Trustcenter der
Deutschen Rentenversicherung

Policy des qualifizierten Zeitstempeldienstes des Trustcenters der Deutschen Rentenversicherung

Version: 04.00

Stand: 12.05.16

Inhalt

1 Policy des qualifizierten Zeitstempeldienstes des Trustcenters der Deutschen Rentenversicherung

1.1 Einleitung

1.1.1 Überblick

Die Träger der Deutschen Rentenversicherung betreiben das Trustcenter der Deutschen Rentenversicherung bis 30.06.2016 gemäß deutschem Signaturgesetz und ab 01.07.2016 gemäß eIDAS-Verordnung [1].

Zu den Leistungen des Trustcenters der Deutschen Rentenversicherung gehört u.a. ein qualifizierter Zeitstempeldienst, der qualifizierte Zeitstempel gemäß Artikel 42 der eIDAS-Verordnung ausstellt.

Das vorliegende Dokument beinhaltet die "Policy des qualifizierten Zeitstempeldienstes des Trustcenters der Deutschen Rentenversicherung". In Kapitel 1 werden die erforderlichen Angaben für ein "TSA Disclosure Statement" gemacht. Ein separates Dokument "TSA Disclosure Statement" wird nicht erstellt.

Diese Policy berücksichtigt die Standards:

- "ETSI EN 319 401" [2] und
- "ETSI EN 319 421" [3]

in der derzeit aktuellen Version des European Telecommunications Standards Institute (ETSI). Das Verhältnis dieser Policy zu den genannten Standards wird in Kapitel 2 erläutert.

1.1.2 Dokumentenidentifikation

Dokumentname	Policy des qualifizierten Zeitstempeldienstes des Trustcenters der Deutschen Rentenversicherung
Version	04.00
OID	1.3.6.1.4.1.22204.1.8.1.1.3

1.1.3 Organisation für die Verwaltung dieses Dokuments

Für die Verwaltung dieser Policy ist die Deutsche Rentenversicherung Bund zuständig.

1.1.4 Kontaktperson

Folgende Ansprechwege hinsichtlich dieser Policy bestehen:

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

1.2 Rechtliche Anforderungen der eIDAS-Verordnung

1.2.1 Artikel 42: Anforderungen an qualifizierte elektronische Zeitstempel

Der qualifizierte Zeitstempeldienst erfüllt die Anforderungen der eIDAS-Verordnung:

- Der qualifizierte Zeitstempel wird mit den gelieferten Daten durch eine qualifizierte elektronische Signatur verbunden. Ein unbemerktes Verändern der verbundenen Daten ist nach heutigem Ermessen ausgeschlossen.
- Der Zeitstempel wird mittels Funkuhr vom Zeitzeichensender DCF77 abgeleitet. Die Genauigkeit des Zeitstempels ist kleiner 1s.
- Die qualifizierte elektronische Signatur wird durch eine geprüfte (Common Criteria Level EAL4+) und bestätigte Signaturerstellungseinheit erstellt. Für den Zeitstempeldienst gibt es je Signaturerstellungseinheit ein qualifiziertes Zertifikat, das vom qualifizierten Wurzelzertifizierungsdienst des Trustcenters der Deutschen Rentenversicherung ausgestellt wird.

1.2.2 Anhang I: Anforderungen an qualifizierte Zertifikate für elektronische Signaturen

Der qualifizierte Zeitstempeldienst erstellt elektronische Zeitstempel, in dem die übergebenen Daten im Format eines Hashwertes zusammen mit einem Zeitstempel qualifiziert elektronisch signiert werden. Die Anforderungen an das qualifizierte Zertifikat des Zeitstempeldienstes werden erfüllt, das Zertifikat beinhaltet u.a.:

- ein QC Statement gemäß [5] geeignet zur maschinellen Prüfung,
- den Namen der qualifizierten Zertifizierungsstelle des Trustcenters der Deutschen Rentenversicherung als Herausgeber,
- den öffentlichen Schlüssel des qualifizierten Zeitstempeldienstes, der zur Validierung signierter Zeitstempel-Antworten erforderlich ist,
- Angaben zur Gültigkeit des Zertifikates,
- die Seriennummer des Zertifikates als eindeutiges Identifikationsmerkmal,
- die URL, von der das Zertifikat des Herausgebers geladen werden kann,
- die URL des OCSP-Responder, der zur Zertifikatsstatusprüfung genutzt werden soll,
- die Nutzung einer qualifizierten Signaturerstellungseinheit wird implizit durch das QC Statement angegeben,
- eine qualifizierte elektronische Signatur.

1.2.3 Anhang II: Anforderungen an qualifizierte elektronische Signaturerstellungseinheiten

Der qualifizierte Zeitstempeldienst erstellt elektronische Zeitstempel, in dem die übergebenen Daten im Format eines Hashwertes zusammen mit einem Zeitstempel qualifiziert elektronisch signiert werden. Die Anforderungen an die genutzte qualifizierte Signaturerstellungseinheit werden erfüllt:

- Vertraulichkeit: Der Signaturschlüssel wird in einer Chipkarte als sichere Signaturerstellungseinheit erstellt und kann nicht exportiert werden,

- Einmaligkeit: Der Signaturschlüssel wird in der Chipkarte 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 den Signaturschlüssel wird ein RSA 2048 Bit Schlüsselpaar benutzt. Gemäß dem gültigen Algorithmen-Katalog [9] ist die Nichtableitbarkeit für die nächsten 7 Jahre gegeben.
- Zweckbindung: Der Signaturschlüssel steht nur dem qualifizierten Zeitstempeldienst zur Verfügung. Des Weiteren ist die Zweckbindung im qualifizierten Zertifikat angegeben.
- Die zum Erstellen des Zeitstempels übergebenen Daten werden durch die Signaturerstellungseinheit nicht geändert. Eine Anzeige dieser Daten ist nicht relevant.
- Die Signaturerstellungseinheiten für den Zeitstempeldienst werden von der qualifizierten Wurzelzertifizierungsstelle der Deutschen Rentenversicherung erstellt und verwaltet.
- Die Signaturschlüssel werden nicht gesichert oder archiviert. Dies ist mit den eingesetzten Chipkarten technisch nicht möglich.

1.3 Teilnehmer und Instanzen

1.3.1 Trustcenter der Deutschen Rentenversicherung

Die Träger der Deutschen Rentenversicherung betreiben das Trustcenter der Deutschen Rentenversicherung bis 30.06.2016 gemäß deutschem Signaturgesetz und ab 01.07.2016 gemäß eIDAS-Verordnung [1].

Zu den Leistungen des Trustcenters der Deutschen Rentenversicherung gehört u.a. ein qualifizierter Zeitstempeldienst, der qualifizierte Zeitstempel gemäß Artikel 42 der eIDAS-Verordnung ausstellt.

Das Trustcenter der Deutschen Rentenversicherung betreibt des Weiteren eine qualifizierte Wurzelzertifizierungsstelle, welche u.a. qualifizierte Zertifikate für den qualifizierten Zeitstempeldienst ausstellt.

Das Trustcenter der Deutschen Rentenversicherung betreibt weiterhin eine fortgeschrittene Wurzelzertifizierungsstelle und darunter mehrere fortgeschrittene Zertifizierungsstellen zur Erstellung von Authentisierungs- und Verschlüsselungs-Zertifikaten. Im Zusammenhang mit dem qualifizierten Zeitstempeldienst erstellt eine fortgeschrittene Zertifizierungsstelle Authentisierungs-Zertifikate für die Benutzer des qualifizierten Zeitstempeldienstes.

1.3.2 Qualifizierter Zeitstempeldienst

Das Trustcenter der Deutsche Rentenversicherung betreibt als Vertrauensdiensteanbieter einen qualifizierten Zeitstempeldienst gemäß eIDAS-Verordnung Artikel 42

1.3.3 Benutzer

Benutzer des qualifizierten Zeitstempeldienstes sind solche Personen und Systeme, die qualifizierte Zeitstempel vom Zeitstempeldienst anfordern können. Der Kreis der Benutzer ist auf Rentenversicherungsträger, Sozialversicherungsträger und andere öffentlich-rechtliche Institutionen der Bundesrepublik Deutschland beschränkt und wird durch die Deutsche Rentenversicherung Bund verwaltet. Die Benutzung des Zeitstempeldienstes erfolgt auf der Grundlage einer Verwaltungsvereinbarung zwischen dem Trustcenter der Deutschen Rentenversicherung und den nutzenden Institutionen.

1.3.4 Vertrauende Parteien

Der Kreis der vertrauenden Parteien ist nicht beschränkt.

1.4 Anwendbarkeit des Zeitstempeldienstes

1.4.1 Typen von Zeitstempeln und ihre Nutzung

Der qualifizierte Zeitstempeldienst des Trustcenters der Deutschen Rentenversicherung erstellt qualifizierte Zeitstempel gemäß eIDAS-Verordnung Artikel 42.

Qualifizierte Zeitstempel können nur von Personen bzw. Systemen angefordert werden, die über ein Authentifizierungszertifikat vom Trustcenter der Deutschen Rentenversicherung verfügen. Dieses Authentisierungszertifikat wird im qualifizierten Zeitstempeldienst hinterlegt und als berechtigt konfiguriert. Ein solches Authentisierungszertifikat erhalten die in Abschnitt 1.3.3 genannten Benutzer nach Abschluss der dort erwähnten Verwaltungsvereinbarung des Trustcenters der Deutschen Rentenversicherung. Die Authentifizierung des Benutzers erfolgt bei Anforderung eines Zeitstempels über einen TLS-Proxy-Server mit Client-Authentisierung.

Der qualifizierte Zeitstempeldienst nutzt zur Erstellung von Zeitstempeln 1 bis N Signaturchipkarten. Jede dieser Signaturchipkarten beinhaltet einen individuellen Signaturschlüssel, für jeden Signaturschlüssel gibt es ein qualifiziertes Zertifikat mit dem entsprechenden Signaturprüfschlüssel. Die erzeugten qualifizierten Zeitstempel sind mit dem Signaturprüfschlüssel des bei Erstellung des Zeitstempels gültigen Zertifikates des Zeitstempeldienstes verifizierbar.

Zertifikate des qualifizierten Zeitstempeldienstes werden von der qualifizierten Wurzelzertifizierungsstelle des Trustcenters der der Deutschen Rentenversicherung ausgestellt. Sie beinhalten alle den gleichen Namen als Zertifikatsinhaber und unterscheiden sich in der Zertifikatsseriennummer.

- Aussteller [Stand Mai 2016]:
  OU=QC Root CA, O=Deutsche Rentenversicherung, C=DE
- Inhaber [Stand Mai 2016]:
  CN=QC Root TSP, OU=QC Root CA, O=Deutsche Rentenversicherung, C=DE

Das Zertifikat der ausstellenden CA ist über den Verzeichnisdienst des Trustcenters der Deutschen Rentenversicherung abrufbar und auf Anforderung auch in der Antwort des Zeitstempeldienstes enthalten. Die Prüfung des Zertifikats hat gemäß den Vorgaben in der zugehörigen Policy zu erfolgen [6].

Von berechtigten Personen und Systemen können Zeitstempel von der Adresse

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

angefordert werden. Das Format der Anfrage sowie der Antwort sind konform zu den Standards RFC 3161 [7] und ETSI 319422 [4]. Unterstützte Hash-Algorithmen für die gelieferten Daten sind SHA-256 und SHA-512.

Die Lebensdauer der qualifizierten Zeitstempel ist grundsätzlich nicht begrenzt. Die Protokolldaten über ausgestellte Zeitstempel werden zum Schutz gegen Kompromittierung von Zeitstempelsignaturschlüsseln für 5 Jahre aufbewahrt. Nach Ablauf dieser 5 Jahre ist der verwendete Zeitstempelsignaturschlüssel nicht mehr in Verwendung und vernichtet, und kann daher nicht mehr kompromittiert werden. Das Trustcenter der Deutschen Rentenversicherung gewährleistet eine Überprüfbarkeit der Signatur des Zeitstempels für mindestens 30 Jahre nach Ablauf der Gültigkeit des zur Prüfung zu verwendenden Zertifikats.

1.4.2 Genauigkeit der Zeitstempel, Protokollierung

Der Zeitstempeldienst stellt die Zeitstempel mit der gesetzlichen deutschen Zeit mit einer Genauigkeit von einer Sekunde aus. Die Synchronisation der Uhr des Zeitstempeldienstes mit der gesetzlichen deutschen Zeit erfolgt einmal alle zwölf Stunden, die Genauigkeitsüberprüfung gegen die gesetzliche Zeit erfolgt alle 10 Sekunden.

Bei Feststellung einer Gangabweichung größer als eine Sekunde stellt der Zeitstempeldienst seinen Dienst automatisch ein. Als Quelle der gesetzlichen Zeit dient ein DCF77-Funkempfänger für das Zeitsignal des Zeitzeichensender DCF77 in Mainflingen der Physikalisch-Technischen Bundesanstalt Braunschweig.

Der Zeitstempeldienst protokolliert alle erstellten Zeitstempel in einer Logdatei. Die Logdatei ist in die tägliche Datensicherung einbezogen. Die Log-Daten werden 5 Jahre lang aufbewahrt.

1.4.3 Zertifizierungen

Die Zeitstempel werden von einer geprüften und bestätigten sicheren Softwarekomponente, dem TSP-Responder, erzeugt.

Die Systemchipkarte des TSP-Responder ist eine geprüfte (Common Criteria Level EAL4+) und bestätigte sichere Signaturerstellungseinheit, welche in der sicheren Umgebung der Wurzelzertifizierungsstelle personalisiert und betrieben wird.

Das Trustcenter der Deutschen Rentenversicherung betreibt den qualifizierten Zeitstempeldienst gemäß eIDAS-Verordnung Artikel 42. Der betrieb des qualifizierten Zeitstempeldienstes ist der zuständigen Aufsichtsstelle gemäß eIDAS-Verordnung Artikel 17 angezeigt.

1.5 Rechte und Pflichten

1.5.1 Pflichten der Benutzer des Zeitstempeldienstes

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

1.5.2 Pflichten der auf Zeitstempeln vertrauenden Parteien

Parteien, die einem vom Trustcenter der Deutschen Rentenversicherung herausgegebenen Zeitstempel vertrauen wollen, sind verpflichtet, die Signatur und den Zertifikatsstatus des Zeitstempeldienstes aktuell gemäß den Vorgaben in [6] zu prüfen.

1.5.3 Haftung des Zeitstempeldienstbetreibers

Das Trustcenter der Deutschen Rentenversicherung haftet nach den allgemeinen gesetzlichen Vorgaben. Für die qualifizierten Signaturzertifikate des Zeitstempeldienstes gelten die Haftungsregelungen gemäß [6].

1.5.4 Datenschutz

Der qualifizierte Zeitstempeldienst erfasst keine personenbezogenen Daten bei der Erstellung von Zeitstempeln. Der Antrag an den qualifizierten Zeitstempeldienst beinhaltet keine personen-bezogenen Daten. Die resultierende Antwort des qualifizierten Zeitstempeldienstes beinhaltet neben dem Zeitstempel auch die Zertifikatskette des ausstellenden Zeitstempels. Diese Zertifikate beinhalten ein Pseudonym für den Inhaber des qualifizierten Zertifikates. Das Zertifikat der qualifizierten Wurzelzertifizierungsstelle ist im Internet auf der Web-Seite des Trustcenter der Deutschen Rentenversicherung Bund veröffentlicht [8].

Die erstellten Zeitstempel werden zur Beweissicherung für 5 Jahre archiviert.

Die Benutzer des qualifizierten Zeitstempeldienstes authentisieren sich an einem vor den qualifizierten Zeitstempeldienst geschalteten TLS-Proxy mittels TLS-Client-Authentisierung. Die Client-Zertifikate zur Authentisierung beinhalten den Organisationsnamen des Anwenders. Diese Zertifikate werden zu Protokollierungs-, Abrechnungs- und Nachweiszwecken gespeichert und nach 5 Jahren gelöscht.

1.5.5 Anwendbares Recht

Es gilt deutsches Recht. Der Gerichtsstand ergibt sich aus dem Gesetz.

2 Referenz zu ETSI EN 319 401 / ETSI EN 319 421

Die vorliegende Policy des qualifizierten Zeitstempeldienstes des Trustcenters der Deutschen Rentenversicherung orientiert sich an den relevanten Normen und Standards:

- ETSI EN 319401: Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers [2]
- ETSI EN 319421: Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps [3]

In diesem Kapitel wird die Referenz dieser TSA Policy zu den Standards definiert. Der Standard ETSI EN 319401 definiert die generellen Anforderungen an die Policy eines Vertrauensdiensteanbieters. Für Vertrauensdiensteanbieter von Zeitstempeldiensten sind die Anforderungen im Standard ETSI EN 319421 detailliert beschrieben. Im Folgenden wird die Referenz zum letztgenannten Standard hergestellt.

2.1 Scope

Diese Policy ist gültig für den qualifizierten Zeitstempeldienst des Trustcenters der Deutschen Rentenversicherung. Wenn in den folgenden Kapiteln vom qualifizierten Zeitstempeldienst gesprochen wird, so ist damit der qualifizierte Zeitstempeldienst des Trustcenters der Deutschen Rentenversicherung gemeint.

2.2 Referenzen

Für das Verständnis dieser Policy sind die Referenzen in Kapitel 3.4 relevant.

2.3 Abkürzungen und Begriffe

Abkürzungen und Begriffe sind in Kapitel 3.2 und 3.3 definiert.

2.4 Konzept

2.4.1 Allgemeine Policy Anforderungen

Der qualifizierte Zeitstempeldienst erstellt qualifizierte Zeitstempel für berechtigte Benutzer von Rentenversicherungsträgern, Sozialversicherungsträgern und anderen öffentlich-rechtlichen Institutionen der Bundesrepublik Deutschland.

2.4.2 Funktionalität Zeitstempeldienst

Der qualifizierte Zeitstempeldienst ist logisch in Funktionsblöcke unterteilt, die für einzelne Aufgaben wie z.B. Monitoring der Signaturerstellungseinheiten, Zeitüberwachung, Zeitaktualisierung, Signaturerstellung zuständig sind. Aus Systemsicht handelt es sich um eine Softwarekomponente, die nicht geteilt werden kann.

2.4.3 Technik Zeitstempeldienst

Im Trustcenter der Deutschen Rentenversicherung wird ein qualifizierter Zeitstempeldienst betrieben. Zur Signaturerstellung nutzt dieser Dienst 1 bis N Signaturchipkarten als sichere Signaturerstellungseinheiten. Die verwendete Technik ist in Kapitel 1.4 beschrieben.

2.4.4 Benutzer Zeitstempeldienst

Die Benutzer des qualifizierten Zeitstempeldienstes sind in Kapitel 1.3 beschrieben.

2.4.5 Policy und Practice Statement

Die Policy des qualifizierten Zeitstempeldienstes ist Inhalt dieses Dokumentes.

Ein separates Dokument für "TSA Practice Statement" ist nicht vorgesehen. Die geforderten Dokumentationen und Regelungen sind im Betriebs- und Sicherheitskonzept des qualifizierten Zeitstempeldienstes bzw. der qualifizierten Wurzelzertifizierungsstelle des Trustcenters der Deutschen Rentenversicherung enthalten und vertraulich. Alle der Öffentlichkeit zugänglichen Informationen in Bezug auf den qualifizierten Zeitstempeldienst finden sich in dieser Policy bzw. in der Policy der qualifizierten Wurzelzertifizierungsstelle [6]. Nutzer des qualifizierten Zeitstempeldienstes im Sinne von Abschnitt 1.3 dieser Policy schließen darüber hinaus eine Verwaltungsvereinbarung mit dem Trustcenter der Deutschen Rentenversicherung ab, in der weitere, für diese Nutzer relevante Informationen enthalten sind.

2.5 Zeitstempeldienst Policy - Anforderungen

2.5.1 Generelle Policy Anforderungen

Der qualifizierte Zeitstempeldienst arbeitet gemäß der "Best Practices Time-Stamp Policy (BTSP)" für Zeitstempeldienste, welche Zeitstempel auf Basis von Public Key Zertifikaten mit einer Genauigkeit von 1s erstellen.

2.5.2 Identifikation der Policy

Der Identifier der "Best Practices Time-Stamp Policy (BTSP)" ist Bestandteil der TSP-Response, d.h. des erstellten Zeitstempels im ASN.1 Format.

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)
```

2.5.3 Benutzer des Zeitstempeldienstes

Der qualifizierte Zeitstempeldienst ist nicht öffentlich verfügbar, sondern ist bzgl. Erstellung von Zeitstempeln auf Benutzer einer öffentlich-rechtlichen Einrichtung der Bundesrepublik

Deutschland beschränkt (Siehe Kapitel 1.3). Die Validierung des Zertifikates des qualifizierten Zeitstempeldienstes ist öffentlich möglich.

2.6 Policy und Betriebsrichtlinien

2.6.1 Risikoeinschätzung

Die Erfassung und Bewertung von Risiken sowie die Ableitung von Maßnahmen zur Risikominimierung im Betrieb des qualifizierten Zeitstempeldienstes sind Gegenstand des Sicherheitskonzeptes des qualifizierten Zeitstempeldienstes bzw. der qualifizierten Wurzelzertifizierungsstelle des Trustcenters der Deutschen Rentenversicherung. Diese Dokumente sind als vertraulich eingestuft. Die Sicherheitskonzepte werden regelmäßig (i.d.R. jährlich) auf Aktualität geprüft und bei Bedarf angepasst.

2.6.2 TSA Practice Statement

In Kapitel 2.4.5 wird bereits darauf verwiesen, dass es kein weiteres Dokument "TSA Practice Statement" gibt. Die Vorgaben zum Betrieb des qualifizierten Zeitstempeldienstes sind im Sicherheitskonzept des qualifizierten Zeitstempeldienstes bzw. der qualifizierten Wurzelzertifizierungsstelle des Trustcenters der Deutschen Rentenversicherung enthalten und vertraulich.

2.6.3 Nutzungsbedingungen

Die allgemeinen Rechte und Pflichten bei der Nutzung des qualifizierten Zeitstempeldienstes sind im Kapitel 1.5 enthalten. Zusätzliche Angaben werden in den Nutzungsbedingungen mit dem Benutzer in einer Verwaltungsvereinbarung definiert (Siehe Kapitel 1.3.3).

2.6.4 Sicherheitskonzept

Die Vorgaben zum Betrieb des qualifizierten Zeitstempeldienstes aus Sicht IT Sicherheit sind im Sicherheitskonzept des qualifizierten Zeitstempeldienstes definiert. Die entsprechenden Vorgaben zur Erstellung und Verwaltung des Schlüsselmaterials und des Public Key Zertifikates des qualifizierten Zeitstempeldienstes sind im Sicherheitskonzept der qualifizierten Wurzelzertifizierungsstelle des Trustcenters der Deutschen Rentenversicherung definiert.

2.6.5 Pflichten des Zeitstempeldienstes

Es gelten die Festlegungen aus Kapitel 1.5.

2.6.6 Informationen für Dritte

Unter Dritte werden in diesem Zusammenhang die Anwender zusammengefasst, die einen erstellten Zeitstempel prüfen wollen.

Im Zeitstempel ist die Zertifikatskette des qualifizierten Zeitstempeldienstes enthalten. Das Zertifikat des qualifizierten Zeitstempeldienstes beinhaltet u.a. die URL des OCSP-Responder der qualifizierten Wurzelzertifizierungsstelle, über den der Sperrstatus dieses

Zertifikates geprüft werden kann. Das Zertifikat der qualifizierten Wurzelzertifizierungsstelle ist öffentlich auf der Web-Seite des Trustcenters der Deutschen Rentenversicherung Bund verfügbar [8].

2.7 Zeitstempeldienst Management

2.7.1 Einführung

Nicht relevant.

2.7.2 Organisation

Der qualifizierte Zeitstempeldienst wird durch die Deutsche Rentenversicherung Bund betrieben. Die Anforderungen an die Organisation sind im Sicherheitskonzept des qualifizierten Zeitstempeldienstes bzw. der qualifizierten Wurzelzertifizierungsstelle des Trustcenters der Deutschen Rentenversicherung beschrieben. Die konkrete Organisation ist im Organisationskonzept des Trustcenters der Deutschen Rentenversicherung definiert.

2.7.3 Personelle Sicherheit

Die Anforderungen an Mitarbeiter im Trustcenter der Deutschen Rentenversicherung sind im Sicherheitskonzept des qualifizierten Zeitstempeldienstes bzw. der qualifizierten Wurzelzertifizierungsstelle des Trustcenters der Deutschen Rentenversicherung beschrieben.

2.7.4 Asset Management

Das Management aller Ressourcen des qualifizierten Zeitstempeldienstes obliegt dem Betriebspersonal des Trustcenters der Deutschen Rentenversicherung Bund. Die entsprechenden Prozeduren zur Prüfung und im Notfall zur Wiederherstellung sind im Betriebskonzept beschrieben.

Im Betrieb des Zeitstempeldienstes entstehen Log-Dateien, die zur Beweissicherung der erstellten Zeitstempel für 5 Jahre archiviert werden (Siehe Kapitel 1.4.2). Die Prozedur zur Archivierung ist Gegenstand des Betriebskonzeptes.

2.7.5 Zugangskontrolle

Der qualifizierte Zeitstempeldienst wird auf dedizierten Servern betrieben. Diese Server sind im Datacenter des Trustcenters aufgebaut und mittels Firewall vom Netz der Deutschen Rentenversicherung bzw. vom Internet logisch getrennt.

Der Zugriff zum Erstellen von qualifizierten Zeitstempeln ist auf dedizierte Netzwerk-Zugänge beschränkt.

Der Zugriff zum Validieren eines qualifizierten Zertifikates des qualifizierten Zeitstempeldienstes erfolgt über den OCSP-Responder der qualifizierten Wurzelzertifizierungsstelle.

Das Management der Server des qualifizierten Zeitstempeldienstes erfolgt entweder lokal an der Konsole des Servers oder Remote mittels SSH. Die Anmeldung am System erfolgt mittels 2-Faktor-Authentisierung durch berechtigte Administratoren.

2.7.6 Kryptografische Verfahren

2.7.6.1 Allgemeines

Die regelmäßige Prüfung der eingesetzten kryptografischen Algorithmen liegt in der Verantwortung des Krypto-Managers des Trustcenters der Deutschen Rentenversicherung. Basis für die Prüfung ist die jährlich herausgegebene Liste der zugelassenen Krypto-Algorithmen, die auf der Web-Seite der Aufsichtsstelle gemäß eIDAS-Verordnung Art. 17 veröffentlicht wird (Siehe [9]).

2.7.6.2 Schlüsselgenerierung

Der Zeitstempeldienst nutzt zur Signaturerstellung für Zeitstempel 1 bis N Signaturerstellungseinheiten auf Basis von geprüften (Common Criteria Level EAL4+) Chipkarten. Die Schlüsselerstellung für diese Chipkarte erfolgt in der sicheren Umgebung des Trustcenters der Deutschen Rentenversicherung direkt auf der Chipkarte. Als Algorithmus kommt RSA 2048 Bit zum Einsatz.

2.7.6.3 Schutz des privaten Schlüssels

Der private Schlüssel kann von der Chipkarte nicht exportiert werden, ein Backup des privaten Schlüssels ist ausgeschlossen. Der Zufallsgenerator der eingesetzten Chipkarte sorgt dafür, dass generierte Schlüssel zufällig und damit weitest möglich einmalig sind.

Vor Nutzung des privaten Schlüssels muss die zugehörige PIN der Chipkarte eingegeben werden. Die Eingabe erfolgt beim Start des qualifizierten Zeitstempeldienstes durch Systemadministratoren.

2.7.6.4 Public Key Zertifikat

Die Public Key Zertifikate für den qualifizierten Zeitstempeldienst werden von der qualifizierten Wurzelzertifizierungsstelle des Trustcenters der Deutschen Rentenversicherung ausgestellt. Das Zertifikat der verwendeten qualifizierten Zeitstempeldienst-Einheit ist Bestandteil der Antwort des qualifizierten Zeitstempeldienstes. Zur Prüfung des Zertifikatsstatus ist der OCSP-Responder der qualifizierten Wurzelzertifizierungsstelle verfügbar.

2.7.6.5 Re-Keying

Die Nutzungsdauer von Schlüsselmaterial und Public Key Zertifikat des qualifizierten Zeitstempeldienstes richten sich nach den in der Bundesrepublik Deutschland zuständigen Vorgaben (Siehe Kapitel 2.7.6.1). Aktuell wird eine Nutzungsdauer von maximal 5 Jahren verwendet.

Ein Re-Keying, d.h. ein Ausstellen eines neuen Zertifikates für einen bereits verwendeten privaten Schlüssel, ist nicht vorgesehen.

2.7.6.6 Life Cycle Management

Die Chipkarten für die Signaturerstellung werden im Werkzustand vom Kartenlieferanten an das Trustcenter der Deutschen Rentenversicherung geliefert. Die Initialisierung dieser Chipkarten inkl. der Schlüsselgenerierung erfolgt in den Räumen und durch das Betriebspersonal des Trustcenters der Deutschen Rentenversicherung. Sollten die

Chipkarten etwas anderes als das Hersteller-Image beinhalten, so wird das von der Initialisierung erkannt und diese Karten werden nicht verwendet.

2.7.6.7 TSU Lebensende

Die Chipkarten zur Signaturerstellung des qualifizierten Zeitstempeldienstes können benutzt werden, bis (a) das zugehörige Zertifikat ungültig wird oder (b) neue Chipkarten im Rahmen eines Schlüsselwechsels erstellt worden sind.

Wenn Chipkarten des Zeitstempeldienstes nicht mehr verwendet werden, dann werden diese Chipkarten inkl. der auf ihnen enthaltenen Schlüssel physikalisch vernichtet.

2.7.7 Zeitstempel

2.7.7.1 Zeitstempelerstellung

Der qualifizierte Zeitstempeldienst erstellt Zeitstempel konform zur Norm ETSI EN 319422 [4]. Die verwendete Uhrzeit entspricht der amtlichen deutschen Zeit mit einer Genauigkeit von 1s (Siehe Kapitel 1.4.2).

2.7.7.2 Zeitsynchronisation

Die Zeitsynchronisation erfolgt auf Basis der amtlichen deutschen Zeit über den Zeitzeichensender DCF77 (Siehe Kapitel 1.4.2).

2.7.8 Physikalische Sicherheit

Die physikalische Sicherheit des qualifizierten Zeitstempeldiensts wird im Sicherheitskonzept des qualifizierten Zeitstempeldienstes betrachtet inkl. der Maßnahmen zur Restrisikominimierung.

2.7.9 Betriebssicherheit

Der qualifizierte Zeitstempeldienst basiert auf einem geprüften und bestätigten Produkt. Das Produkt wird maximal für den Zeitraum seiner Bestätigung eingesetzt. Änderungen an der Installation erfolgen (a) regulär vor Ablauf der Bestätigung durch ein Change-Request-Verfahren oder (b) als Patch im Rahmen eines Incidents. Durchgeführte Änderungen werden dokumentiert.

Patches und Updates werden nur nach vorheriger Prüfung im QS-System und Freigabe durch die Systemadministratoren im Produktivsystem eingespielt.

Die operativen und administrativen Prozesse sind im Betriebskonzept beschrieben.

Die Analyse und Bewertung von Sicherheitsrisiken sowie die Definitionen von Maßnahmen zur Risikominimierung ist Gegenstand des Sicherheitskonzeptes des qualifizierten Zeitstempeldienstes.

2.7.10 Netzwerksicherheit

Für den qualifizierten Zeitstempeldienst gilt bzgl. Netzwerk:

- Der qualifizierte Zeitstempeldienst wird auf dedizierten Servern betrieben. Die Server sind im Datacenter des Trustcenters der Deutschen Rentenversicherung aufgebaut und mittels Firewall vom Netz der Deutschen Rentenversicherung bzw. vom Internet abgetrennt.
- Der Zugang zum qualifizierten Zeitstempeldienst ist begrenzt auf dedizierte Netzwerkzugänge (Interface/Protokoll/Port).
- Der Zugang zum qualifizierten Zeitstempeldienst ist begrenzt auf authentisierte Benutzer.
- Eine Kommunikation vom qualifizierten Zeitstempeldienst zu den anderen Servern im Trustcenter der Deutschen Rentenversicherung ist nicht erforderlich.

Die Netzkonfiguration ist Gegenstand des Netzkonzeptes der Deutschen Rentenversicherung Bund.

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

2.7.11 Incident Management

Der qualifizierte Zeitstempeldienst wird online bzgl. Plattform und Service durch ein zentrales Monitoring überwacht. Alle Aktivitäten des qualifizierten Zeitstempeldienstes werden in Log-Dateien gespeichert und archiviert. Fehlermeldungen in den Log-Dateien werden im Monitoring ausgewertet.

Im Fall eines Plattform-Fehlers im Haupt-System kann auf das Backup-System umgeschaltet werden. Die Prozedur zur Umschaltung ist im Betriebskonzept beschrieben.

Im Fall eines Produkt-Fehlers wird ein Incident geöffnet und Unterstützung vom Hersteller des Produktes auf Basis abgeschlossener Wartungs- und Pflegeverträge angefordert.

2.7.12 Beweissicherung

Alle Aktivitäten des qualifizierten Zeitstempeldienstes werden in Log-Dateien gespeichert und archiviert. Das beinhaltet u.a.

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

Die Log-Dateien werden 5 Jahre archiviert (Siehe Kapitel 1.4). Aus technischen Gründen fehlt die Angabe der Einheit im Zeitstempel. Für die Nachweisführung über Log-Daten ist diese Angabe nicht notwendig.

2.7.13 Notfallmanagement

Die Wiederherstellung des qualifizierten Zeitstempeldienstes nach Ausfall des kompletten Dienstes oder von Komponenten des Dienstes ist im Notfallplan geregelt. Der Notfallplan ist Bestandteil des Betriebskonzeptes des Trustcenters der Deutschen Rentenversicherung.

2.7.14 Einstellung des Betriebes

Es gelten die Regelungen für die Beendigung der Tätigkeit eines qualifizierten Vertrauensdiensteanbieters. Die Prozeduren zur Einstellung des Betriebes des qualifizierten Zeitstempeldienstes sind im Betriebskonzept des Trustcenters der Deutschen Rentenversicherung definiert. Eine Benachrichtigung der Nutzer erfolgt gemäß der abgeschlossenen Verwaltungsvereinbarung.

2.7.15 Compliance

Der qualifizierte Zeitstempeldienst wird gemäß den Anforderungen der eIDAS-Verordnung betrieben. Die relevanten Sicherheitskonzepte sind bei der zuständigen Aufsichtsstelle gemäß eIDAS-Verordnung Art. 17 eingereicht.

2.8 Zusätzliche Anforderungen an den qualifizierten Zeitstempeldienst

2.8.1 TSU QC Public Key Zertifikat

Die Public Key Zertifikate für den qualifizierten Zeitstempeldienst werden von der qualifizierten Wurzelzertifizierungsstelle des Trustcenters der Deutschen Rentenversicherung ausgestellt. Das Zertifikat des qualifizierten Zeitstempeldienstes beinhaltet ein entsprechendes QC Statement [5].

2.8.2 Zeitstempeldienst zur Erstellung von qualifizierten Zeitstempeln

Der qualifizierte Zeitstempeldienst des Trustcenters der Deutschen Rentenversicherung erstellt nur qualifizierte Zeitstempel.

3 Listen, Verweise

3.1 Änderungsverzeichnis

V3.0	Januar 2009	
V4.0	Mai 2016	Anpassung gemäß den Standards ETSI EN 319401, ETSI EN 319421, eIDAS-Verordnung

3.2 Abkürzungen

BNetzA	Bundesnetzagentur
CC	Common Criteria
CEN	European Committee for Standardization (Europäisches Komitee für Normung)
EAL	Evaluation Assurance Level (EAL1 - EAL7)
eIDAS	Electronic Identification and Trust Services for Electronic Transactions in the European Market
ETSI	European Telecommunications Standards Institute (Europäischen Institut für Telekommunikationsnormen)
ISO	International Organization for Standardization (Internationale Normungsorganisation)
ITU	International Telecommunication Union (Internationale Fernmeldeunion)
OID	Object Identifier
QC	Qualified Certificate
QS	Qualitätssicherung
SSL	Secure Socket Layer
TLS	Transport Layer Security (Nachfolger von SSL)
TSA	Time Stamp Authority (Zeitstempeldienst)
TSP	Trusted Service Provider (Vertrauensdiensteanbieter)
TSU	Time Stamp Unit (Zeitstempeleinheit)

3.3 Begriffe

DCF77	Zeitzeichensender der Bundesrepublik Deutschland
Zeitstempeldienst	Zeitstempeldienst zur Erstellung von elektronischen Zeitstempeln unter Nutzung von einer oder mehreren Zeitstempeleinheiten
Zeitstempeleinheit	System aus Hard- und Software, das als eine Einheit verwaltet wird und einen Signaturschlüssel unter seiner Kontrolle hat. Aus Sicht des Zeitstempeldienstes handelt es sich dabei um eine Chipkarte als Signaturerstellungseinheit mit der zugehörigen Signatur-Bibliothek.

3.4 Referenzen

[1] eIDAS-Verordnung Nr. 910/2014 der EU
im Amtsblatt der Europäischen Union, L 257/73
http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A32014R0910

[2] ETSI EN 319401: Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
http://www.etsi.org/deliver/etsi_en/319400_319499/319401/

[3] 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/

[4] 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/

[5] ETSI TS 101862: Qualified Certificate Profile

[6] Certificate Policy der Wurzelzertifizierungsstelle der Deutschen Rentenversicherung

[7] RFC 3161: Internet X.509 Public Key Infrastructure Time Stamp Protocol (TSP)

[8] Web-Seite des Trustcenters der Deutschen Rentenversicherung Bund
http://www.deutsche-rentenversicherung-bund.de/static/trustcenter/policy.html

[9] Web-Seite der Bundes Netz Agentur zur Veröffentlichung geeigneter Algorithmen
http://www.bundesnetzagentur.de/cln_1432/DE/Service-Funktionen/QualifizierteelektronischeSignatur/WelcheAufgabenhatdieBundesnetzagentur/GeeigneteAlgorithmenfestlegen/geeignetealgorithmenfestlegen_node.html