Trustcenter der
Deutschen Rentenversicherung

Policy für den Zeitstempeldienst der Wurzelzertifizierungsstelle der Deutschen Rentenversicherung

Version 3.0

Stand 23.01.2009

Inhalt

1 Einleitung

1.1 Überblick

Die Träger der Deutschen Rentenversicherung betreiben ein gemeinschaftliches Trustcenter zur Bereitstellung von Zertifizierungsdiensten nach dem deutschen Signaturgesetz (SigG). Zu den Leistungen des Trustcenters der deutschen Rentenversicherung gehört auch ein Zeitstempeldienst, der qualifizierte Zeitstempel im Sinne des §2 Nr. 14 SigG ausstellt.

Das vorliegende Dokument ist die Policy des Zeitstempeldienstes der Wurzelzertifizierungsstelle der Deutschen Rentenversicherung. Es gilt auch als das von der Policy geforderte „TSA Disclosure Statement“. Die für dieses Statement geforderten Angaben finden sich in Kapitel 1.

Die vorliegende Certificate Policy basiert auf dem Standard „TS 102 023 – Policy requirements for time-stamping authorities“ in der Version 1.1.1 des European Telecommunications Standards Institute (ETSI). Das Verhältnis der vorliegenden Certificate Policy zum genannten Standard wird in Abschnitt 2 erläutert.

1.2 Dokumentenidentifikation

Bezeichnung des Dokuments:

Policy für den Zeitstempeldienst der Deutschen Rentenversicherung Bund,

Version 3.

Der ASN.1 Object Identifier (OID) für dieses Dokument ist

1.3.6.1.4.1.22204.1.8.1.1.3.

1.3 Teilnehmer und Instanzen

1.3.1 Trustcenter der Deutschen Rentenversicherung

Die Deutsche Rentenversicherung Bund betreibt eine Wurzelzertifizierungsstelle für die Ausgabe von Zertifikaten an Zertifizierungsstellen der Rentenversicherung und an den Zeitstempeldienst der Deutschen Rentenversicherung. Die Wurzelzertifizierungsstelle der Deutschen Rentenversicherung verwendet für die Erstellung der Zertifikate ein zentrales Zertifizierungssystem mit jeweils einer CA für qualifizierte und nichtqualifizierte Zertifikate.

Die Schlüssel, mit denen die beiden CA’s der Wurzelzertifizierungsstelle (die eine für qualifizierte Zertifikate, die andere für nicht qualifizierte Zertifikate) Zertifikate unterzeichnen, sind die grundlegenden „Vertrauensanker“ der Hierarchie. Über diese Schlüssel stellt jede Wurzelzertifizierungsstelle selbstsignierte Zertifikate aus.

Die CA für qualifizierte Zertifikate der Wurzelzertifizierungsstelle der Deutschen Rentenversicherung stellt die Zertifikate für den Zeitstempeldienst des Trustcenters der Deutschen Rentenversicherung aus.

1.3.2 Zeitstempeldienst der Deutschen Rentenversicherung

Die Deutsche Rentenversicherung Bund betreibt als Bestandteil der Wurzelzertifizierungsstelle der Deutschen Rentenversicherung in ihrer Rolle als qualifizierter Zertifizierungsdiensteanbieter gemäß SigG einen Zeitstempeldienst, der qualifizierte Zeitstempel im Sinne des §2 Nr. 14 SigG ausstellt.

1.3.3 Benutzer

Benutzer des Zeitstempeldienstes sind solche Personen und Systeme, die Zeitstempel vom Zeitstempeldienst anfordern können. Der Kreis der Benutzer ist auf

Rentenversicherungsträger, Sozialversicherungsträger und andere öffentlich-rechtliche Institutionen beschränkt und wird durch die Deutsche Rentenversicherung Bund verwaltet. Die Benutzung des Zeitstempeldienstes erfolgt auf der Grundlage einer Verwaltungsvereinbarung zwischen der Deutschen Rentenversicherung Bund 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 Zeitstempeldienst der Deutschen Rentenversicherung gibt qualifizierte Zeitstempel im Sinne des §2 Nr. 14 SigG aus.

Die Lebensdauer von Zeitstempeln ist grundsätzlich nicht begrenzt. Protokolldaten über ausgestellte Zeitstempel werden zum Schutz gegen die 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.

Die erzeugten Zeitstempel sind mit dem jeweils bei Erstellung des Zeitstempels gültigen Zertifikat des Zeitstempeldienstes verifizierbar. Das Zertifikat des Zeitstempeldienstes wird von der Wurzelzertifizierungsstelle der Deutschen Rentenversicherung (Subject: OU=QC Root CA, O=Deutsche Rentenversicherung, C=DE) auf den Namen CN=QC Root TSP, OU=QC Root CA, O=Deutsche Rentenversicherung, C=DE ausgestellt und ist über den Verzeichnisdienst der Wurzelzertifizierungsstelle der Deutschen Rentenversicherung abrufbar, und auf Anforderung auch im Response des Zeitstempeldienstes enthalten. Die Prüfung des Zertifikats hat gemäß der Vorgaben in dem Dokument „Certificate Policy und Certification Practice Statement der Wurzelzertifizierungsstelle der Deutschen Rentenversicherung“ [1] zu erfolgen.

Diese Zeitstempel können nur von Personen angefordert werden, die über ein Authentifizierungszertifikat verfügen, das bei der Deutschen Rentenversicherung hinterlegt und zur Nutzung des Zeitstempeldienstes als berechtigt konfiguriert wurde. Ein solches Zertifikat erhalten die in Abschnitt 1.3.3 genannten Benutzer nach Abschluss der dort erwähnten Verwaltungsvereinbarung von der Wurzelzertifizierungsstelle der Deutschen Rentenversicherung. Die Authentifizierung bei der Anforderung erfolgt über SSL.

Von berechtigten Personen und Systemen können Zeitstempel an der Adresse https:// tsp.tc.deutsche-rentenversicherung.de abgefragt werden. Das Format der Anfrage sowie der Antwort ist konform zum Standard ISIS-MTT. Unterstützte Hash-Algorithmen sind SHA-1, SHA-256, SHA-512 und RIPEMD-160.

1.4.2 Genauigkeit der Zeitstempel, Protokollierung

Der Zeitstempeldienst stellt die Zeitstempel mit der gesetzlichen Zeit und einer Genauigkeit von einer Sekunde aus. Die Synchronisation der Uhr des Zeitstempeldienstes mit der gesetzlichen Zeit erfolgt einmal alle zwölf Stunden, die Genauigkeitsüberprüfung gegen die gesetzliche Zeit 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 der Physikalisch-Technischen Bundesanstalt Braunschweig.

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

1.4.3 Pflichten der Benutzer des Zeitstempeldienstes

Die Pflichten der Benutzer des Zeitstempeldienstes im Sinne von Abschnitt 1.3.3 sind in der als Vorraussetzung für die Zulassung zur Nutzung abzuschließenden Verwaltungsvereinbarung geregelt.

1.4.4 Pflichten der auf Zeitstempeln vertrauenden Parteien

Parteien, die einem von der Deutschen Rentenversicherung herausgegebenen Zeitstempel vertrauen wollen, sind verpflichtet, die Signatur und den Zertifikatsstatus des Zeitstempeldienstes aktuell gemäß den Vorgaben in [1] zu prüfen.

1.4.5 Haftung des Zeitstempeldienstbetreibers

Die Wurzelzertifizierungsstelle der Deutschen Rentenversicherung haftet nach den allgemeinen gesetzlichen Vorgaben. Für die qualifizierten Signaturzertifikate des Zeitstempeldienstes gelten die Haftungsregelungen des SigG.

1.4.6 Datenschutz

Die Wurzelzertifizierungsstelle der Deutschen Rentenversicherung hält die gesetzlichen Bestimmungen zum Schutz der erhobenen personenbezogenen Daten ein (§ 14 SigG, ergänzend BDSG). Personenbezogene Daten werden in Form von Zertifikaten bei Anforderungen von Zeitstempeln zu Protokollierungs-, Abrechnungs- und Nachweiszwecken gespeichert und nach 5 Jahren gelöscht.

1.4.7 Anwendbares Recht

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

1.4.8 Zertifizierungen

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

Die TSP-Systemchipkarte des TSP-Responders ist eine gemäß SigG geprüfte und bestätigte sichere Signaturerstellungseinheit und wurde in der sicheren Umgebung der Wurzelzertifizierungsstelle personalisiert.

Der Betrieb des Zeitstempeldienstes erfolgt durch die Wurzelzertifizierungsstelle gemäß einem Sicherheitskonzept, das den Anforderungen des SigG genügt. Der Betrieb des Zertifizierungsdienstes (einschließlich des Zeitstempeldienstes) ist bei der Bundesnetzagentur angezeigt.

1.4.9 Organisation für die Verwaltung dieses Dokuments

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

1.4.10 Kontaktperson

Folgende Ansprechwege hinsichtlich dieser Policy bestehen:

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

2 Verhältnis zu ETSI TS 102 023

Allgemein basiert die vorliegende Policy auf den in „TS 102 023 – Policy requirements for time-stamping authorities“ des European Telecommunications Standards Institute (ETSI) genannten Anforderungen. In diesem Abschnitt wird das Verhältnis der vorliegenden Policy zu den Anforderungen des TS 102 023 genau definiert.

Bemerkung: Da TS 101 023 zum Zeitpunkt der Erstellung der vorliegenden Policy nur in englischer Sprache vorliegt, wird im Anhang eine Übersetzung der relevanten Kapitel 4 bis 7 von TS 101 023 gegeben.

2.1 Abweichungen von ETSI TS 102 023

2.1.1 TSA Practice Statement (Klausel 7.1.1 von TS 102 023)

Ein separates Practice Statement der TSA gibt es nicht. Die von der Klausel 7.1.1 von TS 102 023 geforderten Dokumentationen und Regelungen sind im Betriebs- und Sicherheitskonzept des Zeitstempeldienstes bzw. der Wurzelzertifizierungsstelle der Deutschen Rentenversicherung enthalten und vertraulich. Alle der Öffentlichkeit zugänglichen Informationen in Bezug auf den Zeitstempeldienst finden sich in dieser Policy und in dem Dokument „Certificate Policy und Certification Practice Statement der Wurzelzertifizierungsstelle der Deutschen Rentenversicherung“ [1]. Nutzer des Zeitstempeldienstes im Sinne von Abschnitt 1.3.3 dieser Policy schließen darüber hinaus eine Verwaltungsvereinbarung mit der Deutschen Rentenversicherung Bund, in der weitere, für diese Nutzer relevante Informationen enthalten sind.

2.1.2 TSA Disclosure Statement (Klausel 7.1.2 von TS 102 023)

Das TSA Disclosure Statement ist in Abschnitt 1 dieser Policy enthalten.

2.1.3 Zeitstempel (Klausel 7.3.1 h) von TS 102 023)

Aus technischen Gründen fehlt eine Unitangabe im Zeitstempel. Für die Nachweisführung über Logdaten ist diese Angabe auch nicht notwendig.

2.1.4 Stellenbeschreibungen (Klausel 7.4.3 b), c) von TS 102 023)

Stellenbeschreibungen im Sinne der oben genannten Klauseln sind im Sicherheits- und Betriebskonzept des Zeitstempeldienstes der Deutschen Rentenversicherung zu finden.

2.1.5 Kompromittierung von TSA-Diensten (Klausel 7.4.8 b), d) von TS 102 023)

Eine Benachrichtigung der Nutzer entsprechend der Klauseln 7.4.8 b) und d) von TS 102 023 erfolgt nach Maßgabe der Verwaltungsvereinbarung.

2.1.6 Beendigung der TSA-Dienste (Klausel 7.4.9 von TS 102 023)

Es gelten die Regelungen für die Beendigung der Tätigkeit eines qualifizierten Zertifizierungsdiensteanbieters gemäß SigG/SigV.

2.2 Über ETSI TS 102 023 hinausgehende Anforderungen

Die Zertifizierungsstelle der Deutschen Rentenversicherung Bund als Betreiber des Zeitstempeldienstes ist ein qualifizierter Zertifizierungsdiensteanbieter gemäß deutschem Signaturgesetz und hat ihre Betriebsaufnahme bei der zuständigen Behörde angezeigt.

Soweit das deutsche Signaturgesetz und die Signaturverordnung strengere Forderungen an den Betreiber der Zertifizierungsstelle als qualifiziertem Zertifizierungsdiensteanbieter stellen, werden diese strengeren Anforderungen – auch bezüglich des Zeitstempeldienstes - erfüllt.

2.3 Nicht anwendbare Anforderungen aus ETSI TS 102 023

2.3.1 Schutz des privaten Schlüssel der TSUs (Klausel 7.2.2 b), c) von TS 102 023)

Ein Backup privater Schlüssel der TSUs findet nicht statt.

2.3.2 Sicherheitsmanagement (Klause 7.4.1 e) von TS 102 023)

Der Zeitstempeldienst wird ohne Outsourcing-Partner erbracht.

Anhang A – Teilübersetzung von ETSI TS 102 023

Die vorliegende Policy basiert auf dem Standard „TS 101 023 – Policy requirements for time-stamping authorities“ des European Telecommunications Standards Institute (ETSI). Da dieser Standard zum Zeitpunkt der Erstellung der vorliegenden Certificate Policy nur in englischer Sprache vorliegt, wird in diesem Anhang eine Übersetzung der relevanten Kapitel 4 bis 7 von TS 101 456 gegeben.

Hinweis: Die Zertifizierungsstelle hat sich um eine getreue Übersetzung bemüht. Es handelt sich jedoch nicht um eine von ETSI oder im rechtlichen Sinne anerkannte Übersetzung. Im Zweifel sind daher die Anforderungen dieser Übersetzung ausschlaggebend.

4. Begriffe

4.1 Zeitstempel-Dienste

Die Bereitstellung von Zeitstempel-Diensten wird zur Unterscheidung in die folgenden Bereiche unterteilt:

- Zeitstempelerzeugung: Dieser Bereich erzeugt die Zeitstempel.
- Zeitstempel-Management: Dieser Bereich überwacht und kontrolliert den Betrieb der Zeitstempel-Dienste, um die Diensteerbringung gemäß diesem TSA zu gewährleisten. Der Bereich umfasst die Inbetriebnahme und Beendigung des Zeitstempel- Dienstes. Bspw. stellt das Zeitstempel-Management sicher, dass die für die Zeitstempelung verwendete Uhr auch genau auf die UTC eingestellt ist.

Diese Unterscheidung der Dienste dient lediglich der Erläuterung der in diesem Dokument aufgeführten Anforderungen, bedeutet aber keinen Ausschluss von anderen Unterscheidungen bei der Implementierung von Zeitstempeldiensten.

4.2 Zeitstempel-Anbieter

Die ausstellende Stelle für Zeitstempel heißt Zeitstempelanbieter (Time Stamping Authority - TSA) und ist die Vertrauensinstanz für die Nutzer der Zeitstempeldienste: Anwender und Empfänger. Die TSA trägt die Gesamtverantwortung für die Zeitstempeldienste gemäß Satz 4.1.

Die TSA ist verantwortlich für den Betrieb von einer oder mehr TSUs (Zeitstempel-Unit), die wiederum im Namen der TSA Zeitstempel erstellen und signieren. Die für einen Zeitstempel verantwortliche TSA ist aus dem Zeitstempel erkennbar.

Die TSA kann andere Stellen benennen, die Teile der Zeitstempel-Dienste übernehmen. Trotzdem behält die TSA die Gesamtverantwortung und stellt sicher, dass die in diesem Dokument genannten Policy-Anforderungen erfüllt werden. So kann die TSA auch sämtliche Dienste outsourcen, einschließlich derjenigen Dienste, die Zeitstempel erzeugen und dabei die Schlüssel der TSUs verwenden. Trotzdem gehören die privaten Schlüssel oder Schlüssel zur Erzeugung von Zeitstempeln der TSA, denn sie ist für die Erfüllung der hier beschriebenen Anforderungen verantwortlich.

Eine TSA kann mehrere identifizierbare Zeitstempel-Units betreiben. Jede Unit hat einen anderen Schlüssel.

Eine TSA ist gemäß Definition der EU-Richtlinie zu Elektronischen Signaturen (Art. 2 (11)) ein Zertifizierungsdiensteanbieter, der Zeitstempel ausgibt.

4.3 Anwender

Anwender eines Zeitstempeldienstes kann entweder eine Organisation mit mehreren End-Usern oder ein einzelner End-User sein.

Handelt es sich beim Anwender um eine Organisation, gehen die entsprechenden Pflichten nicht nur auf die Organisation, sondern auch auf den End-User über. In einigen Fällen ist die Organisation verantwortlich für die ordnungsgemäße Erfüllung der Pflichten ihrer End-User und es wird erwartet, dass sie ihre End-User entsprechend informiert.

Ist der Anwender ein End-User, so ist er unmittelbar selbst verantwortlich, falls er seinen Verpflichtungen nicht korrekt nachgekommen ist.

4.4 Zeitstempel-Policy und TSA Practice Statement

Dieser Abschnitt erläutert die Funktionen der Zeitstempel-Policy und des TSA Practice Statement. Er bedeutet aber keine bindende Vorgabe bezüglich der Form einer Zeitstempel-Policy oder eines Practice Statements.

4.4.1 Zweck

Im Allgemeinen legt die Zeitstempel-Policy fest, „was eingehalten wird“ während das TSA Practice Statement festlegt, „wie es eingehalten wird“, das heißt welche Prozesse die TSA verwendet um Zeitstempel zu erstellen und die Genauigkeit der verwendeten Uhr zu gewährleisten. Die Beziehung zwischen Zeitstempel-Policy und TSA Practice Statement ist im Wesen vergleichbar mit einer Geschäftspolitik, die die Geschäftsanforderungen definiert, während ausführende Stellen die Umsetzung und die konkreten Abläufe ausgestalten.

Das vorliegende Dokument definiert eine Zeitstempel-Policy, um den gängigen Anforderungen an vertrauenswürdige Zeitstempel-Dienste gerecht zu werden. Die TSA präzisiert im TSA Practice Statement, wie diese Anforderungen genau aussehen.

4.4.2 Detaillierungsgrad

Das TSA Practice Statement ist viel spezifischer als eine Zeitstempel-Policy. Ein TSA Practice Statement ist also eine wesentlich detailliertere Beschreibung der Vertragsbedingungen sowie der Geschäfts- und Betriebsprozesse einer TSA: einerseits der Erteilung von Zeitstempeln und andererseits der Verwaltung der Zeitstempel-Dienste. Das TSA Practice Statement einer TSA setzt die von der Zeitstempel-Policy vorgegebenen Regeln durch. Ein TSA Practice Statement definiert gemäß Zeitstempel-Policy, wie eine bestimmte TSA die technischen, organisatorischen und prozessualen Anforderungen umsetzt.

Anmerkung: Auch noch detailliertere interne Dokumente können für eine TSA erforderlich sein, um die Prozesse zur Erfüllung der Anforderungen aus dem TSA Practice Statement im Detail zu beschreiben.

4.4.3 Inhalt

Inhaltlich weicht die Zeitstempel-Policy erheblich vom TSA Practice Statement ab. Eine Zeitstempel-Policy wird unabhängig von den spezifischen Besonderheiten der Betriebsumgebung einer TSA erstellt. Ein TSA Practice Statement hingegen ist zugeschnitten auf Organisationsstruktur, Betriebsprozesse, Einrichtung und Infrastruktur einer TSA. Eine Zeitstempel-Policy kann vom Anwender der Zeitstempeldienste definiert werden, während das TSA Practice Statement immer vom Anbieter festgelegt wird.

5. Zeitstempel-Policies

5.1 Kurzbeschreibung

Eine Zeitstempel-Policy ist ein „benanntes Regelwerk, das die Anwendungsmöglichkeiten eines Zeitstempels für eine jeweilige Anwendergruppe und/oder eine Menge von Anwendungen mit gemeinsamen Sicherheitsanforderungen aufzeigt“.

Das vorliegende Dokument definiert Anforderungen für eine grundlegende Zeitstempel-Policy für TSAs, die Zeitstempel mit einer Genauigkeit von 1 Sekunde oder weniger ausgeben, auf der Basis von Public-Key-Zertifikaten.

Anmerkung 1: Ohne zusätzliche Maßnahmen ist der Empfänger gegebenenfalls nicht in der Lage, die Gültigkeit eines Zeitstempels nach der Gültigkeitsdauer des zugehörigen Zertifikats festzustellen.

Eine TSA kann aber auch ihre eigene Policy festlegen, die wiederum die in diesem Dokument definierte Policy noch erweitert/verstärkt. So eine Policy soll die hier aufgeführten Anforderungen umfassen oder weiter einschränken.

Wenn eine TSA und alle TSUs eine Genauigkeit von einer Sekunde oder weniger erreichen, sollte das im TSA Disclosure Statement auch so aufgeführt werden (siehe Abschnitt 7.1.2): Jeder Zeitstempel wird mit einer Genauigkeit von einer Sekunde oder weniger ausgegeben.

Anmerkung 2: Anforderung: Ein Zeitstempel muss eine eindeutige Referenz auf die angewandte Policy beinhalten.

5.2 Identifizierung

Die OID [X.208] dieser grundlegenden Zeitstempel-Policy lautet: itu-t (0) identified-organization(4) etsi (0) time-stamp-policy(2023), policy-identifiers(1), baseline-ts-policy (1)

In dem für Anwender und Empfänger erhältlichen TSA Disclosure Statement sollte eine TSA ebenfalls eine OID aus der Zeitstempel-Policy angeben, deren Einhaltung sie zusichert.

5.3 Anwendergruppe und Anwendungsmöglichkeiten

Diese Policy zielt darauf ab, die Anforderungen für das Zeitstempeln von qualifizierten elektronischen Signaturen (Europäische Richtlinie zu elektronischen Signaturen) für eine lange Gültigkeitsdauer (TS 101 733) zu erfüllen. Sie ist aber auch generell anwendbar auf Anforderungen vergleichbarer Qualität.

Diese Policy kann sowohl für öffentliche als auch nicht-öffentliche Zeitstempel-Dienste genutzt werden.

5.4 Konformität

Die TSA muss die OID für die Zeitstempel-Policy in ihre Zeitstempeln gemäß den Ausführungen in Abschnitt 5.2 aufnehmen oder aber ihre eigene Policy entwickeln, die die Anforderungen dieses Dokuments beinhaltet bzw. weiter einschränkt:

a) wenn die TSA die Einhaltung der Zeitstempel-Policy zusichert und ihren Anwendern und Empfänger auf Anfrage den Nachweis für die Einhaltung erbringt, oder

b) wenn die TSA die Übereinstimmung mit der Zeitstempel-Policy durch eine dritte Stelle hat prüfen lassen.

Eine zur Zeitstempel-Policy konforme TSA muss zeigen, dass

a) sie ihren Verpflichtungen gemäß Abschnitt 6.1 nachgekommen ist;

b) sie Maßnahmen ergriffen hat, um die in Abschnitt 7 genannten Anforderungen zu erfüllen.

6. Verpflichtungen und Verantwortlichkeiten

6.1 Verpflichtungen der TSA

6.1.1. Allgemeines

Die TSA muss gewährleisten, dass alle auf sie zutreffenden Anforderungen gemäß Abschnitt 7 umgesetzt sind, und zwar entsprechend der ausgewählten Zeitstempel-Policy.

Die TSA muss die Einhaltung der hier vorgeschriebenen Prozesse gewährleisten, auch wenn Aufgaben der TSA an Dritte übertragen wurden.

Die TSA muss weiterhin die zusätzlichen Verpflichtungen, die im Zeitstempel beschrieben oder referenziert werden, einhalten.

Die TSA muss alle Zeitstempel-Dienste in Übereinstimmung mit ihrem TSA Practice Statements anbieten.

6.1.2 TSA Verpflichtungen gegenüber den Anwendern

Die TSA muss die in ihren Geschäftsbedingungen zugesicherten Leistungen erfüllen, einschließlich der Verfügbarkeit und Genauigkeit ihrer Dienste.

6.2 Verpflichtungen des Anwenders

Dieses Dokument erlegt dem Anwender keine besonderen Verpflichtungen auf, die über TSA-spezifische, in den Geschäftsbedingungen der TSA beschriebene Verpflichtungen, hinausgehen.

Anmerkung: Es wird empfohlen, dass der Anwender umgehend nach Erhalt seinen Zeitstempel auf eine korrekte Signatur hin überprüft und kontrolliert, dass der private Schlüssel für die Zeitstempelsignatur nicht kompromittiert wurde.

6.3 Verpflichtungen der Empfänger

Die dem Empfänger bekanntzumachenden Geschäftsbedingungen (Abschnitt 7.1.2) sollen die Auflage enthalten, dass der Empfänger mit Erhalt des Zeitstempels

a) kontrollieren muss, dass der Zeitstempel korrekt signiert wurde und dass der private Schlüssel zur Unterzeichnung des Zeitstempels bis zum Zeitpunkt dieser Überprüfung nicht kompromittiert wurde.

   Anmerkung: Während der Gültigkeitsdauer des Zertifikats des Zeitstempeldienstes kann die Gültigkeit des Signaturschlüssels überprüft werden, indem der Sperrstatus des TSU-Zertifikats geprüft wird.

b) alle in der Zeitstempel-Policy enthaltenen Beschränkungen für die Nutzung von Zeitstempeln berücksichtigen muss

c) alle weiteren vorgeschriebenen Sicherheitsmaßnahmen aus Verträgen oder sonstigen Quellen berücksichtigt.

6.4 Haftung

Das vorliegende Dokument macht keine näheren Ausführungen zur Haftung. Insbesondere ist zu berücksichtigen, dass eine TSA ihre Haftung im Rahmen der geltenden Gesetze ausschließen oder beschränken kann.

7. Anforderungen an die Organisation der TSA

Die TSA muss Maßnahmen ergreifen, die die nachfolgend aufgeführten Anforderungen erfüllen.

Die Anforderungen dieser Policy enthalten keine Beschränkungen hinsichtlich einer Vergütung der Erbringung von Zeitstempeldiensten.

Die Anforderungen leiten sich aus den Sicherheitszielen ab und werden durch spezifische Anforderungen für Maßnahmen ergänzt, wo diese Ziele zuverlässig erfüllt werden müssen.

Anmerkung: Die einzelnen Maßnahmen ergeben sich aus einer Abwägung zwischen der erforderlichen Zuverlässigkeit und einer Minimierung der Beschränkungen für die Technik, mit der die TSA Zeitstempel ausstellt. In Abschnitt 7.4 (TSA Management and Operation) wird auf eine separate Beschreibung von detaillierteren Anforderungen für die Maßnahmen verwiesen. Aus diesen Gründen kann der Detaillierungsgrad der beschriebenen Anforderungen je nach Thema variieren.

Die Bereitstellung eines Zeitstempels als Antwort auf eine Anfrage liegt im Ermessen der TSA, abhängig von den Service Level Agreements mit dem Anwender.

7.1 Practice and Disclosure Statements

7.1.1 TSA Practice Statement

Die TSA muss gewährleisten, dass sie die erforderliche Zuverlässigkeit bieten kann, die für die Bereitstellung von Zeitstempel-Diensten notwendig ist.

Im Einzelnen:

a) Die TSA muss eine Risikoanalyse durchgeführt haben, um die Unternehmenswerte und die Bedrohungen dieser Werte einzuschätzen, um wiederum die notwendigen Sicherheitsmaßnahmen und Betriebsprozesse definieren zu können.

b) Die TSA muss eine Darstellung ihrer Vorgänge und Prozesse erstellen, mit denen sie die Anforderungen dieser Zeitstempel-Policy erfüllt.

   Anmerkung 1: In dieser Policy sind keine Anforderungen aufgeführt, die sich auf die Struktur des TSA Practice Statements beziehen.

c) Das TSA Practice Statement muss die Pflichten aller externen Stellen, die die TSA-Dienste unterstützen, mit den dazugehörigen Policies und Betriebsabläufen aufzeigen.

d) Die TSA muss ihren Zeitstempel-Anwendern und -Empfängern das TSA Practice Statement und gegebenenfalls weitere relevante Dokumente zur Verfügung stellen, um die Einhaltung der Zeitstempel-Policy bewerten zu können.

   Anmerkung 2: Die TSA muss grundsätzlich nicht alle Einzelheiten ihrer Betriebsabläufe veröffentlichen.

e) Die TSA muss ihre Geschäftsbedingungen für die Erbringung von Zeitstempel-Diensten wie in Abschnitt 7.1.2 beschrieben allen Anwendern und potenziellen Empfängern bekanntgeben.

f) Die TSA muss ein Organ der Geschäftsführung haben, das das Practice Statement verabschiedet.

g) Die Führungsebene der TSA muss sicherstellen, dass die Abläufe ordnungsgemäß implementiert werden.

h) Die TSA muss einen Review-Prozess für ihre Abläufe aufsetzen und dabei auch die Verantwortlichkeit für die Pflege des TSA Practice Statements festlegen.

i) Die TSA muss geplante Änderungen ihres Practice Statements rechtzeitig ankündigen und das geänderte Practice Statement nach der Verabschiedung gemäß Buchstabe f) unverzüglich gemäß Buchstabe d) bereitstellen.

7.1.2 TSA Disclosure Statement

Die TSA muss ihre Geschäftsbedingungen zur Erbringung von Zeitstempel-Diensten allen Zeitstempel-Anwendern und potenziellen Empfängern bekanntgeben. Diese Bekanntmachung muss für jede TSA-Zeitstempel.Policy mindestens folgende Informationen enthalten:

a) TSA-Kontaktinformationen

b) Die verwendete Zeitstempel-Policy

c) Mindestens einen Hash-Algorithmus, der auf die zu stempelnden Daten angewendet werden kann (hier wird kein Hash-Algorithmus vorgeschrieben)

d) Die voraussichtliche Lebensdauer der Signatur des Zeitstempels (abhängig von den verwendeten Hash- und Signatur-Algorithmen und von der Länge des privaten Schlüssels)

e) Die Genauigkeit der Zeit in den Zeitstempeln in bezug auf UTC.

f) Mögliche Beschränkungen bezüglich der Nutzung der Zeitstempel-Dienste

g) Mögliche Pflichten der Anwender, wie in Abschnitt 6.2 beschrieben

h) Die Pflichten der Empfänger, wie in Abschnitt 6.3 beschrieben.

i) Informationen, wie der Zeitstempel zu überprüfen ist, damit sich die Empfänger auf den Zeitstempel nach menschlichem Ermessen verlassen können (siehe Abschnitt 6.3) sowie mögliche Beschränkungen der Gültigkeitsdauer.

j) Den Zeitraum, über den Protokolle von TSA-Vorgängen aufbewahrt werden (siehe Abschnitt 7.4.10).

k) Das anwendbare Rechtssystem, einschließlich der Aussagen zur Erfüllung nationaler rechtlicher Anforderungen an Zeitstempeldienste.

l) Haftungsbeschränkungen

m) Die Verfahrensweisen bei Beschwerden und in Streitfällen.

n) Ob die TSA bezüglich der Einhaltung dieser Zeitstempel-Policy zertifiziert wurde, und wenn ja, durch welche unabhängige Stelle.

   Anmerkung 1: Es wird ebenfalls empfohlen, dass die TSA Aussagen zur Verfügbarkeit ihrer Dienste mit in ihr Zeitstempel Disclosure Statement aufnimmt: zum Beispiel die geschätzte Mean Time Between Failureder Zeitstempel-Dienste, die durchschnittliche Wiederherstellungszeit im Anschluss an den Ausfall und die Vorsorgemaßnahmen für den Wiederanlauf einschließlich der Datensicherung.

Diese Informationen müssen über ein dauerhaftes Kommunikationsmedium bereitgestellt werden. Die Informationen müssen in einer gängigen, verständlichen Sprache formuliert sein. Die Übertragung kann elektronisch erfolgen.

Anmerkung 2: Ein Template für ein TSA Disclosure Statements ist im Anhang D zu finden. Alternativ kann es aber auch als Teil eines Anwender-/Empfänger-Agreements bereitgestellt werden. Dieses TSA Disclosure Statement kann in einem TSA Practice Statement enthalten sein, wenn dies für den Leser unmissverständlich und leicht erkennbar ist.

7.2 Schlüsselmanagement-Lebenszyklus

7.2.1 Schlüsselerzeugung

Die TSA muss gewährleisten, dass alle kryptografischen Schlüssel in einer gesicherten Umgebung erzeugt wurden.

Im Einzelnen:

a) Die Generierung der TSU Signing Key(s) muss in einer physikalisch sicheren Umgebung (Abschnitt 7.4.4) von vertrauenswürdigem Personal (Abschnitt 7.4.3) mindestens im Vier-Augen-Prinzip durchgeführt werden. Das für diese Funktion berechtigte Personal muss beschränkt werden auf die Personen, die gemäß TSA Practice Statement hierfür erforderlich sind.

b) Die Erzeugung der TSU Signing Keys muss in einem kryptografischen -Modul erfolgen, das außerdem:

   - die Anforderungen aus FIPS 140-1 Level 3 oder höher erfüllt, oder
   - die Anforderungen aus dem CEN Workshop Agreement 14167-2 (CWA 1417-2) erfüllt, oder
   - als sicheres System gemäß EAL 4 oder höher nach ISO 15408 oder vergleichbaren Sicherheitskriterien geprüft wurde. Die Prüfung muss auf der Basis eines Security Targets oder eines Schutzprofils gemäß den Anforderungen dieses Dokuments erfolgt sein und auf einer Risikoanalyse basieren, die physikalische und andere nicht-technische Sicherheitsmaßnahmen berücksichtigt.

c) Der TSU-Schlüsselerzeugungs-Algorithmus, die daraus resultierende Schlüssellänge und der Signatur-Algorithmus, die für die Signierung von Zeitstempeln genutzt werden, müssen von einer nationalen Aufsichtsbehörde anerkannt oder nach dem neuesten Stand der Technik für die Erstellung von Zeitstempeln durch eine TSA geeignet sein.

7.2.2 Schutz des Privaten Schlüssels der TSUs

Die TSA muss die Vertraulichkeit der privaten Schlüssel der TSUs und die Aufrechterhaltung der Integrität gewährleisten.

Im Einzelnen:

a) Der Private Schlüssel der TSUs muss in einem kryptografischen Modul vorgehalten und angewendet werden, das

   - die Anforderungen aus FIPS 140-1 Level 3 oder höher erfüllt, oder
   - die Anforderungen aus dem CEN Workshop Agreement 14167-2 (CWA 1417-2) erfüllt, oder
   - als sicheres System gemäß EAL 4 oder höher nach ISO 15408 oder vergleichbaren Sicherheitskriterien geprüft wurde. Die Prüfung muss auf der Basis eines Security Targets oder eines Schutzprofils gemäß den Anforderungen dieses Dokuments erfolgt sein und auf einer Risikoanalyse basieren, die physikalische und andere nicht-technische Sicherheitsmaßnahmen berücksichtigt.

   Anmerkung: Von einem Backup der Privaten Schlüssel der TSUs wird abgeraten, um das Risiko einer Schlüsselkompromittierung zu minimieren.

b) Wenn Private Schlüssel der TSUs gesichert werden, dürfen sie nur von vertrauenswürdigem Personal mindestens im Vier-Augen-Prinzip kopiert, abgelegt und wiederhergestellt werden, und zwar in einer physikalisch sicheren Umgebung (Abs. 7.4.4). Das für diese Funktion berechtigte Personal muss beschränkt werden auf die Personen, die gemäß TSA Practice Statement hierfür erforderlich sind.

c) Alle Backup-Kopien der Privaten Schlüssel der TSUs müssen besonders geschützt werden, um die Vertraulichkeit auch bei der Speicherung außerhalb des Krypto-Moduls zu gewährleisten.

7.2.3 Verteilung der öffentlichen Schlüssel der TSUs

Die TSA muss gewährleisten, dass die Integrität und Echtheit der öffentlichen Signaturprüfschlüssel der TSUs und der verwendeten Parameter während der Verteilung an die Empfänger gewahrt wird.

Im Einzelnen:

a) Die öffentlichen Signaturprüfschlüssel der TSUs müssen den Empfängern in einem Public-Key-Zertifikat übermittelt werden.

   Anmerkung: TSU-Zertifikate können zum Beispiel von einer Zertifizierungsstelle ausgegeben werden, die von derselben Organisation wie die TSA betrieben wird, oder von einer anderen Zertifizierungsstelle.

b) Die öffentlichen Signaturprüfschlüssel der TSUs müssen von einer Zertifizierungsstelle ausgegeben werden, die nach einer Certificate Policy arbeitet, die ein Sicherheitsniveau entsprechend dieser Zeitstempel-Policy oder höher erfüllt.

7.2.4 Erneuerung der TSU-Schlüssel

Die Gültigkeitsdauer eines TSU-Zertifikats darf nicht länger sein als der Zeitraum, für den die gewählten Algorithmen und die Schlüssellänge als sicher angesehen wird. (Abschnitt 7.2.1.c)

Anmerkung 1: Folgendes ist zu beachten, wenn die Gültigkeitsdauer weiter beschränkt wird:

- Abs. 7.4.10 erfordert, dass Unterlagen bezüglich der Erbringung von Zeitstempel-Diensten für eine angemessene Zeit aufbewahrt werden, mindestens aber ein Jahr nach Ablauf der Gültigkeitsdauer der Signaturschlüssel der TSUs. Je länger die Gültigkeitsdauer des TSU-Zertifikats ist, desto länger müssen auch die Aufzeichnungen aufbewahrt werden.
- Sollte ein Privater Schlüssel einer TSU kompromittiert werden, so steigt die Anzahl der betroffenen Zeitstempel mit der Gültigkeitsdauer des TSU-Zertifikats.

Anmerkung 2: Eine Kompromittierung von TSU-Schlüsseln ist nicht nur abhängig von den Eigenschaften des verwendeten Krypto-Moduls, sondern auch von den Abläufen bei der System-Initialisierung und beim Schlüssel-Export (wenn diese Funktion unterstützt wird).

7.2.5 Ende des Lebenszyklus von TSU-Schlüsseln

Die TSA muss gewährleisten, dass die privaten Signaturschlüssel der TSUs nicht über ihre Gültigkeitsdauer hinaus benutzt werden.

Im Einzelnen:

a) Organisatorische oder technische Prozesse müssen gewährleisten, dass ein neuer Schlüssel eingesetzt wird, sobald ein TSU-Schlüssel abläuft.

b) Die privaten Signaturschlüssel der TSUs oder ihre Schlüsselteile, einschließlich aller Kopien, müssen vernichtet werden, und zwar so, dass die privaten Schlüssel nicht wiederhergestellt werden können.

c) Das System zur Erzeugung von Zeitstempeln muss jeden Versuch unterbinden, Zeitstempel zu erzeugen, wenn der private Signaturschlüssel abgelaufen ist.

7.2.6 Life Cycle Management der Signaturerstellungseinheit von Zeitstempeln

Die TSA muss die Sicherheit kryptografischer Hardware während ihrer gesamten Lebensdauer gewährleisten.

Im Einzelnen muss die TSA gewährleisten, dass:

a) Signaturerstellungseinheiten für Zeitstempel nicht während der Auslieferung manipuliert werden.

b) Signaturerstellungseinheiten für Zeitstempel nicht während der Lagerung manipuliert werden.

c) die Installation, Aktivierung und Duplizierung von TSU-Signaturschlüsseln in der Signaturerstellungseinheit nur von vertrauenswürdigem Personal , mindestens im Vier-Augen-Prinzip und in einer physikalisch gesicherten Umgebung durchgeführt wird (Abs. 7.4.4)

d) Signaturerstellungseinheiten für Zeitstempel korrekt funktionieren.

e) Private Signaturschlüssel der TSUs, die in Signaturerstellungseinheiten für Zeitstempel gespeichert werden, bei der Entsorgung dieser Module gelöscht werden.

7.3 Zeitstempeldienste

7.3.1 Zeitstempel

Die TSA muss gewährleisten, dass Zeitstempel sicher erzeugt werden und die korrekte Zeit beinhalten.

Im Einzelnen:

a) Die Zeitstempel-Policy muss im Zeitstempel referenziert werden.

b) Jeder Zeitstempel muss ein eigenes Identifizierungsmerkmal haben

c) Der von der TSU im Zeitstempel genutzte Zeitwert muss auf mindestes einen Echtzeitwert von einem UTC(k)-Labor zurückgeführt werden können.

   Anmerkung 1: Das Bureau International des Poids et Mesures (BIPM) errechnet die UTC-Zeit auf der Basis der lokalen Repräsentationen UTC(k) zahlreicher Atomuhren in nationalen metrologischen Instituten und nationalen Sternwarten auf der ganzen Welt. Das BIPM publiziert eine Liste der Abweichungen zwischen UTC und UTC(k) („Circular T“) . Diese Liste ist auf der BIPM-Website (www.bipm.org) abrufbar und umfasst alle Institute, die anerkannte UTC(k) Zeitreihen haben.

d) Die im Zeitstempel genutzte Zeit muss mit der UTC synchronisiert werden, und zwar mit einer Genauigkeit, wie in dieser Policy definiert und falls vorhanden, mit einer Genauigkeit wie im Zeitstempel selbst definiert.

e) Wenn die Zeitstempel-Uhr des Providers (Abs. 7.3.2c) nicht die erforderliche Genauigkeit aufweist (Abs. 7.1.2e), darf der Zeitstempel nicht erzeugt werden

f) Der Zeitstempel muss eine Darstellung (zum Beispiel als Hash-Wert) des gestempelten Dokuments enthalten, das vom Anfragenden angegeben wurde.

g) Der Zeitstempel muss mit einem Schlüssel signiert sein, der speziell für diesen Zweck generiert wurde.

   Anmerkung 2: Ein Protokoll für Zeitstempel ist in RFC 3631 definiert und in TS 101 861 ausgearbeitet.

   Anmerkung 3: Im Falle mehrer Anfragen fast zur selben Zeit wird die Einhaltung der Reihenfolge innerhalb der Genauigkeit der TSU-Uhr nicht gefordert.

h) Der Zeitstempel muss enthalten:

   - soweit anwendbar, ein Identifizierungsmerkmal des Landes, in dem die TSA ansässig ist;
   - ein Identifizierungsmerkmal der TSA

- ein Identifizierungsmerkmal der Unit, die die Zeitstempel ausgibt

7.3.2 Uhr-Synchronisation mit UTC

Die TSA muss gewährleisten, dass ihre Uhr mit der angegebenen Genauigkeit mit der UTC synchronisiert ist.

Im Einzelnen:

a) Die Kalibrierung der TSU-Uhren muss so erfolgen, dass davon ausgegangen werden kann, dass die Uhren nicht außerhalb der geforderten Genauigkeit gehen.

b) Die TSU-Uhren müssen vor Bedrohungen geschützt werden, die zu einer unbemerkten Verstellung der Uhr in einen Bereich außerhalb ihrer Kalibrierung führen können.

   Anmerkung 1: Zu den Bedrohungen zählen auch die Manipulation durch nicht-autorisiertes Personal, sowie Radio- oder Elektrik-Schocks.

c) Die TSA hat zu gewährleisten, dass erkannt wird, wenn die Zeit aus dem Zeitstempel von der UTC-Zeit abweicht (siehe auch 7.3.1e))

   Anmerkung 2: Zeitstempel-Empfänger sind über solche Vorfälle zu informieren (siehe Abs. 7.4.8)

d) Die TSA muss gewährleisten, dass die Uhr-Synchronisierung auch aufrechterhalten wird, wenn eine Schaltsekunde gemäß den Bekanntmachungen der dafür zuständigen Stelle auftritt. Die Umstellung für die Schaltsekunde muss in der letzten Minute desjenigen Tages erfolgen, für den die Schaltsekunde geplant war. Es ist eine Aufzeichnung des exakten Zeitpunkts (mit der angegebenen Genauigkeit) anzufertigen, an dem die Uhrumstellung erfolgt ist.

   Anmerkung 3: Eine Schaltsekunde ist eine Einstellung der UTC, die durch Überspringen oder Zufügen einer Extra-Sekunde in der letzten Sekunde eines UTC-Monats erreicht wird. Erste Priorität haben dabei Ende Dezember und Ende Juni, zweite Priorität jeweils Ende März oder Ende September.

7.4 TSA Management und Betrieb

7.4.1 Sicherheitsmanagement

Die TSA hat zu gewährleisten, dass die Administrations- und Managementprozesse geeignet und entsprechend anerkannter Best Practice umgesetzt sind.

Im Einzelnen:

a) Die TSA behält die Verantwortlichkeit für alle Bereiche der Bereitstellung von Zeitstempel-Diensten innerhalb des Umfangs dieser Zeitstempel-Policy, egal, ob Funktionen outgesourct wurden oder nicht. Verantwortlichkeiten Dritter müssen durch die TSA klar definiert werden bzw. entsprechende Vereinbarungen getroffen werden, um Dritte daran zu binden, alle von der TSA geforderten Maßnahmen auch umzusetzen. Die TSA ist weiterhin verantwortlich für die Bekanntgabe der relevanten Abläufe aller beteiligten Parteien.

b) Das TSA Management muss Leitlinien für die Informations-Sicherheit geben, und zwar durch ein geeignetes Steuerungs-Forum auf der Führungsebene, das für die Erstellung der TSA Information Security Policy zuständig ist. Die TSA muss die Veröffentlichung und Kommunikation dieser Policy an alle Mitarbeiter gewähren, die davon betroffen sind.

c) Die für die Sicherheit innerhalb der TSA notwendige Sicherheitsinfrastruktur muss durchgängig erhalten bleiben. Alle Veränderungen mit Auswirkungen auf das

realisierte Sicherheitsniveau müssen vom TSA Management Forum genehmigt werden.

Anmerkung 1: Für weitere Anleitungen zum Information Security Management und zu Sicherheitsinfrastrukturen, dem Management Information Security Forum und Information Security Policies, siehe ISO/IEC 17799.

d) Die Sicherheitsmaßnahmen und Betriebsprozesse für TSA-Einrichtungen, -Systeme und Informationswerte zur Erzeugung von Zeitstempel-Diensten müssen dokumentiert, implementiert und aufrecht erhalten werden.

Anmerkung 2: Die vorhandene Dokumentation (gewöhnlich System Security Policy oder Bedienerhandbuch genannt) sollte alle relevanten Ziele, Objekte und potenziellen Bedrohungen in Verbindung mit den angebotenen Diensten identifizieren, sowie die notwendigen Schutzmaßnahmen, um die Auswirkungen solcher Bedrohungen zu vermeiden oder zu begrenzen. Die Dokumentation soll mit der unter Abs. 7.1.1a beschriebenen Risikoanalyse einhergehen. Sie soll die Vorgaben, Anweisungen und Prozesse beschreiben, mit denen die beschriebenen Dienste und die zugehörigen Sicherheitsanforderungen realisiert werden können, und außerdem die Vorgehensweisen zu Sicherheitsvorfällen und Notfallsituationen darstellen.

e) Die TSA muss gewährleisten, dass die Informationssicherheit aufrecht erhalten wird, auch wenn die Verantwortlichkeit für einzelne TSA-Funktionen an eine andere Organisation oder Körperschaft outgesourct wurde.

7.4.2 Werte-Klassifizierung und -Management

Die TSA muss gewährleisten, dass ihre Informationen und andere Werte einen angemessenen Schutz erhalten.

Im Einzelnen:

- Die TSA muss laufend ein Verzeichnis aller Werte führen und eine Klassifizierung nach dem Schutzbedarf für diese Werte in Übereinstimmung mit der Risiko-Analyse durchführen.

7.4.3. Personelle Sicherheit

Die TSA muss dafür sorgen, dass die Personal- und Einstellungsprozesse die Vertrauenswürdigkeit des TSA-Betriebs unterstützen und verstärken.

Im Einzelnen

a) Die TSA muss Personal beschäftigen, das über entsprechendes Sachkunde, Erfahrung und Qualifikation für die angebotenen Dienste entsprechend seiner jeweiligen Aufgabe verfügt.

Anmerkung 1: Das TSA-Personal sollte die Anforderungen an „Sachkunde, Erfahrung und Qualifikation“ durch Schulungen und Nachweise, praktische Erfahrung oder einer Kombination aus diesen beiden erfüllen.

Anmerkung 2: Das TSA-Personal umfasst dasjenige Personal, das zur Durchführung von Aufgaben zur Erbringung der Zeitstempel-Dienste der TSA angestellt ist. Personal, das mit der Überwachung der TSA-Dienste betraut ist, muss kein TSA-Personal in diesem Sinne sein.

b) Sicherheitsfunktionen und Verantwortlichkeiten gemäß Definition der TSA Security Policy müssen in den Stellenbeschreibungen enthalten sein. Vertrauenspositionen, von denen die Sicherheit des TSA-Betriebs abhängt, müssen klar benannt sein.

c) Für das TSA-Personal (festangestellt oder temporär) müssen Stellenbeschreibungen vorhanden sein, die die Grundsätze des Vier-Augen-Prinzips, der geringstmöglichen Zugriffsrechte, einer Bestimmung der Kritikalität der Stelle aufgrund von Pflichten und Zugriffsrechten, einer Überprüfung des persönlichen Hintergrunds sowie Weiterbildung und Sicherheitsbewusstsein berücksichtigt. Wo erforderlich, muss zwischen übergreifenden und TSA-spezifischen Aufgaben unterschieden werden. Letztere müssen inklusive der erforderlichen Fähigkeiten und Erfahrungen beschrieben werden.

d) Das Personal muss Administrations- und Managementprozesse üben, die mit den TSA Information Security Management-Abläufen einhergehen. (Abs. 7.4.1)

Anmerkung 3: Siehe ISO/IEC 17799 für eine weitere Hilfestellung.

Die folgenden zusätzlichen Maßnahmen müssen beim Zeitstempel-Management umgesetzt werden:

e) Es muss Führungspersonal mit folgenden Qualifikationen beschäftigt werden:

- Kenntnis der Zeitstempel-Technologie, und
- Kenntnis der Technologie Elektronischer Signaturen, und
- Kenntnis der Mechanismen für die Kalibrierung oder Synchronisierung der TSU-Uhren mit UTC, und
- Vertrautheit mit den Sicherheitsmaßnahmen für Personal mit Sicherheits-Verantwortlichkeiten, und
- Erfahrung mit Informationssicherheit und Risikoanalysen.

f) Das gesamte Personal in Vertrauenspositionen muss frei von Interessenkonflikten sein, die Objektivität des TSA-Betriebs gefährden könnten.

g) Vertrauenspositionen umfassen die folgenden Verantwortlichkeiten:

- Security Officers: Gesamtverantwortung für das Management der Umsetzung der Sicherheitsmaßnahmen
- System-Administratoren: autorisiert zur Installation, Konfiguration und Aufrechterhaltung der vertrauenswürdigen TSA-Systeme für das Zeitstempel-Management.
- System-Operatoren: Verantwortlich für den täglichen Betrieb der vertrauenswürdigen TSA-Systeme. Autorisiert, das System-Backup und Recovery durchzuführen
- System-Auditoren: autorisiert, Archive und Audit-Logs der vertrauenswürdigen TSA-Systeme einzusehen.

h) Das TSA-Personal muss durch das für die Sicherheit zuständige Senior Management formal in die Vertrauenspositionen berufen werden.

i) Die TSA darf für die Vertrauenspositionen oder das Management keine Personen einsetzen, die eine Vorstrafe für ein Verbrechen oder eine andere Straftat haben, die sie oder ihn für diese Position ungeeignet erscheinen lassen. Das Personal darf keinen Zugang zu Vertrauensfunktionen haben, solange nicht alle notwendigen Überprüfungen abgeschlossen sind.

Anmerkung 4: In einigen Ländern ist es evtl. für die TSA nicht möglich, ohne Zusammenarbeit mit dem Bewerber Informationen über dessen Vorstrafen zu erhalten.

7.4.4 Physikalische und Umgebungs-Sicherheit

Die TSA hat zu gewährleisten, dass der physikalische Zugang zu kritischen Diensten kontrolliert und physikalische Risiken zu ihren Werten gesenkt werden.

Im Einzelnen

a) Für Zeitstempel-Erzeugung und Zeitstempel-Management gilt:

   - Der physikalische Zugang zu den Zeitstempel-Einrichtungen muss auf die ordnungsgemäß dafür autorisierten Einzelpersonen beschränkt sein.
   - Es müssen Maßnahmen ergriffen werden, um Verlust, Beschädigung oder Kompromittierung von Anlagen und Unterbrechungen des Geschäftsbetriebs zu vermeiden, und
   - Es müssen Maßnahmen ergriffen werden, um die Kompromittierung oder den Diebstahl von Informationen oder Informationsverarbeitungsanlagen vermeiden.

b) Ein Zugangsschutz muss im Krypto-Modul enthalten sein, um die Anforderungen an die Sicherheit von Krypto-Modulen gemäß Abs. 7.2.1 und Abs. 7.2.2 zu gewährleisten.

c) Folgende zusätzliche Maßnahmen müssen für das Zeitstempel-Management umgesetzt werden:

   - Die Zeitstempel-Management Einrichtungen müssen in einer Umgebung betrieben werden, die die Dienste physikalisch vor der Kompromittierung durch nicht autorisierten Zugang zu Systemen oder Daten schützt.
   - Physikalischer Schutz muss durch die Schaffung von klar definierten Sicherheits-Zonen (das heißt physikalischen Barrieren) rund um das Zeitstempel-Management. Teile der Betriebsstätte, die mit anderen Organisationen geteilt werden, müssen sich außerhalb dieser Zone befinden.
   - Physikalische und Umgebungs-Sicherheitsmaßnahmen müssen umgesetzt werden, um die Gebäude, in denen sich die System-Ressourcen befinden, die System-Ressourcen selbst und die Bereiche, die deren Betrieb unterstützen, zu schützen. Die TSA Policy zur physikalischen und Umgebungssicherheit für die das Zeitstempel-Management bertreffenden Systeme müssen mindestens umfassen: physikalische Zugangskontrolle, Naturkatastrophenschutz, Brandschutzmaßnahmen, Ausfall von Versorgungsleistungen (zum Beispiel Strom, Telekommunikation), Einsturzgefahr, Rohrbruch, Schutz vor Diebstahl, Einbruch und unbefugtem Zutritt, Disaster Recovery.
   - Maßnahmen zum Schutz vor unbefugter Entfernung von Geräten, Informationen, Datenträgern und Software mit Bezug zu den Zeitstempeldiensten vom Gelände.

     Anmerkung 1: Für weitere Anleitungen zu physikalischer und Umgebungs-Sicherheit, siehe ISO/IEC 17799.

     Anmerkung 2: Andere Aufgaben können innerhalb der Sicherheits-Zone wahrgenommen werden, wenn sichergestellt ist, dass nur autorisiertem Personal der Zutritt gestattet wird.

7.4.5 Management des Betriebes

Die TSA muss sicherstellen, dass die TSA-Systemkomponenten sicher sind und ordnungsgemäß betrieben werden, mit einem möglichst niedrigen Risiko von Fehlfunktionen:

Im Einzelnen

a) Die Integrität der TSA-System-Komponenten muss vor Viren, Schadprogrammen und nicht autorisierter Software geschützt werden.

b) Das Reporting von Sicherheitsvorfällen und darauf abgestimmte Reaktions-Prozesse müssen so umgesetzt werden, dass die Schäden durch Sicherheitsvorfälle und Fehlfunktionen auf ein Minimum gesenkt werden.

c) Mit den in vertrauenswürdigen TSA-Systemen eingesetzten Datenträger müssen sicher verfahren werden, um sie vor Zerstörung, Diebstahl, nicht-autorisiertem Zugang und Veraltung zu schützen.

   Anmerkung 1: Jeder Mitarbeiter mit Führungsverantwortung ist zuständig für die Planung und effektive Umsetzung der Zeitstempel-Policy und den damit verbundenen Abläufen, wie sie im Zeitstempel-Practice Statement beschrieben sind.

d) Es müssen Vorgehensweisen etabliert und implementiert werden für alle Vertrauenspositionen und administrativen Rollen, die Einfluss auf die Erbringung der Zeitstempel-Dienste haben.

Handhabung und Sicherheit von Datenträgern

e) Alle Datenträger müssen vorsichtig behandelt werden in Übereinstimmung mit den Forderungen des Informations-Klassifizierungs-Schemas (Abs. 7.4.2). Datenträger mit sensiblen Inhalten müssen sicher entsorgt werden, wenn sie nicht mehr benutzt werden.

Systemplanung

f) Der Kapazitätsbedarf muss überwacht und Hochrechnungen der zukünftigen Kapazitätsanforderungen müssen gemacht werden, um die Verfügbarkeit der erforderlichen Rechen- und Speicherkapazität sicherzustellen.

Reporting von Sicherheitsvorfällen und Reaktion

g) Die TSA muss zeitnah und planvoll agieren, um schnell auf die Vorfälle reagieren zu können und um Schäden durch Sicherheitsverletzungen zu begrenzen. Alle Vorfälle müssen nach ihrem Eintritt so schnell wie möglich an die Führungsebene berichtet werden.

Zusätzlich müssen die folgenden Sicherheitsmaßnahmen für das Zeitstempel-Management umgesetzt werden:

Betriebsprozesse und -verantwortlichkeiten

h) Die Sicherheitsaufgaben der TSA müssen von anderen Betriebsaufgaben getrennt werden.

   Anmerkung 2: Die Verantwortlichkeiten der Sicherheitsaufgaben der TSA umfassen:

   - Betriebsprozesse und -verantwortlichkeiten
   - Sichere Systemplanung und Abnahme
   - Schutz vor Schad-Software
   - Gebäudewartung
   - Netzwerk-Management
   - Aktive Überwachung der Audit-Journals, Analyse von Vorfällen und gegebenenfalls Ergreifen der erforderlichen Folgemaßnahmen
   - Sicherheit und Handhabung von Datenträgern

- Daten- und Software-Austausch

Diese Aufgaben müssen von vertrauenswürdigem TSA-Personal geleitet werden, können aber auch von Nicht-Spezialisten oder Betriebspersonal (unter Aufsicht) durchgeführt werden, soweit in der angewandten Security Policy und Dokumenten zu Rollen und Rechten beschrieben.

7.4.6 Management des Systemzugangs

Die TSA muss sicherstellen, dass der Zugang zu Systemen der TSA nur den ordnungsgemäß dafür autorisierten Personen möglich ist.

Im Einzelnen:

a) Es müssen Sicherheitsmaßnahmen (zum Beispiel Firewalls) zum Schutz der internen TSA -Netzdomänen implementiert werden, um den unbefugten Zugang zu verhindern, und zwar auch für Nutzer und sonstige Dritte.

   Anmerkung 1: Firewalls sollten so konfiguriert sein, dass jegliche Protokolle und Zugänge abgeblockt werden, die nicht für den Betrieb der TSA notwendig sind.

b) Die TSA muss eine wirksame Administration der Zugänge für Anwender, Administratoren und Auditoren gewährleisten, um die Sicherheit der Systeme aufrecht zu erhalten, einschließlich des Managements von User-Accounts, regelmäßiger Audits und einer zeitnahen Anpassung oder Entziehung von Zugangsberechtigungen.

c) Die TSA muss sicherstellen, dass der Zugang zu Informationen und Funktionen von Anwendungssystemen in Übereinstimmung mit der Strategie für die Zugangs-Kontrolle beschränkt wird, und dass die TSA-Systeme über ausreichende technische Sicherheitsmaßnahmen verfügen, um die Trennung von vertrauenswürdigen Rollen in den TSA Abläufen, einschließlich der Trennung von Sicherheitsadministration- und -betriebs. Insbesondere wird die Nutzung von Dienstprogrammen (Utilities) beschränkt und genau überprüft.

d) Vor der Nutzung von kritischen Anwendungen in Verbindung mit Zeitstempeln muss sich das TSA-Personal ordnungsgemäß identifizieren und authentisieren.

e) Die vom TSA-Personal durchgeführten Aktivitäten müssen Personen zuzurechnen sein, zum Beispiel durch die Aufbewahrung von Event.-Logs (vgl. Abschnitt 7.4.10).

Zusätzlich müssen die folgenden Sicherheitsmaßnahmen für das Zeitstempel-Management umgesetzt werden:

f) Die TSA muss sicherstellen, dass sich lokale Netzkomponenten (zum Beispiel Router) in einer physikalisch sicheren Umgebung befinden und dass ihre Konfiguration in regelmäßigen Abständen auf Übereinstimmung mit den TSA-Anforderungen überprüft wird.

g) Durchgängige Überwachungs- und Alarmierungseinrichtungen müssen eingerichtet werden, damit die TSA alle nicht-autorisierten und/oder ungewöhnlichen Zugriffsversuche auf ihre Ressourcen erkennen, registrieren und in zeitnaher Weise darauf reagieren kann.

   Anmerkung 2: Das können zum Beispiel sein: Intrusion–Detection-Systeme, die Überwachung der Zugangs-Kontrolle und Alarmanlagen.

7.4.7 Einrichtung und Wartung vertrauenswürdiger Systeme

Die TSA muss vertrauenswürdige Systeme und Produkte einsetzen, die gegen Manipulationen geschützt sind.

Anmerkung: Die für die TSA-Dienste durchgeführte Risikoanalyse (vgl. Abschnitt 7.1.1) sollte kritische Dienste identifizieren, die vertrauenswürdige Systeme erfordern, und die nötigen Sicherheitsniveaus (Assurance Levels) bestimmen.

Im Einzelnen:

a) Eine Schutzbedarfsanalyse muss in der Entwurfs- und Anforderungsdefinitionsphase jedes Entwicklungsprojektes, durchgeführt werden, das von der TSA oder im Auftrag der TSA durchgeführt wird, um zu gewährleisten, dass Sicherheit in die IT-Systeme integriert wird.

b) Change-Management-Verfahren müssen für die verschiedenen Releases, Veränderungen und Notfall-Anpassungen aller eingesetzten Software eingerichtet werden.

7.4.8 Kompromittierung von TSA-Diensten

Die TSA muss gewährleisten, dass im Falle von Vorfällen, die die Sicherheit der TSA-Dienste beeinträchtigen, einschließlich der Kompromittierung von privaten Signaturschlüsseln von TSUs oder einer erkannten Abweichung der TSU-Uhr, die notwendigen Informationen hierzu den Zeitstempel-Anwendern und -Empfängern zugänglich gemacht werden.

Im Einzelnen:

a) Der Notfallplan der TSA muss die Kompromittierung oder vermutete Kompromittierung von privaten Signaturschlüsseln von TSUs und eine Abweichung einer TSU-Uhr, die Auswirkungen auf ausgegebene Zeitstempel haben könnte, behandeln.

b) Im Falle einer (vermuteten) Kompromittierung oder einer Abweichung einer TSU-Uhr muss die TSA allen Zeitstempel-Anwendern und -Empfängern eine Beschreibung des Vorfalls übermitteln.

c) Im Falle der (vermuteten) Kompromittierung des Betriebes einer TSU (zum Beispiel einer TSU-Schlüssel-Kompromittierung) oder einer Abweichung der TSU-Uhr darf die TSU keine Zeitstempel ausgeben, bis Maßnahmen zur Bewältigung der Kompromittierung ergriffen sind.

d) Im Falle einer schweren Kompromittierung des Betriebs der TSA oder einer Abweichung der TSU-Uhr muss die TSA, wo immer möglich, alle Zeitstempel-Anwender und -Empfänger informieren, wie Zeitstempel, die möglicherweise betroffen sind, identifiziert werden können, soweit dies nicht den Datenschutz der TSA-Nutzer oder die Sicherheit der TSA-Dienste verletzt.

   Anmerkung: Wird der private Schlüssel kompromittiert, so kann eine Protokollierung aller von der TSA erzeugten Zeitstempel eine Möglichkeit bieten, um zwischen echten und falsch zurückdatierten Zeitstempeln zu unterscheiden. Die Verwendung zweier Zeitstempel von zwei verschiedenen TSAs wäre eine weitere Möglichkeit zur Behandlung dieses Problems.

7.4.9 Beendigung der TSA-Dienste

Die TSA muss sicherstellen, dass die möglichen negativen Auswirkungen, die aus einer Einstellung des Betriebs der Zeitstempeldienste resultieren, für Zeitstempel-Anwender und -Empfänger so gering wie möglich gehalten werden. Insbesondere muss die erforderliche Information zur Überprüfung der Korrektheit eines Zeitstempels weiter vorgehalten werden.

Im Einzelnen:

a) Vor der Einstellung der TSA-Zeitstempeldienste müssen mindestens die folgenden Schritte ausgeführt werden:

- die TSA muss allen Zeitstempel-Anwendern und Empfängern Informationen zur Einstellung ihrer Dienste bereitstellen.
- die TSA muss allen ihren Subauftragnehmern die Vollmacht entziehen, bei der Ausübung von Funktionen im Zusammenhang mit der Erstellung von Zeitstempeln in ihrem Namen zu handeln.
- die TSA muss einer zuverlässigen Stelle die Pflicht zur Vorhaltung von Event-Log- und Audit-Archiven (vgl. Abschnitt 7.4.10) auferlegen, damit für einen angemessenen Zeitraum der ordnungsgemäße Betrieb der TSA nachgewiesen werden kann.
- Die TSA muss ihrer Verpflichtung gegenüber den Zeitstempel-Empfängern zur Bekanntgabe ihres öffentlichen Schlüssels oder ihrer Zertifikate für eine angemessene Zeit weiter nachkommen oder diese an eine zuverlässige Stelle übertragen.
- Private Schlüssel von TSUs müssen einschließlich eventueller Sicherungskopien so vernichtet werden, dass eine Wiederherstellung der privaten Schlüssel unmöglich ist.

b) Die TSA muss eine Vereinbarung treffen, um die Kosten, die zur Erfüllung dieser Minimal-Anforderungen anfallen, für den Fall abzudecken, dass die TSA in Konkurs geht oder aus anderen Gründen die erforderlichen Mittel nicht selbst aufbringen kann.

c) Die TSA muss in ihrem Practice Statement die Vorkehrungen für die Beendigung ihrer Dienste bekannt geben. Dies muss beinhalten:
   - Benachrichtigung der betroffenen Stellen,
   - Übertragung der TSA-Pflichten an Dritte.

d) Die TSA muss Maßnahmen ergreifen, um das TSU-Zertifikat zu sperren.

7.4.10 Erfüllung der gesetzlichen Anforderungen

Die TSA muss ihre Erfüllung der gesetzlichen Anforderungen sicherstellen.

Im Einzelnen:

a) Die TSA muss gewährleisten, dass die Anforderungen der Europäischen Datenschutzrichtlinie (Dir 95/46/EC), umgesetzt durch die nationale Gesetzgebung, eingehalten werden.

b) Es müssen geeignete technische und organisatorische Maßnahmen gegen eine nicht-autorisierte oder gesetzeswidrige Verarbeitung von personenbezogenen Daten und gegen den unbeabsichtigten Verlust, die Zerstörung oder die Schädigung personenbezogener Daten umgesetzt werden.

c) Die von den Anwendern an die TSA übergebenen Daten müssen vor der Preisgabe an Dritte vollständig geschützt werden, außer mit dem Einverständnis der Anwender, bei Vorliegen eines gerichtlichen Beschlusses oder anderer gesetzlicher Anforderungen.

7.4.11 Aufbewahrung von Informationen zum Betrieb der Zeitstempel-Dienste

Die TSA muss gewährleisten, dass alle relevanten Informationen bezüglich des Betriebs der Zeitstempel-Dienste für einen definierten Zeitraum aufbewahrt werden, insbesondere zum Zwecke der Nachweisführung in gerichtlichen Verfahren.

Im Einzelnen:

Allgemein:

a) Die TSA muss dokumentieren, welche spezifischen Ereignisse und Daten geloggt werden müssen.

b) Die Vertraulichkeit und Integrität der aktuellen und archivierten Aufzeichnungen bezüglich des Betriebs der Zeitstempel-Dienste müssen erhalten werden.

c) Aufzeichnungen bezüglich des Betriebs der Zeitstempel-Dienste müssen vollständig und vertraulich in Übereinstimmung mit den veröffentlichten Geschäftsprozessen archiviert werden.

d) Aufzeichnungen zum Betrieb der Zeitstempeldienste müssen bei Bedarf zum Nachweis des ordnungsgemäßen Betriebes der Zeitstempeldienste im Rahmen von gerichtlichen Verfahren bereitgestellt werden.

e) Der exakte Zeitpunkt von wichtigen Ereignissen in der TSA-Umgebung, im Key-Management und bei der Uhr-Synchronisation muss aufgezeichnet werden.

f) Aufzeichnungen zu den Zeitstempel-Diensten müssen für einen Zeitraum nach Ablauf der Gültigkeit der Signaturschlüssel der TSUs aufbewahrt werden, der den Erfordernissen zur gerichtlichen Nachweisführung und den Angaben im TSA Disclosure Statement (vgl. 7.1.2) entspricht.

g) Die Aufzeichnung der Ereignisse muss so erfolgen, dass sie nicht ohne weiteres innerhalb des erforderlichen Aufbewahrungszeitraums gelöscht oder zerstört werden können (außer sie wurden zuvor zuverlässig auf dauerhafte Datenträger überspielt).

   Anmerkung: Das kann zum Beispiel erreicht werden durch die Verwendung von einmal-beschreibbaren Datenträgern, durch ein Verzeichnis aller benutzten Wechsel-Datenträger sowie durch eine ausgelagerte Datensicherung.

h) Alle Informationen über Anwender müssen vertraulich gehalten werden, außer es liegt eine Genehmigung des Anwenders für die weitere Verbreitung vor.

TSU-Schlüssel-Management

i) Alle Ereignisse zum Lebenszyklus von TSU-Schlüsseln müssen aufgezeichnet werden.

j) Alle Ereignisse zum Lebenszyklus von TSU-Zertifikaten (wenn vorhanden) müssen aufgezeichnet werden.

Uhr-Synchronisierung

k) Alle Ereignisse zur Synchronisierung von TSU-Uhren mit UTC müssen aufgezeichnet werden. Das umfasst auch die Informationen über die normale Re-Kalibrierung oder Synchronisierung der für Zeitstempel genutzten Uhren.

l) Alle Ereignisse zur Erkennung eines Verlusts der Synchronisierung müssen aufgezeichnet werden.

7.5 Organisatorisches

Die TSA muss gewährleisten, dass ihre Organisation zuverlässig ist.

Im Einzelnen:

a) Leitlinien und Verfahrensweisen, nach denen die TSA arbeitet, dürfen nicht diskriminierend sein.

b) Die TSA muss ihre Dienste für alle Anwender verfügbar machen, deren Aktivitäten in das erklärte Tätigkeitsfeld der TSA fallen, und die erklären, die Pflichten zu erfüllen, die im TSA Disclosure Statement definiert sind.

c) Die TSA ist eine Rechtsperson nach nationalem Gesetz.

d) Die TSA betreibt ein Qualitäts-Management-System und ein Informations-Sicherheits-Management-System, das für die erbrachte Zeitstempeldienste geeignet ist.

e) Die TSA hat eine für ihre Tätigkeit geeignete Haftungsvorsorge getroffen.

f) Sie verfügt über die erforderliche Finanzkraft und die erforderlichen Ressourcen, um in Übereinstimmung mit dieser Policy tätig zu werden.

   Anmerkung 1: Das schließt auch die Anforderungen für die Beendigung der Tätigkeit gemäß Abschnitt 7.4.9 ein.

g) Sie beschäftigt ausreichend Personal mit der erforderlichen Ausbildung, Übung, technischen Sachkunde und Erfahrung für Art, Ausmaß und Umfang der Tätigkeiten, die für die Erbringung der Zeitstempel-Dienste erforderlich sind.

   Anmerkung 2: Das von der TSA beschäftigte Personal umfasst alle Personen, die zur Erfüllung von Aufgaben für die Unterstützung der Zeitstempel-Dienste der TSA angestellt sind.
   Personen, die nur in die Überwachung der Dienste der TSA eingebunden sind, müssen nicht TSA-Personal sein.

h) Sie hat Leitlinien und Verfahrensweisen für die Klärung von Beschwerden und Streitigkeiten von Kunden oder anderen Stellen zur Erbringung der Zeitstempel-Dienste oder anderen Dingen, die damit in Verbindung stehen.

i) Sie hat überall dort eine ordnungsgemäß dokumentierte Vereinbarung und vertragliche Beziehung, wo die Erbringung ihrer Dienste Unteraufträge, Outsourcing oder andere Vereinbarungen umfasst.

Referenzen

[1] Certificate Policy und Certification Practice Statement der Wurzelzertifizierungsstelle der Deutschen Rentenversicherung