Sicherheitsrisiken sowie die Definitionen von Maßnahmen zur Risikominimierung sind Gegenstand des Sicherheitskonzeptes.

Die Vorgaben zum Betrieb des Zeitstempeldienstes DRV QC Root TSA aus Sicht IT-Sicherheit sind im Sicherheitskonzept des Zeitstempeldienstes DRV QC Root TSA definiert. Die entsprechenden Vorgaben zur Erstellung und Verwaltung des Schlüsselmateri als und des Public Key Zertifikates des Zeitstempeldienstes DRV QC Root TSA sind im Sicherheitskonzept des Zertifikatsdienstes DRV QC Root CA definiert. Diese Dokumente sind als vertraulich eingestuft und nicht öffentlich verfügbar.

Der VDA DRV Bund führt ein Verzeichnis der aktuellen Konfiguration der technischen Systeme (Asset Management):

- Die eingesetzten technischen Systeme inkl. Software und Hardware Komponenten werden mit einer Asset Management Software dokumentiert.

Die Maßnahmen im Sicherheitsmanagement sind detailliert im Sicherheitskonzept [9] festgelegt. Das Sicherheitskonzept muss regelmäßig auf Aktualität geprüft werden.

6.7 Sicherheitsmaßnahmen für das Netzwerk

Die Sicherheitsmaßnahmen werden detailliert im Dokument Certification Practice Statements des Zertifikatsdienstes DRV QC Root CA [8] definiert.

6.8 Zeitstempel

Jedes technische System synchronisiert seine Systemzeit auf geeignete Weise.

Die Server für den Validierungsdienst (OCSP-Responder) und den qualifizierten Zeitstempeldienst werden einmal täglich durch den Zeitstempeldienst DRV QC Root TSA mit dem deutschen Zeitsignal-Sender DCF77 synchronisiert. Die Zeit von DCF77 basiert auf dem deutschen UTC Labor UTC(PTB) bei der Physikalisch Technischen Bundesanstalt.

Alle anderen Server im Trustcenter der DRV werden mit dem NTP-Server der DRV Bund synchronisiert.

7.1 Zertifikatsprofil

7.2 Sperrlistenprofil

7.3 OSCP Profil

7.4 TSA Profil

Tabelle 3: Signaturalgorithmus für qualifizierte Zeitstempel

7.4.2 TSA Policy

Die OID der BTSP lautet:

```
0.4.0.2023.1.1
itu-t(0)
identified-organization(4)
etsi(0)
time-stamp-policy(2023)
policy-identifiers(1)
best-practices-ts-policy(1)
```

8 Konformitätsprüfung (Compliance Audit, Assessments)

8.1 Häufigkeit und Umstände der Überprüfung

Die vollständige Konformitätsprüfung erfolgt regulär alle zwei Jahre gemäß Artikel 20 eIDAS-VO [1].

Nach einem Jahr ist ein Wiederholungsaudit vorgesehen. Schwerpunkte sind dabei die gefundenen Schwachstellen des letzten kompletten Audits.

Wenn größere Änderungen an den technischen Systemen oder den Prozessabläufen durchgeführt werden, ist eine Meldung an die Konformitätsbewertungsstelle erforderlich. Nach Abstimmung mit dieser kann eine außerordentliche Konformitätsbewertung erforderlich werden.

8.2 Identität und Qualifikation des Überprüfers

Die Konformitätsbewertung wird durch eine Konformitätsbewertungsstelle durchgeführt, welche durch die nationale Aufsichtsstelle gemäß Artikel 17 eIDAS-VO [1] mit der Konformitätsbewertung beauftragt ist.

8.3 Verhältnis von Prüfer zu Überprüftem

Es gibt außerhalb der Konformitätsbewertung keine geschäftlichen Bindungen zwischen dem VDA DRV Bund und der Konformitätsbewertungsstelle.

8.4 Überprüfte Bereiche

Die Konformitätsbewertung erfolgt für die produktiven Haupt- und Backup-Systeme des Zeitstempeldienstes DRV QC Root TSA.

8.5 Mängelbeseitigung

Die Mitarbeiter des VDA DRV Bund beheben die während der Konformitätsbewertung gefunden Mängel nach Vorgaben der Konformitätsbewertungsstelle.

8.6 Veröffentlichung der Ergebnisse

Das Zertifikat der Konformitätsbewertung wird durch die Konformitätsbewertungsstelle veröffentlicht [14].

9 Weitere geschäftliche und rechtliche Angelegenheiten

9.1 Gebühren

9.1.1 Gebühren für Zertifikatserstellung oder -erneuerung

Die Gebühren werden in der Verwaltungsvereinbarung mit der nutzenden Institution geregelt.

9.1.2 Gebühren für Zugriff auf Zertifikate

Die Gebühren werden in der Verwaltungsvereinbarung mit der nutzenden Institution geregelt.

9.1.3 Gebühren für Sperrung oder Statusabfragen

Die Gebühren werden in der Verwaltungsvereinbarung mit der nutzenden Institution geregelt.

9.1.4 Andere Gebühren

Keine Angaben.

9.1.5 Gebührenerstattung

Keine Angaben.

9.2 Finanzielle Verantwortung

9.2.1 Deckungsvorsorge

Die Deutsche Rentenversicherung Bund verfügt über die notwendige Deckungsvorsorge gemäß Artikel 24 eIDAS-VO [1] für den Zeitstempeldienst DRV QC Root TSA für Schäden gemäß Artikel 13 eIDAS-VO.

9.2.2 Weitere Vermögenswerte

Die Systeme des Zeitstempeldienstes DRV QC Root TSA werden durch die DRV Bund bereitgestellt.

9.2.3 Versicherung oder Garantie für Endteilnehmer

Keine Angaben.

9.3 Vertraulichkeit von Geschäftsinformationen

9.3.1 Vertraulich zu behandelnde Daten

Die Informationen im Sicherheitskonzept (Risikoanalyse, Sicherheitsmaßnahmen) sind als vertraulich und die Festlegungen zum Betrieb des Zeitstempeldienstes DRV QC Root TSA (Certification Practice Statements [8], Betriebskonzept, etc.) sind als "Nur für den Dienstgebrauch" eingestuft.

9.3.2 Nicht vertraulich zu behandelnde Daten

Keine Angaben.

9.3.3 Verantwortung zum Schutz vertraulicher Informationen

Die Verantwortung zum Schutz vertraulicher Informationen tragen die Systemverwalter und Mitarbeiter des VDA DRV Bund, welche diese Daten erstellen, nutzen und speichern.

9.4 Schutz personenbezogener Daten

9.4.1 Richtlinie zur Verarbeitung personenbezogener Daten

Der Zeitstempeldienst DRV QC Root TSA erfasst keine personenbezogenen Daten bei der Erstellung von Zeitstempeln. Der elektronische Antrag an den Zeitstempeldienst beinhaltet keine personen-bezogenen Daten. Die resultierende elektronische Antwort des Zeitstempeldienstes beinhaltet neben dem Zeitstempel auch die Zertifikatskette des ausstellenden Zeitstempels.

9.4.2 Vertraulich zu behandelnde Daten

Die Identifikationsdaten der Benutzer des Zeitstempeldienstes DRV QC Root TSA sind vertraulich zu behandeln.

9.4.3 Nicht vertraulich zu behandelnde Daten

Keine Angaben.

9.4.4 Verantwortung zum Schutz personenbezogener Daten

Die Verantwortung zum Schutz vertraulicher Informationen tragen die Systemverwalter und Mitarbeiter des VDA DRV Bund, welche diese Daten erfassen, verarbeiten und speichern.

9.4.5 Einwilligung und Nutzung personenbezogener Daten

Die Benutzer des Zeitstempeldienstes DRV QC Root TSA stimmen in einer Verwaltungsvereinbarung zu, dass für ihre Institution ein Organisationszertifikat erstellt und dass dieses Zertifikat zu Auswertungszwecken durch den Zeitstempeldienst gespeichert werden darf.

9.4.6 Offenlegung bei gerichtlicher Anordnung oder im Rahmen gerichtlicher Beweisführung

Nicht relevant.

9.4.7 Andere Umstände einer Veröffentlichung

Keine Angaben.

9.5 Urheberrechte

Keine Angaben.

9.6 Pflichten

9.6.1 Pflichten des VDA

Die Pflichten des VDA DRV Bund sind in der Certificate Policy des Zertifikatsdienstes DRV QC Root CA festgelegt [7].

9.6.2 Pflichten des Zeitstempeldienstes

Die Pflichten des Zeitstempeldienstes DRV QC Root TSA sind in der als Voraussetzung zur Nutzung des Zeitstempeldienstes abzuschließenden Verwaltungsvereinbarung geregelt.

9.6.3 Pflichten des Benutzers

Die Pflichten der Benutzer des Zeitstempeldienstes DRV QC Root TSA im Sinne von Abschnitt 1.3.3 sind in der als Voraussetzung zur Nutzung des Zeitstempeldienstes abzuschließenden Verwaltungsvereinbarung geregelt.

9.6.4 Pflichten der vertrauenden Partei (Relying Parties)

Parteien, die einem vom Trustcenter der DRV herausgegebenen Zeitstempel vertrauen wollen, sind verpflichtet, die Signatur und den Zertifikatsstatus des Zeitstempeldienstes DRV QC Root TSA gemäß den Vorgaben in der Certificate Policy des Zertifikatsdienstes DRV QC Root CA [7] zu prüfen.

9.6.5 Pflichten anderer Teilnehmer

Keine Angaben

9.7 Haftung

Der VDA DRV Bund haftet nach den allgemeinen gesetzlichen Vorgaben. Für die qualifizierten Signaturzertifikate des Zeitstempeldienstes DRV QC Root TSA gelten die Haftungsregelungen gemäß Certificate Policy des Zertifikatsdienstes DRV QC Root CA [7].

9.8 Haftungsbeschränkung

Haftung besteht nur im Rahmen der gesetzlichen Vorgaben.

9.9 Haftungsfreistellung

Keine Angaben.

9.10 Inkrafttreten und Aufhebung

9.10.1 Inkrafttreten

Dieses Dokument ist vom Tage seiner Veröffentlichung an gültig. Seine Gültigkeit endet mit der Einstellung des Zeitstempeldienstes DRV QC Root TSA.

9.10.2 Aufhebung

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

9.10.3 Konsequenzen der Aufhebung

Wenn dieses Dokument ungültig wird, dann dürfen keine qualifizierten Zeitstempel mehr nach dieser Richtlinie erstellt werden.

9.11 Individuelle Benachrichtigungen und Kommunikation mit Teilnehmern

Die Veröffentlichung dieser Richtlinie erfolgt auf der Web-Seite der DRV Bund (Siehe 2.2). Eine individuelle Benachrichtigung der Benutzer des Zeitstempeldienstes DRV QC Root TSA erfolgt gemäß den Festlegungen in der Verwaltungsvereinbarung.

9.12 Änderungen der Richtlinie

9.12.1 Vorgehen bei Änderungen

Der VDA DRV Bund behält sich die Änderung dieses Dokuments vor. Diese kann insbesondere durch eine Weiterentwicklung der technischen oder rechtlichen Gegebenheiten erforderlich sein.

Bei Ergänzungen oder Modifikationen entscheidet der VDA DRV Bund, ob sich daraus signifikante Änderungen der Sicherheit des Zeitstempeldienstes DRV QC Root TSA, des Vertrauens, welches den Zeitstempel entgegengebracht werden kann, der Rechte und Pflichten der Teilnehmer oder der Anwendbarkeit der Zeitstempel ergeben. Falls dies der Fall ist, wird die Versionsnummer auf die nächste volle Nummer erhöht.

9.12.2 Benachrichtigungsmechanismus und Fristen

Sollten die Änderungen sicherheitsrelevante Aspekte oder die Verfahren hinsichtlich der Zeitstempelnutzer betreffen, wie beispielsweise Änderungen des Ablaufs, des Validierungsdienstes, der Kontaktinformationen oder der Haftung, wird der VDA DRV Bund die Nutzer des Zeitstempeldienstes in geeigneter Weise benachrichtigen.

Hinsichtlich übriger Änderungen, insbesondere der Verbesserung geringfügiger redaktioneller Versehen oder der Beifügung von Erläuterungen, kann eine Benachrichtigung der Nutzer des Zeitstempeldienstes unterbleiben.

Die jeweils aktuelle Schriftversion dieses Textes ersetzt sämtliche vorhergehende Versionen. Mündliche Kundmachungen erfolgen nicht.

9.12.3 Umstände, die eine Änderung des Richtlinienbezeichners (OID) erfordern

Eine Änderung der Richtlinien-OID ist dann erforderlich, wenn sich der Umfang der beinhalteten Vertrauensdienste ändert.

9.13 Konfliktbeilegung

Für die Prüfung von Beschwerden und die Beilegung von Meinungsverschiedenheiten ist die Schiedsstelle des Trustcenters der Deutschen Rentenversicherung zuständig.

Die Schiedsstelle ist erreichbar unter

E-Mail	Trustcenter-gRV@drv-bund.de
Postadresse	Deutsche Rentenversicherung Bund 1170-05 Trustcenter / Schiedsstelle D-10704 Berlin

9.14 Geltendes Recht

Es gilt grundsätzlich deutsches Recht, mit Ausnahme der eIDAS-VO, welche als Europäischer Rechtsakt unmittelbare Wirkung entfaltet und Anwendungsvorrang vor den nationalen Regelungen genießt.

9.15 Konformität mit geltendem Recht

Der Zeitstempeldienst DRV QC Root TSA arbeitet als Vertrauensdienst zur Erstellung qualifizierter Zeitstempel konform zu Artikel 42 eIDAS-VO [1] und den relevanten ETSI-Normen [4], [5] und [6]

9.16 Weitere Regelungen

9.16.1 Vollständigkeit

Keine Angaben.

9.16.2 Abtretung der Rechte

Keine Angaben.

9.16.3 Salvatorische Klausel

Sollten einzelne Bestimmungen dieses Dokumentes unwirksam oder undurchführbar sein, bleibt davon die Wirksamkeit des restlichen Dokumentes unberührt.

9.16.4 Rechtliche Auseinandersetzungen / Erfüllungsort

Der Gerichtsstand ergibt sich aus dem Gesetz.

9.16.5 Force Majeure

Keine Angaben.

9.17 Andere Regelungen

Keine Angaben.

10 Abkürzungen und Begriffe

10.1 Abkürzungen

AD	Auskunftsdienst (OCSP-Statusauskünfte)
APC	Arbeitsplatz-PC
BDSG	Bundesdatenschutzgesetz
BNetzA	Bundesnetzagentur
BSI	Bundesamt für Sicherheit in der Informationstechnik
C	Country
CA	Certification Authority
CAB	Conformity Assessment Body (Konformitätsbewertungsstelle)
CAR	Conformity Assessment Report (Konformitätsbewertungsbericht)
CC	Common Criteria (ISO/IEC 15408)
CERTSN	Zertifikatsseriennummer
CK	Chipkarte
CN	Common Name
CP	Certificate Policy
CPS	Certification Practice Statements
CRL	Certificate Revocation List (Sperrliste)
DMS	Document Management System
DN	Distinguished Name
DNS	Domain Name Service
DRV	Deutsche Rentenversicherung
DRV BB	Deutsche Rentenversicherung Berlin-Brandenburg
DRV RL	Deutsche Rentenversicherung Rheinland
DRV WF	Deutsche Rentenversicherung Westfalen
DSRV	Datenstelle der Träger der Rentenversicherung
EAL	Evaluation Assurance Level
EE	End Entity
eIDAS	Electronic Identification and Trust Services for Electronic Transactions in the European Market
eIDAS-VO	eIDAS-Verordnung
EN	European Norm
ES-CK	Einzelsignaturchipkarte
ETSI	European Telecommunications Standard Institute
EU	European Union
FQDN	Fully Qualified Domain Name

HSM	Hardware Security Module
HSM-SCK	HSM-Systemchipkarte
HTTP	Hyper Text Transfer Protocol
HW	Hardware
ID	Identifikation
IETF	Internet Engineering Task Force
IT	Information Technology (Informationstechnik)
ITSEC	Information Technology Security Evaluation Criteria
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MA	Mitarbeiter
MA-CK	Mitarbeiterchipkarte
MA-Tool	Mitarbeiter-Tool
MS-CK	Massensignaturchipkarte
NAB	National Accreditation Body (Nationale Akkreditierungsstelle)
Nonce	Number used once
NSB	National Supervisory Body (Nationale Aufsichtsstelle)
NTP	Network Time Protocol
O	Organization
OCSP	Online Certificate Status Protocol
OCSPR	OCSP-Responder (Software des AD)
OID	Object Identifier
OU	Organizational Unit
PBS	Produktiv Backup System
PC	Personal Computer
PEN	Private Enterprise Number
PHS	Produktiv Haupt System
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PN	Pseudonym
PP	Protection Profile
PSE	Personal Security Environment
PTB	Physikalisch-technische Bundesanstalt Braunschweig
PUK	Personal Unblocking Key
QC	Qualified Certificate

QSCD	Qualifizierte elektronische Signaturerstellungseinheit (Qualified Signature Creation Device)
QTSP	Qualified Trust Service Provider (Qualifizierter Vertrauensdiensteanbieter)
RFC	Request for Comments - Internet Standards der IETF
RSA	Asymmetrischer Kryptografischer Algorithmus von Rivest, Shamir und Adleman
RV	Rentenversicherung
SHA	Secure Hash Algorithm
SigG	Signaturgesetz
SW	Software
SYS-CK	Systemchipkarte
TC	Trustcenter
TCDRV	Trustcenter der Deutschen Rentenversicherung
TSA	Time Stamp Authority (Zeitstempeldienst)
TSL	Trust Service Status List
TSP	Trust Service Provider
UHD	User Help Desk
URL	Unified Ressource Locator
UTC	Universal Time Coordinated
VD	Verzeichnisdienst (LDAP-Repository)
VDA	Vertrauensdiensteanbieter
VO	Verordnung
WAN	Wide Area Network
X.509	ITU-Standard für Zertifikate und Sperrlisten

10.2 Begriffe

Certificate Policy (CP)	Der Begriff „Certificate Policy“ steht für die Gesamtheit der Regeln und Vorgaben, welche die Anwendbarkeit eines Zertifikatstyps festlegen. Die Zielsetzung einer Certificate Policy ist im RFC 3647 ausführlich dargestellt. Insbesondere sollte eine Certificate Policy darlegen, • Welche Vorgaben zur Erstellung von Schlüsseln und Zertifikaten bzgl. Registrierung, Generierung und Veröffentlichung gelten, • Welche Vorgaben für die Anwendung der Zertifikate sowie der zugehörigen Schlüssel und Signaturerstellungseinheiten gelten, • Welche Bedeutung den Zertifikaten und ihrer Anwendung zukommt, das heißt welche Sicherheit, Beweiskraft, oder rechtliche Relevanz die mit ihnen erzeugten Signaturen besitzen.
Certification Practice Statements (CPS)	Nach RFC 3647 legt das „Certification Practice Statements“ (CPS) die Praktiken dar, die ein VDA bei der Erstellung und Management der Zertifikate anwendet. Das CPS Dokument macht Vorgaben bzgl. des Betriebes eines Zertifikatsdienstes. Das Dokument enthält keine Bestimmungen, die Rechte oder Pflichten von Personen begründen, ändern oder aufheben würden.
DCF77	Der Zeitzeichensender DCF77 der Bundesrepublik Deutschland wird in Mainflingen durch das PTB Braunschweig betrieben. Das PTB betreibt 4 hoch-präzise Cäsium-Uhren als Zeitnormal für die nationale Referenzzeit UTC(PTB). Die UTC(PTB) ist eine Quelle der Internationalen Atomzeit TAI des BIPM. Die bekannteste Zeitskala des BIPM ist die Weltzeit UTC.
EE-Zertifikat	Zertifikat für Endbenutzer (End Entity)
eIDAS-Verordnung	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
Mandant im Trustcenter der DRV	Als Mandanten werden die Träger der Deutschen Rentenversicherung bezeichnet, welche einen eigenen qualifizierten Zertifikatsdienst betreiben und damit als Vertrauensdiensteanbieter gemäß eIDAS-VO auftreten.
Qualifizierte EE-Zertifikate im Trustcenter der DRV	Qualifizierte Zertifikate für: • Mitarbeiter der DRV Rheinland bzw. DRV Westfalen auf MA-CK, • Mitarbeiter der DRV Bund auf ES-CK, • Mitarbeiter von RV-Trägern auf MS-CK.
Qualifizierte Systemzertifikate im Trustcenter der DRV	Qualifizierte Zertifikate für den Betrieb von: • Zertifikatsdienste DRV QC Root CA, DRV QC 70 MA CA, DRV QC 13 MA CA und DRV QC 11 MA CA, • Zeitstempeldienst DRV QC Root TSA, • Validierungsdienste DRV QC Root OCSP, DRV QC 70 MA OCSP, DRV QC 13 MA OCSP und DRV QC 11 MA OCSP
Qualifizierte Validierungsdienste der Mandanten im Trustcenter der DRV	Qualifizierter Vertrauensdienste: • DRV QC 70 MA OCSP • DRV QC 13 MA OCSP • DRV QC 11 MA OCSP

Qualifizierte Vertrauensdienste im Trustcenter der DRV	Qualifizierte Vertrauensdienste im Kontext des Trustcenters der DRV sind die elektronischen Dienste: • Zertifikatsdienst zur Ausstellung und Validierung qualifizierter elektronischer Zertifikate, • Zeitstempeldienst zur Erstellung qualifizierter elektronischer Zeitstempel.
Qualifizierte Zertifikatsdienste der Mandanten im Trustcenter der DRV	Qualifizierter Vertrauensdienste: • DRV QC 70 MA CA • DRV QC 13 MA CA • DRV QC 11 MA CA
Qualifizierter Vertrauensdiensteanbieter	Ein qualifizierter Vertrauensdiensteanbieter ist ein Vertrauensdiensteanbieter, der einen oder mehrere qualifizierte Vertrauensdienste erbringt und dem von der Aufsichtsstelle der Status eines qualifizierten Anbieters verliehen wurde.
Systemchipkarte	QSCD für qualifizierte Systemzertifikate
Validierungsdienst	Dienst zur Bereitstellung von Zertifikatsstatusauskünften auf Basis eines OCSP-Responder
Vertrauensdiensteanbieter	Ein Vertrauensdiensteanbieter ist eine natürliche oder juristische Person, die einen oder mehrere Vertrauensdienste als qualifizierter oder nichtqualifizierter Vertrauensdiensteanbieter erbringt.
Zeitstempeldienst DRV QC Root TSA	Qualifizierter Vertrauensdienst des VDA DRV Bund für die Ausstellung: • qualifizierter elektronischer Zeitstempel.
Zertifikatsdienst DRV QC 11 MA CA	Qualifizierter Vertrauensdienst des VDA DRV Westfalen für die Ausstellung: • qualifizierter EE-Zertifikate, • der Zertifikate des Validierungsdienstes DRV QC 11 MA OCSP.
Zertifikatsdienst DRV QC 13 MA CA	Qualifizierter Vertrauensdienst des VDA DRV Rheinland für die Ausstellung: • qualifizierter EE-Zertifikate, • der Zertifikate des Validierungsdienstes DRV QC 13 MA OCSP.
Zertifikatsdienst DRV QC 70 MA CA	Qualifizierter Vertrauensdienst des VDA DRV Bund für die Ausstellung: • qualifizierter EE-Zertifikaten, • der Zertifikate des Validierungsdienstes DRV QC 70 MA OCSP.
Zertifikatsdienst DRV QC Root CA	Qualifizierter Vertrauensdienst des VDA DRV Bund für die Ausstellung: • der Ausstellerzertifikate der Zertifikatsdienste DRV QC Root CA, DRV QC 70 MA CA, DRV QC 13 MA CA und DRV QC 11 MA CA, • der Zertifikate des Zeitstempeldienstes DRV QC Root TSA, • der Zertifikate des Validierungsdienstes DRV QC Root OCSP.

11 Informationen zum Dokument

11.1 Änderungsverzeichnis

Version	Datum	Kap.	Änderungsgrund	Bearbeiter
01.00.00	27.06.2006	Alle	Ersterstellung	DRV Bund
02.00.00	10.08.2007	Alle	Migration zu stärkeren kryptographischen Verfahren	DRV Bund
03.00.00	23.01.2007	Alle	Prüfung des Zeitstempel-Zertifikates über Sperrlisten entfällt	DRV Bund
04.00.00	12.05.2016	Alle	Anpassung gemäß den Standards ETSI EN 319401, ETSI EN 319421, Verordnung 910/2014 der EU (eIDAS-VO)	DRV Bund
04.01.00	03.06.2016	Alle	Aufbewahrungsfrist für Logdateien auf 5 Jahre festgelegt	Atos
04.02.00	30.09.2016	Alle	Schiedsstelle definiert	Atos
05.00.00	---	---	Version wird aus formalen Gründen übersprungen	---
06.00.00	21.04.2017	Alle	Anpassung an RFC3647	Atos

11.2 Abbildungsverzeichnis

Abbildung 1 Qualifizierte Vertrauensdienste im Trustcenter der DRV	4
Abbildung 2 Richtlinien Dokumente des Zeitstempeldienstes DRV QC Root TSA	5

11.3 Tabellenverzeichnis

Tabelle 1: Veröffentlichte Informationen	9
Tabelle 2: Zugangskontrolle zu Veröffentlichungspunkten	9
Tabelle 3: Signaturalgorithmus für qualifizierte Zeitstempel	21

11.4 Referenzen

- [1] eIDAS-VO: Verordnung Nr. 910/2014 der EU im Amtsblatt der Europäischen Union, L257/73; <http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A32014R0910>
- [2] RFC 3647: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework; Freigabe November 2003; <http://www.faqs.org/rfcs/rfc3647.html>
- [3] RFC 3161: Internet X.509 Public Key Infrastructure Time Stamp Protocol (TSP) <http://www.faqs.org/rfcs/rfc3161.html>
- [4] ETSI EN 319 401 V2.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers http://www.etsi.org/deliver/etsi_en/319400_319499/319401/
- [5] ETSI EN 319421: Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps http://www.etsi.org/deliver/etsi_en/319400_319499/319421/
- [6] ETSI EN 319422: Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles http://www.etsi.org/deliver/etsi_en/319400_319499/319422/
- [7] Certificate Policy des Zertifikatsdienstes DRV QC Root CA <http://www.deutsche-rentenversicherung-bund.de/static/trustcenter/policy.html>
- [8] Certification Practice Statements des Zertifikatsdienstes DRV QC Root CA
- [9] Sicherheitskonzept des VDA DRV Bund
- [10] Beendigungsplan des Trustcenters der Deutschen Rentenversicherung
- [11] Web-Seite des VDA Deutsche Rentenversicherung Bund <http://www.deutsche-rentenversicherung-bund.de/static/trustcenter/policy.html>
- [12] Web-Seite der Bundesnetzagentur zur Veröffentlichung geeigneter Algorithmen https://www.bundesnetzagentur.de/cln_1412/DE/Service-Funktionen/ElektronischeVertrauensdienste/QES/WelcheAufgabenhatdieBundesnetzagentur/GeeigneteAlgorithmenfestlegen/geeignetealgorithmenfestlegen_node.html
- [13] Web-Seite der Bundesnetzagentur zur Veröffentlichung der nationalen Vertrauensliste; <https://www.nrca-ds.de>
- [14] Web-Seite des TÜVIT zur Veröffentlichung von Konformitätsbewertungen für Vertrauensdiensteanbieter; <https://www.tuvit.de/de/zertifikate-1265-4512.htm>
- [15] Physikalisch Technische Bundesanstalt, Arbeitsgruppe 4.41 Schaltsekunden, <https://www.ptb.de/cms/de/ptb/fachabteilungen/abt4/fb-44/ag-441/darstellung-der-gesetzlichen-zeit/schaltsekunden.html>
- [16] Physikalisch Technische Bundesanstalt, Arbeitsgruppe 4.42 Zeitübertragung, <https://www.ptb.de/cms/ptb/fachabteilungen/abt4/fb-44/ag-442.html>