Policy für den sicheren Zeitstempeldienst des BEV

Version 1.3

3. April 2008

1 Dokumenteninformation

1.1 Zweck und Gültigkeit

Dieses Dokument enthält die Policy für den sicheren Zeitstempeldienst des BEV. Es wird vom BEV veröffentlicht und gemäß § 6 Abs. 2 SigG der Telekom-Control-Kommission als Aufsichtsstelle für elektronische Signaturen angezeigt.

1.2 Dokumentenhistorie

VERSION	DATUM	ÄNDERUNGSGRUND IN DIESEM DOKUMENT
1.0	30.11.2006	Version für die Anzeige der Aufnahme des Dienstes bei der TKK
1.1	16.12.2007	Änderung der Webseite in Punkt 3.1 auf www.bev.gv.at
1.2	13.07.2007	Anmerkung unter 3.4, dass MD5, SAH-1 wegen Sicherheitsbedenken nicht verwendet werden und zudem gemäß Empfehlung 2048 BIT-Verschlüsselung verwendet wird
1.3	03.04.2008	Änderung der Telefon- bzw. Faxnummer des BEV in Punkt 3.1 auf Tel. +43(0)1-211 10-0, Fax +43(0)1-211 10-2199

2 Inhaltsverzeichnis

3 Einleitung

3.1 Bundesamt für Eich- und Vermessungswesen (BEV)

Das Bundesamt für Eich- und Vermessungswesen (BEV) ist eine dem Bundesministerium für Wirtschaft und Arbeit nachgeordnete Bundesbehörde. Zu den Aufgaben des BEV zählt unter anderem der Betrieb von mehreren Atomuhren. Diese Atomuhren sind Teil des weltweiten Netzwerks von Zeitgebern, aus denen in den Mitgliedstaaten der Internationalen Meterkonvention alle offiziellen Zeitangaben abgeleitet werden.

Dieses Dokument beschreibt den vom BEV betriebenen sicheren Zeitstempeldienst. Ein Zeitstempeldienst ist eine Dienstleistung, mit welcher beliebige elektronische Dokumente mit einer fälschungssicheren Zeitangabe versehen werden können. Als „sicherer Zeitstempeldienst“ wird ein Zeitstempeldienst bezeichnet, welcher die entsprechenden hohen Anforderungen des Signaturgesetzes erfüllt.

Kontaktinformationen: Bundesamt für Eich- und Vermessungswesen, Schiffamtsgasse 1-3, 1025 Wien, http://www.bev.gv.at/, Tel. +43(0)1-211 10-0, Fax +43(0)1-211 10-2199, E-Mail: zeitstempeldienst@bev.gv.at.

Alle für den sicheren Zeitstempeldienst des BEV relevanten Informationen, insbesondere die aktuelle Fassung dieser Policy, werden auf der Website www.bev.gv.at/ veröffentlicht.

3.2 Identifikation

Diese Policy enthält alle Angaben, die eine „Time-stamp Policy“ nach dem Standard ETSI TS 102 023 enthalten muss. Solche Dokumente werden durch einen ASN.1 Object Identifier (OID) identifiziert, der auch in den ausgestellten Zeitstempeln angeführt wird, um die Konformität der ausgestellten Zeitstempel mit diesem Standard ersichtlich zu machen. Der OID dieser Policy lautet: 1.2.40.0.10.1.8.1.

3.3 Anwendungsbereich des sicheren Zeitstempeldienstes

Der sichere Zeitstempeldienst des BEV wird nach Maßgabe der unter 3.7 genannten Bedingungen öffentlich angeboten und kann für jeden Zweck verwendet werden, bei dem elektronische Dokumente mit einer fälschungssicheren Zeitangabe einer unabhängigen, vertrauenswürdigen Stelle versehen werden sollen. Insbesondere kann der sichere Zeitstempeldienste dazu verwendet werden, den Sicherheitswert elektronischer Signaturen zu erhöhen (vgl. § 17 SigV – Nachsignieren), etwa für die Erstellung von qualifizierten elektronischen Signaturen mit Langzeitgültigkeit wie sie im Standard ETSI TS 101 733 definiert wurden.

3.4 Verwendete Algorithmen und Formate des sicheren Zeitstempeldienstes

Die an den sicheren Zeitstempeldienst übermittelten Hashwerte der mit einem Zeitstempel zu versehenden Dokumente können mit den Algorithmen SHA-1, RIPEMD-160, SHA-256, SHA-384 oder SHA-512 erstellt werden. Dabei handelt es sich um jene kryptographischen Hashfunktionen, welche von den in Österreich mit der Vollziehung des Signaturgesetzes betrauten Einrichtungen (Rundfunk und Telekom Regulierungs-GmbH und A-SIT) für sichere elektronische Signaturen empfohlen werden.

Zur Berechnung des Hashwertes des Zeitstempels selbst wird der Algorithmus SHA-256 eingesetzt. Als Signaturalgorithmus wird RSA eingesetzt, die Schlüssellänge aller für den sicheren Zeitstempeldienst verwendeten Schlüsselpaare beträgt, wie im Standard empfohlen, 2048 Bit.

Die Hashfunktion MD5 wird nicht unterstützt. Da die Hashfunktion MD5 nie den Anforderungen der österreichischen Signaturverordnung entsprochen hat und da Experten auch die Kollisionsresistenz von SHA-1 in Zweifel ziehen, erscheinen diese Abweichungen vom Standard auch aus Sicht der RTR-GmbH notwendig.

Die ausgestellten Zeitstempel sowie die Kommunikation zwischen den Clients und den Servern des sicheren Zeitstempeldienstes entsprechen dem Standard RFC 3161.

3.5 Erwartete Lebensdauer der Zeitstempel

Aufgrund des technischen Fortschrittes werden kryptographische Verfahren mit der Zeit schwächer. Die Rechenleistung von Computern steigt im Zeitverlauf exponenziell, weshalb immer längere kryptographische Schlüssel mit Rechenleistung gebrochen werden können. Die vom BEV ausgewählten Verfahren (RSA mit 2048 Bit, SHA-256) sind mit den derzeit zur Verfügung stehenden Methoden und dem absehbaren Anstieg der Rechnerleistung auf Jahrzehnte hinaus auch mit sehr hohem finanziellem Aufwand nicht zu brechen. Neben der Rechnerleistung wächst aber auch der wissenschaftliche Erkenntnisstand. Fortschritte in der Kryptographie können dazu führen, dass der Aufwand, um einen Algorithmus zu brechen, sprunghaft abgesenkt wird. Anders als bei der Rechnerleistung, deren zukünftige Entwicklung aufgrund der exponenziellen Steigerung in den letzten Jahrzehnten recht gut abgeschätzt werden kann, lässt sich der wissenschaftliche Fortschritt schwerer abschätzen. Die für die elektronische Signatur zuständigen Behörden geben daher in der Regel nur für einige Jahre (in Österreich und Deutschland im Regelfall sechs Jahre) Empfehlungen ab. Die Algorithmen RSA mit 2048 Bit und SHA-256 werden in diesen Empfehlungen uneingeschränkt bis zum Ende der jeweiligen Geltungsdauer der Empfehlung genannt.

Das BEV schließt sich diesen Empfehlungen an: für die mit dem sicheren Zeitstempeldienst des BEV erzeugten Zeitstempel ist davon auszugehen, dass die Zeitstempel über einen Zeitraum von mindestens sechs Jahren auch mit hohem finanziellen Aufwand nicht gefälscht werden können. Das BEV wird die einschlägige Entwicklung beobachten und die von ihm verwendeten Algorithmen gegebenenfalls dem Stand der Forschung entsprechend austauschen, diese Policy überarbeiten und auf der Website über den Sachverhalt informieren.

Um den Beweiswert elektronischer Dokumente langfristig zu sichern, wird empfohlen, ein Archivsystem zu verwenden, das die Dokumente (samt ihren Signaturen) regelmäßig, im Abstand von wenigen Jahren, mit einem neuen sicheren Zeitstempel versieht, der jeweils dem aktuellsten Stand der Technik entspricht („Nachsignieren“). Damit wird dokumentiert, dass die bereits am Dokument angebrachten elektronischen Signaturen und Zeitstempel zu einem Zeitpunkt erstellt wurden, als sie nach dem Stand der wissenschaftlichen Forschung unbestritten noch nicht fälschbar waren. Es ist dabei nicht erforderlich, dass der neuerlich

angebrachte Zeitstempel vom selben Zeitstempeldienst oder einem anderen Anbieter eines Zeitstempeldienstes angebracht wird. Der sichere Zeitstempeldienst des BEV kann daher auch dazu verwendet werden, den Beweiswert von elektronischen Dokumenten zu sichern, die von anderen Personen oder anderen Zeitstempeldiensten mit einer elektronischen Signatur versehen wurden.

3.6 Genauigkeit der Zeitstempel

Die in diesem Dokument beschriebenen Sicherheitsmaßnahmen gewährleisten, dass keiner der vom sicheren Zeitstempeldienst des BEV ausgestellten Zeitstempel um mehr als eine Sekunde von der Koordinierten Weltzeit (Coordinated Universal Time – UTC) abweicht.

3.7 Nutzungsbedingungen

Das BEV behält sich vor, den Zeitstempeldienst frei für beliebige Nutzer anzubieten oder mit bestimmten Nutzern bzw. Nutzergruppen Service Level Agreements abzuschließen. Soweit die Dienstleistung kostenlos und für beliebige Nutzer angeboten wird, erfolgt dies für Testzwecke, jegliche Gewährleistung und Haftung ist ausgeschlossen. Soweit die Dienstleistung im Rahmen von Service Level Agreements angeboten wird, richtet sich die Nutzung nach den jeweiligen Service Level Agreements.

Mit dem Zeitstempeldienst können beliebige elektronische Dokumente mit Zeitstempeln versehen werden. Für die Erstellung eines Zeitstempels wird nicht das gesamte Dokument, sondern nur ein Hashwert des Dokumentes an das BEV übermittelt. Die Verantwortung für den Inhalt der Dokumente und für die korrekte Berechnung des Hashwerts liegt daher ausschließlich beim Nutzer des Dienstes.

Verpflichtungen für die Nutzer des Zeitstempeldienstes sind auch unten in 3.9 genannt, Verpflichtungen derer, die auf Zeitstempel vertrauen, in 3.10 und 3.11, Regelungen zur Haftung in 3.14.

3.8 Verpflichtungen des BEV als Anbieter des sicheren Zeitstempeldienstes

Das BEV ist als Anbieter eines sicheren Zeitstempeldienstes zur Einhaltung aller relevanten Anforderungen nach dem Signaturgesetz und der Signaturverordnung verpflichtet. Gemäß § 10 SigG sind für sichere Zeitstempeldienste technische Komponenten und Verfahren zu verwenden, die die Richtigkeit und Unverfälschtheit der Zeitangabe sicherstellen. § 18 SigG und § 9 SigV richten Anforderungen an die zu verwendenden Signaturerstellungseinheiten, insbesondere muss die Erfüllung dieser Anforderungen von einer Bestätigungsstelle geprüft werden.

Weiters verpflichtet sich das BEV selbst zur Einhaltung des Standards ETSI TS 102 023, auf dem diese Policy beruht. Aus diesem europäischen Standard ergeben sich zusätzliche detaillierte Anforderungen, unter anderem die Genauigkeit von einer Sekunde (siehe oben 3.6).

3.9 Verpflichtungen der Nutzer des Zeitstempeldienstes

Der Zeitstempeldienst entspricht dem Standard RFC 3161. Der Server des Zeitstempeldienstes nimmt Requests entgegen, die entsprechend diesem Standard formatiert sind, und antwortet darauf mit dem Standard entsprechenden Zeitstempeln bzw. Fehlermeldungen. Es liegt im Verantwortungsbereich des Nutzers, dass der Hashwert des mit einem Zeitstempel zu versehenden Dokumentes korrekt berechnet wird und dass das verwendete Hashverfahren im Zeitstempel-Request korrekt bezeichnet wird. Der Zeitstempeldienst akzeptiert nur die oben unter Punkt 3.4 genannten Hashfunktionen und prüft dabei nach, dass die Länge des übergebenen Hashwertes der Bezeichnung der vom Nutzer verwendeten Hashfunktion entspricht. Da das mit dem Zeitstempel zu versehende Dokument selbst nicht vorgelegt wird, kann der Zeitstempeldienst die korrekte Berechnung des Hashwertes durch die Software des Nutzers aber nicht nachprüfen.

Es sei darauf hingewiesen, dass das BEV jederzeit das verwendete Schlüsselpaar des Zeitstempeldienstes austauschen kann (siehe unten 4.4) und dass der Nutzer aufgrund der redundaten Ausführung des Systems nicht damit rechnen kann, dass sein Zeitstempel-Request von einem bestimmten Server bearbeitet wird. Nutzer des Zertifizierungsdienstes sollen daher Software verwenden, die durch einen Schlüsselwechsel nicht beeinträchtigt wird.

Darüber hinaus sind die Nutzer verpflichtet, die oben unter 3.7 genannten Nutzungsbedingungen bzw. die abgeschlossenen Service Level Agreements zu beachten.

3.10 Verpflichtungen derer, die auf Zeitstempel vertrauen

Wer auf den Sicherheitswert der vom sicheren Zeitstempeldienst des BEV erzeugten Zeitstempel vertrauen will, muss die im Folgenden angeführten Informationen zur Prüfung von Zeitstempeln und zur Haftung beachten.

3.11 Information zur Prüfung von Zeitstempeln

Der Zeitstempeldienst entspricht dem Standard RFC 3161. Für die Signaturen der Zeitstempel werden die oben unter 3.4 genannten Algorithmen (RSA mit 2048 Bit, SHA-256) verwendet, die Signaturen beruhen auf Zertifikaten nach dem Standard X.509. Bei der Überprüfung der Gültigkeit von Zeitstempeln muss Software verwendet werden, die diesen Standards entspricht.

Um sich zu überzeugen, dass das Zertifikat, auf welchem die Signatur der Zeitstempel beruht, tatsächlich das Zertifikat des BEV ist, wird empfohlen, die Zertifikatskette bis zum Top-Zertifikat der österreichischen Aufsichtsstelle für elektronische Signaturen zu überprüfen, in deren Verzeichnis alle österreichischen Zertifizierungsdienste eingetragen sind. Das derzeitige Top-Zertifikat der österreichischen Aufsichtsstelle ist ein selbst-signiertes Zertifikat mit der Ausstellerbezeichnung „Telekom-Control-Kommission Top 1“, ist bis 13.09.2010 gültig und am SHA-1-Fingerabdruck „91 49 29 ee c7 a0 21 b5 da 49 1a 35 a5 98 4c 2c f2 5b c7 55“ eindeutig erkennbar. Über allfällige diesbezügliche Änderungen informiert die Aufsichtsstelle ihrem Sicherheits- und Zertifizierungskonzept entsprechend auf der Website http://www.signatur.rtr.at/, dort kann auch das Top-Zertifikat der Aufsichtsstelle abgerufen werden. Alle für die Überprüfung der Zeitstempel maßgeblichen Zertifikate werden auch auf der Website des BEV veröffentlicht.

Alle Zertifikate in der Zertifikatskette zwischen den Zertifikaten des sicheren Zeitstempeldienstes des BEV und dem Top-Zertifikat der Aufsichtsstelle enthalten Verweise auf die entsprechenden Widerrufslisten. Um die Echtheit und Gültigkeit eines Zeitstempels zu überprüfen, muss Software verwendet werden, die solche Zertifikatsketten und die

entsprechenden Widerrufslisten prüfen kann. Es sei darauf verwiesen, dass viele handelsübliche Softwareprodukte Signaturen und Zeitstempel nur zum aktuellen Zeitpunkt prüfen und daher eine Fehlermeldung ausgeben, wenn eines der geprüften Zertifikate bereits abgelaufen ist oder in der Zwischenzeit widerrufen wurde. Gerade bei der Prüfung von Zeitstempeln, deren Erstellung einige Jahre zurückliegt, können solche Fehlermeldungen irreführend sein. Es wird daher empfohlen, Software zu verwenden, die in der Lage ist, die Zertifikatskette zum historischen Zeitpunkt, an welchem der Zeitstempel erstellt wurde, zu prüfen. Zu diesem Zeitpunkt müssen alle damals verwendeten Zertifikate bis hinauf zum Top-Zertifikat der Aufsichtsstelle gültig und nicht widerrufen gewesen sein. Ein späterer Ablauf des Gültigkeitszeitraums eines Zertifikates oder ein später erfolgter Widerruf eines Zertifikates beseitigt die Gültigkeit der erstellten Zeitstempels nicht. Der Sicherheitswert eines Zeitstempels verringert sich nur durch den technischen Fortschritt (siehe oben 3.5) aber nicht durch den Ablauf der Gültigkeit oder Widerruf eines der verwendeten Zertifikate.

Für den Fall, dass der sichere Zeitstempeldienst verwendet wird, um die zeitliche Reihenfolge von Dokumenten zu bestimmen (etwa dann, wenn Anträge in der Reihenfolge des Einlangens bearbeitet werden), wird empfohlen, die eindeutige Seriennummer als Maßzahl heranzuziehen und nicht die in den Zeitstempeln ausgewiesenen Zeitangaben. Da die Zeitangaben keine Sekundenbruchteile enthalten, können nämlich mehrere Zeitstempel die selbe Zeit aufweisen. Außerdem werden die Zeitstempel nach dem Prinzip der Lastverteilung von mindestens zwei verschiedenen Zeitstempeldienst-Servern erzeugt, deren Uhren um Sekundenbruchteile voneinander abweichen können. Die Seriennummern hingegen stammen für alle Zeitstempel aus dem selben Datenbanksystem und geben daher zuverlässig Auskunft über die Reihenfolge der erstellten Zeitstempel.

3.12 Archivierungsdauer der Log-Informationen

Über die Erstellung jedes einzelnen Zeitstempels wird ein Eintrag in einer Log-Datei erstellt, der unter anderem die laufende Seriennummer des Zeitstempels, die Zeitangabe und den Hashwert des mit dem Zeitstempel versehenen Dokumentes (nicht aber das Dokument selbst) enthält (siehe unten 6.11). Diese Log-Informationen werden mindestens drei Jahre lang aufbewahrt. Während dieses Zeitraums erteilt das BEV Personen, die ein rechtliches Interesse daran geltend machen (z. B. weil ein Rechtsstreit über ein mit einem Zeitstempel versehenes Dokument anhängig ist), auf Anfrage Auskunft über den jeweiligen Eintrag der Log-Datei.

Weiters sei auf die im Folgenden unter 3.14 angeführten Informationen zur Haftung verwiesen.

3.13 Anwendbare rechtliche Vorschriften

Das BEV ist eine dem Bundesministerium für Wirtschaft und Arbeit nachgeordnete Bundesbehörde und hat seinen Sitz in Wien. Es unterliegt somit österreichischem Recht und der Gerichtsstand ist (soweit nicht besondere Bestimmungen zur Anwendung kommen) Wien.

Für den sicheren Zeitstempeldienst sind insbesondere das Signaturgesetz (vgl. die §§ 10 und 18 SigG) und die Signaturverordnung (vgl. die §§ 14 und 15 SigV) von Relevanz.

Als Anbieter eines sicheren Zeitstempeldienstes unterliegt das BEV der Aufsicht der Telekom-Control-Kommission als Aufsichtsstelle für elektronische Signaturen (§ 13 SigG). Die Erbringung des Zeitstempeldienstes wird gemäß § 6 Abs 2 SigG bei der Aufsichtsstelle angezeigt, dabei werden auch diese Policy sowie allfällige Änderungen der Aufsichtsstelle vorgelegt. Die Aufsichtsstelle veröffentlicht auf ihrer Website http://www.signatur.rtr.at/ ein Verzeichnis der österreichischen Zertifizierungsdiensteanbieter, sowie Informationen über die von den Zertifizierungsdiensteanbietern erbrachten Dienste.

3.14 Haftungsbeschränkungen

Für den sicheren Zeitstempeldienst gelten die Schadenersatzregelungen des österreichischen Zivilrechts. § 23 SigG enthält eine Sonderregelung für die Haftung von Zertifizierungsdiensteanbietern, die qualifizierte Zertifikate ausstellen (§ 23 Abs. 1 SigG) oder „sichere elektronische Signaturverfahren bereitstellen“ (§ 23 Abs. 2 SigG). Das BEV stellt weder qualifizierte Zertifikate aus, noch stellt es Produkte bereit, mit denen Personen im eigenen Namen sichere elektronische Signaturen erstellen können. Das BEV ist aber gemäß §§ 10 und 18 SigG verpflichtet, für seinen sicheren Zeitstempeldienst Signaturerstellungseinheiten zu verwenden, die von einer Bestätigungsstelle nach § 18 Abs. 5 SigG bescheinigt wurden.

Als Anbieter eines sicheren Zeitstempeldienstes kennt das BEV die von ihm mit einem Zeitstempel versehenen Dokumente nicht. An den sicheren Zeitstempeldienst werden ausschließlich die Hashwerte dieser Dokumente übermittelt, aus welchen sich keinerlei Rückschlüsse auf den Inhalt des Dokumentes ableiten lassen. Das BEV haftet daher keineswegs für den Inhalt irgendeines mit einem Zeitstempel versehenen Dokumentes. Das BEV haftet in diesem Zusammenhang ausschließlich für die Einhaltung der Policy. Dies bedeutet im Wesentlichen, dass einlangende Zeitstempel-Requests auf ihre formale Richtigkeit geprüft werden, dass der darin enthaltene Hashwert mit einer genauen Zeitangabe versehen und ein dem Standard RFC 3161 entsprechender Zeitstempel erzeugt wird und dass dafür technische Komponenten und Verfahren eingesetzt werden, die den Anforderungen der einschlägigen Rechtsvorschriften und dieser Policy entsprechen.

Das BEV garantiert keine bestimmte Lebensdauer der erstellten Zeitstempel. Entsprechend dem oben unter 3.5 Ausgeführten ist eine langfristige Unfälschbarkeit der erstellten Zeitstempel zu erwarten. Das BEV orientiert sich dabei am Stand der Forschung und den Empfehlungen von in Österreich und anderen Staaten zuständigen Behörden für elektronische Signaturen. Es kann aber nie völlig ausgeschlossen werden, dass überraschende wissenschaftliche Fortschritte eine bislang allgemein als langfristig sehr sichere Technologie plötzlich weniger sicher erscheinen lassen. Dieses Risiko tragen alle, die auf die Sicherheit von Technologien angewiesen sind. Das BEV übernimmt diesbezüglich keinerlei Haftung.

Der sichere Zeitstempeldienst des BEV wird auf mindestens zwei voneinander unabhängigen Servern an zwei unterschiedlichen Standorten angeboten. Die meisten eingesetzten Komponenten sind redundant ausgeführt. Dadurch wird eine sehr hohe Verfügbarkeit des Zeitstempeldienstes erreicht. Gewährleistung für die Verfügbarkeit sowie Gewährleistung für die Interoperabilität zwischen der verwendeten Software auf den Clients und den Servern des Zeitstempeldienstes wird aber nur im Rahmen von Service Level Agreements zugesichert. Gegenüber Personen und Einrichtungen, die keine ausdrückliche diesbezügliche Vereinbarung mit dem BEV geschlossen haben, wird keinerlei Verfügbarkeit zugesichert. Das BEV kann Personen und Einrichtungen – unter Umständen auch der breiten Öffentlichkeit – die unentgeltliche Nutzung des sicheren Zeitstempeldienstes zu Testzwecken auch ohne Abschluss eines Service Level Agreements gestatten. Das BEV übernimmt diesbezüglich keinerlei Haftung: Das BEV haftet diesfalls auch nicht für die Interoperabilität und es behält sich vor, den Zugang zum Zeitstempeldienst jederzeit – auch ohne Angabe von Gründen und ohne Vorankündigung – einzuschränken oder zu sperren.

Die Haftung für leichte Fahrlässigkeit (ausgenommen Personenschäden) wird ausgeschlossen.

3.15 Streitbeilegung

Das BEV wird sich bemühen, bei Beschwerden eine Lösung zur Zufriedenheit der Nutzer zu finden.

Gemäß § 15 Abs. 4 SigG können Kunden oder Interessenvertretungen Streit- oder Beschwerdefälle, die mit einem Zertifizierungsdiensteanbieter nicht befriedigend gelöst worde

sind, der Rundfunk und Telekom Regulierungs-GmbH (http://www.rtr.at/) zur Streitschlichtung vorlegen. Die Zuständigkeit der ordentlichen Gerichte bleibt unberührt. Das BEV wird an solchen Streitschlichtungsverfahren entsprechend den von der RTR-GmbH erlassenen Verfahrensrichtlinien mitwirken und sich um eine einvernehmliche Lösung bemühen.

3.16 Konformitätserklärung

Diese Policy orientiert sich an den Anforderungen und der Gliederung des Standards ETSI TS 102 023 v1.2.1 (2003-01) „Policy requirements for time-stamping authorities“. Dieser europäische Standard wurde auch als RFC 3628 veröffentlicht. Das BEV erfüllt alle Anforderungen dieses Standards.

Gemäß § 6 Abs. 4 SigG hat das BEV diese der Aufsichtsstelle vorgelegte Policy sowohl bei der Aufnahme des Dienstes als auch während der Ausübung seiner Tätigkeit zu erfüllen. Das BEV unterliegt der Aufsicht der Telekom-Control-Kommission als Aufsichtsstelle für elektronische Signaturen, die sich gemäß § 13 Abs. 2 Z 1 SigG insbesondere auf die Einhaltung des Sicherheits- und Zertifizierungskonzeptes bezieht.

4 Schlüsselmanagement

4.1 Generierung der Schlüssel für den Zeitstempeldienst

Alle Schlüsselpaare des sicheren Zeitstempeldienstes des BEV werden in gesicherter Umgebung (siehe unten 6.4) unter Wahrung des Vier-Augen-Prinzips von zwei Personen erzeugt, die mit der Rolle eines Schlüsselbeauftragten betraut wurden (siehe unten 6.3). Für jeden Server wird genau ein Schlüsselpaar erzeugt. Alle erzeugten Schlüsselpaare werden mit 01 beginnend fortlaufend durchnummeriert, d. h. bei Aufnahme des Dienstes werden die Schlüssel mit den Nummern 01 und 02 eingesetzt.

Die Schlüsselgenerierung erfolgt in einer sicheren Signaturerstellungseinheit, die entweder über eine Zertifizierung nach FIPS 140-1 (bzw. FIPS 140-2) level 3 oder höher oder über eine Zertifizierung nach einem Common Criteria Protection Profile EAL 4 (z. B. CWA 14169, CWA 14167-2, CWA 14167-4) oder vergleichbaren Sicherheitskriterien (z. B. nach ITSEC) verfügt. Die Erfüllung der Sicherheitsanforderungen muss gemäß § 18 Abs. 5 SigG und § 9 SigV von einer Bestätigungsstelle geprüft sein. Bei der Schlüsselgenerierung müssen die Einsatzbedingungen aus der Bescheinigung der Bestätigungsstelle (§ 9 Abs. 4 SigV) bzw. die technisch-organisatorischen Sicherheitsmaßnahmen nach § 9 Abs. 3 SigV eingehalten werden.

Die Schlüssel werden so erzeugt bzw. die Signaturerstellungseinheit so konfiguriert, dass ein Export der Schlüssel aus der Signaturerstellungseinheit nicht möglich ist. Weitere Sicherheitsanforderungen an die vertrauenswürdigen Systeme zur Schlüsselgenerierung sind unten in 4.6 beschrieben.

Als Algorithmus für alle Schlüsselpaar des sicheren Zeitstempeldienstes wird RSA verwendet, als Schlüssellänge 2048 Bit. Bei der Auswahl der näheren Parameter der Schlüsselgenerierung werden die Anforderungen des Anhangs der Signaturverordnung sowie die Empfehlungen internationaler Standards (z. B. ETSI TS 102 176) sowie der für elektronische Signatur zuständigen Behörden beachtet.

4.2 Schutz des privaten Schlüssels

Die privaten Schlüssel des sicheren Zeitstempeldienstes werden in der sicheren Signaturerstellungseinheit gespeichert, in welcher sie erzeugt wurden (siehe oben 4.1). Sie verlassen diese Einheit nie. Die Signaturerstellungseinheit wird so konfiguriert, dass die privaten Schlüssel nicht exportiert werden können (siehe unten 4.6). Es gibt daher auch kein Backup der privaten Schlüssel. Wird ein Schlüssel wegen eines Defekts einer Signaturerstellungseinheit verloren, dann wird ein neues Schlüsselpaar erzeugt (siehe oben 4.1).

Die privaten Schlüssel des sicheren Zeitstempeldienstes werden ausschließlich zur Signatur von sicheren Zeitstempeln im Rahmen dieses Dienstes verwendet.

4.3 Verteilung der öffentlichen Schlüssel

Für die öffentlichen Schlüssel des sicheren Zeitstempeldienstes des BEV wird ein Zertifikat im Format X.509 ausgestellt. Die Schlüssel werden dabei so bezeichnet, dass auf das BEV als Anbieter des Zeitstempeldienstes, auf die Bezeichnung des Dienstes und auf die fortlaufende

Nummer des Schlüsselpaares verwiesen wird, z. B. „C=AT, O=Bundesamt für Eich- und Vermessungswesen, CN=Sicherer Zeitstempeldienst-01“.

Die Zertifikate des sicheren Zeitstempeldienstes sowie alle in der Zertifizierungshierarchie darüber liegenden Zertifikate bis hin zu einem selbstsignierten Wurzelzertifikat werden auf der Website des BEV veröffentlicht.

Das BEV wird dabei vorzugsweise Zertifikate verwenden, die ihm gemäß § 13 Abs. 3 SigG von der Telekom-Control-Kommission als Aufsichtsstelle für elektronische Signaturen ausgestellt werden. Damit können die Zeitstempel bis hin zum Top-Zertifikat im Verzeichnis der österreichischen Aufsichtsstelle geprüft werden (siehe oben 3.11). Das BEV behält sich aber vor, stattdessen andere Zertifikate einzusetzen (z. B. selbst ausgestellte Zertifikate oder von einem anderen Zertifizierungsdiensteanbieter ausgestellte Zertifikate). Diesfalls werden auf der Website des BEV entsprechende Angaben zur Zertifikatshierarchie und zur Prüfung der Zertifikatskette veröffentlicht. In jedem Fall wird darauf geachtet, dass die Policy, auf deren Grundlage die Zertifikate ausgestellt werden, ein dieser Policy für den sicheren Zeitstempeldienst vergleichbares Sicherheitsniveau gewährleistet.

4.4 Schlüsselwechsel

Ein Schlüsselwechsel erfolgt jedenfalls dann, wenn der verwendete Algorithmus (RSA), die verwendete Schlüssellänge (2048 Bit) oder die Algorithmen in den für den Schlüssel ausgestellten Zertifikaten nicht mehr als ausreichend sicher angesehen werden (siehe oben 3.5). Für den sicheren Zeitstempeldienst werden nur Zertifikate verwendet, deren Algorithmen über die gesamte Gültigkeitsdauer als ausreichend sicher angesehen werden.

Auch im Fall einer Kompromittierung wird ein Schlüsselwechsel vorgenommen (siehe unten 6.8).

Darüber hinaus kann die BEV zu jedem beliebigen Zeitpunkt einen Schlüsselwechsel vornehmen, z. B. wenn ein Server oder eine Signaturerstellungseinheit ausgetauscht werden soll.

Der bevorstehende Ablauf eines für einen Schlüssel des sicheren Zeitstempeldienstes ausgestellten Zertifikates beeinträchtigt die weitere Nutzung des Schlüssels nicht. Soweit der verwendete Algorithmus und die verwendete Schlüssellänge weiterhin als ausreichend sicher angesehen werden, wird dafür Sorge getragen, dass vor Ablauf des Zertifikates ein neues Zertifikates ausgestellt wird (welches im Subject-Feld den selben Inhalt aufweist).

4.5 Ende des Lebenszyklus der privaten Schlüssel

Das BEV stellt sicher, dass ein Schlüssel, der entsprechend dem oben unter 4.4 Ausgeführten außer Betrieb genommen wurde, nicht mehr weiter verwendet werden kann.

Es wird organisatorisch sichergestellt, dass in den unter 4.4 beschriebenen Fällen ein Schlüsselwechsel erfolgt. Weiters wird technisch sichergestellt, dass die Software des Zeitstempeldienstes keine Zeitstempel mehr erzeugt, wenn das Zertifikat, auf dem der Zeitstempel beruht, abgelaufen ist.

Von jedem privaten Schlüssel existiert nur ein einziges Exemplar in jener sicheren Signaturerstellungseinheit, in welcher er erzeugt wurde. Wenn ein Schlüssel außer Betrieb genommen wird, dann wird er unter Wahrung des Vier-Augen-Prinzips von zwei mit der Rolle eines Schlüsselbeauftragten betrauten Personen mit der Löschfunktion dieser Signaturerstellungseinheit unwiederbringlich gelöscht.

4.6 Lebenszyklus der Signaturerstellungseinheiten

Die sicheren Signaturerstellungseinheiten, die für den sicheren Zeitstempeldienst eingesetzt werden, werden während ihres gesamten Lebenszyklus geschützt. Das bedeutet insbesondere:

Vor der Inbetriebnahme einer Signaturerstellungseinheit wird entsprechend der Dokumentation des Gerätes und mit dessen Selbsttest-Funktionen geprüft, dass das Gerät ein Originalgerät ist und auf dem Transportweg nicht manipuliert wurde.

Durch die in Kapitel 6 beschriebenen Maßnahmen wird sichergestellt, dass die Signaturerstellungseinheit während ihrer gesamten Betriebszeit nicht verändert werden kann. Die Signaturerstellungseinheit verfügt über einen evaluierten Tamper-Detection-Mechanismus, der Manipulationsversuche erkennt und dabei alle gespeicherten Schlüssel automatisch unwiederbringlich löscht. Weiters wird die Signaturerstellungseinheit so konfiguriert, dass keine neue Firmware in das Gerät geladen und keine Veränderung der sicherheitsrelevanten Einstellungen der Konfiguration vorgenommen werden kann, ohne dass die gespeicherten Schlüssel unwiederbringlich gelöscht werden.

Die Inbetriebnahme der Signaturerstellungseinheiten, die Schlüsselgenerierung sowie die Außerbetriebnahme von Schlüsseln oder des gesamten Gerätes wird ausschließlich unter Wahrung des Vier-Augen-Prinzips von zwei mit der Rolle eines Schlüsselbeaurftragten betrauten Personen wahrgenommen. Über alle diesbezüglichen Vorgänge wird ein Protokoll angelegt.

Die korrekte Funktion der Signaturerstellungseinheiten wird laufend durch Selbsttests der Geräte geprüft. Durch organisatorische Maßnahmen wird sichergestellt, dass Fehlermeldungen erkannt und entsprechend behandelt werden.

Bevor eine Signaturerstellungseinheit außer Betrieb genommen wird, werden alle darauf gespeicherten Schlüssel mit den Löschfunktionen des Gerätes unwiederbringlich gelöscht. Ist dies wegen eines Defekts des Gerätes nicht mehr möglich, dann wird das Gerät auf andere Weise so zerstört, dass die Schlüssel unwiederbringlich gelöscht sind.

5 Zeitstempelung

5.1 Zeitstempel

Das BEV stellt sicher, dass alle Zeitstempel in sicherer Weise ausgestellt werden und die korrekte Zeit aufweisen. Die ausgestellten Zeitstempel entsprechen dem Standard RFC 3161 entsprechend dem im Standard ETSI TS 101 861 spezifizierten Profil (mit der Ausnahme, dass als Hashwert des Zeitstempels SHA-256 verwendet wird, da bei SHA-1 Zweifel an der langfristigen Sicherheit aufgetreten sind). Entsprechend RFC 3161 enthalten die Zeitstempel insbesondere:

- den ASN.1 Object Identifier dieser Policy (siehe oben 3.2),
- einen eindeutigen Bezeichner, dargestellt durch eine fortlaufend vergebene Seriennummer,
- die Zeitangabe, die direkt (siehe 5.2) von den Zeitgebern UTC(BEV) übernommen wird,
- diese Zeitangabe darf maximal eine Sekunde von UTC abweichen, diese maximale Abweichung wird ebenfalls im Zeitstempel angeführt (wenn der Server feststellt, dass ein Fehler vorliegt, aufgrund dessen der Zeitstempel möglicherweise um mehr als eine Sekunde von UTC abeichen könnte, wird kein Zeitstempel ausgestellt),
- den Hashwert des mit einem Zeitstempel zu versehenden Dokumentes,
- Angaben zum Staat (C=AT), zum Namen des Anbieters des Zeitstempeldienstanbieters (O=Bundesamt für Eich- und Vermessungswesen) und zum Server, der den Zeitstempel erstellt hat. Letzterer wird durch die fortlaufende Nummer des verwendeten Schlüsselpaars gekennzeichnet (CN=Sicherer Zeitstempeldienst-xx).

Alle Zeitstempel werden mit einem Schlüssel signiert, der ausschließlich für diesen Zweck vorgesehen ist.

5.2 Zeitgenauigkeit

Das für den Zeitstempeldienst verwendete Zeitsignal stammt direkt von den vom BEV selbst betriebenen Atomuhren. Diese gehören zu jenem internationalen Netzwerk von Atomuhren, das von dem durch die Internationale Meterkonvention eingerichteten Bureau International des Poids et Mesures (BIPM) verwaltet wird.

Das BEV betreibt drei Atomuhren, die untereinander und mit anderen Atomuhren im Netzwerk des BIPM synchronisiert werden. Zwei dieser Atomuhren sind jeweils mit einem im selben Raum untergebrachten NTP-Server verbunden. Über einen VPN-Tunnel wird das Zeitsignal von diesen NTP-Servern zu den beiden Servern des Zeitstempeldienstes in den beiden Rechenzentren des BEV geleitet.

Als weitere Zeitquelle dient ein GPS-Empfänger, der in einem anderen Gebäude des BEV untergebracht ist. Auch von diesem GPS-Empfänger wird das Zeitsignal mittels NTP über einen VPN-Tunnel an die beiden Server des Zeitstempeldienstes übertragen.

Darüber hinaus beziehen die beiden Server des Zeitstempeldienstes mittels NTP Zeitsignale von ausgewählten NTP-Servern im Internet.

Auf den beiden Servern des Zeitstempeldienstes ist jeweils ein NTP-Server installiert, der die solcherart erhaltenen Zeitsignale verwendet, um die Systemuhr zu synchronisieren. Der NTP-

Server ist so konfiguriert, dass er den NTP-Servern der Atomuhren größte Priorität einräumt und auf die anderen Zeitsignale nur dann zurückgreift, wenn das Zeitsignal von den Atomuhren ausfällt.

Die vom BEV implementierten Sicherheitsmaßnahmen (siehe Kapitel 6), insbesondere die verwendeten VPN-Tunnel, verhindern eine Manipulation der Zeitgeber und eine Manipulation des Zeitsignals auf dem Weg von den Zeitgebern zu den Servern des sicheren Zeitstempeldienstes.

Weiters wurden Sicherheitsmaßnahmen implementiert, durch die Fehler erkannt würden, bei denen die Verbindung zwischen den Zeitgebern und den Servern des Zeitstempeldienstes unterbrochen würde. Wenn die Gefahr besteht, dass die Zeit des Servers um mehr als eine Sekunde von UTC abweicht, würde sich der betreffende Server des Zeitstempeldienstes bis zur Störungsbehebung abschalten.

Die verwendeten Komponenten gewährleisten auch die korrekte Behandlung von Schaltsekunden. Über die Zeitpunkte, wann Schaltsekunden eingefügt oder gestrichen werden, führt das BEV aufgrund seiner Tätigkeiten beim Betrieb der UTC(BEV) Zeitgeber im Rahmen des BIPM ohnehin Protokoll.

Wenn ein Zwischenfall festgestellt wird, aufgrund dessen zu vermuten ist, dass Zeitstempel mit einer Abweichung zu UTC von mehr als einer Sekunde ausgestellt wurden, werden die Nutzer des Zeitstempeldienstes und die auf den Zeitstempeldienst vertrauenden Personen informiert (siehe unten 6.8).

6 Management und Betrieb

6.1 Sicherheitsmanagement

Das BEV stellt sicher, dass alle administrativen und organisatorischen Maßnahmen ergriffen werden, welche ein dem sicheren Zeitstempeldienst angemessenes Sicherheitsniveau gewährleisten und dem Stand der Technik entsprechen.

Das BEV trägt die Gesamtverantwortung für die Erbringung des sicheren Zeitstempeldienstes und für die Einhaltung dieser Policy, unabhängig davon ob die dafür erforderlichen Tätigkeiten selbst erbracht oder an Auftragnehmer ausgelagert werden. Wenn Aufgaben an Auftragnehmer außerhalb des BEV ausgelagert werden, werden diese Aufgaben klar definiert und die Erfüllung der Anforderungen dieser Policy wird durch geeignete Verträge sichergestellt.

Zu den ausgelagerten Tätigkeiten gehört insbesondere die Durchführung von Kontrollgängen durch eine externe Portierfirma sowie Dienstleistungen eines beauftragten Rechenzentrum. Der Rechenzentrumsbetreiber übernimmt dabei aber nur das Serverhousing, die Internetanbindung sowie die Zutrittsverwaltung. Die Server des BEV befinden sich jeweils in einem eigenen absperrbaren Bereich, der ausschließlich für das BEV vorgesehen ist. Der Zutritt zu diesem Bereich ist nur Mitarbeitern des BEV gestattet, die dem Betreiber des Rechenzentrums namentlich genannt wurden (siehe unten 6.4).

Das Sicherheitsmanagement, insbesondere die Weiterentwicklung dieser Policy und die Qualitätssicherung obliegen dem Leiter des Bundesamtes. Änderungen dieser Policy werden vom Leiter des Bundesamtes beschlossen.

Alle Sicherheitsmaßnahmen und betrieblichen Abläufe des sicheren Zeitstempeldienstes werden schriftlich dokumentiert, jeweils auf dem aktuellen Stand gehalten und in den entsprechenden Organisationseinheiten (siehe auch 6.3) umgesetzt.

Den mit Aufgaben des sicheren Zeitstempeldienstes befassten Mitarbeitern (siehe 6.3) und Auftragnehmern werden jeweils die aktuelle Fassung dieser Policy und der internen Sicherheitsrichtlinien und Betriebshandbücher zur Verfügung gestellt und sie werden zur Einhaltung dieser Policy in der jeweils aktuellen Fassung verpflichtet.

6.2 Sicherheitsrelevante Einrichtungen

Die folgenden Einrichtungen werden für die Erbringung des sicheren Zeitstempeldienstes benötigt. Das BEV sorgt durch die in Kapitel 6 beschriebenen Maßnahmen für einen angemessen Schutz dieser sicherheitsrelevanten Einrichtungen.

- In einem der Gebäude des BEV („Gebäude E“) befinden sich in einem durch Zutrittskontrollen (siehe unten 6.4) gesicherten Raum drei Atomuhren, von denen zwei für den Zeitstempeldienst verwendet werden, sowie zwei NTP-Server, weiters in diesem und anderen Räumen die erforderliche Netzwerkinfrastruktur.
- In einem anderen Gebäude des BEV („Gebäude A“) befindet sich ein GPS-Empfänger sowie ein NTP-Server und Netzwerkinfrastruktur. Am Dach des Gebäudes ist dessen Antenne angebracht.
- In zwei weiteren Gebäuden befinden sich Rechenzentren eines Dienstleisters des BEV. Das BEV hat in diesen beiden Rechenzentren jeweils einen eigenen absperrbaren Bereich angemietet. Darin befinden sich verschiedenste Server des BEV, insbesondere die beiden

Server des sicheren Zeitstempeldienstes. Die sicheren Signaturerstellungseinheiten befinden sich je nach dem ausgewählten Produkt entweder innerhalb der Server (z. B. als PCI-Karten) oder sie werden durch mechanische Maßnahmen (versperrbares Behältnis) vor unbefugtem Entfernen bzw. unbefugtem Trennen der Verbindung zum Server geschützt. Weiters befinden sich in den Rechenzentren auch die Datenbankserver, auf denen das Datenbanksystem des BEV läuft. Dieses Datenbanksystem wird zur Archivierung der Log-Dateien des sicheren Zeitstempeldienstes sowie zur Vergabe der eindeutigen, streng aufsteigend vergebenen Seriennummern der Zeitstempel verwendet.

- Die genannten Gebäude sind durch vom BEV selbst betriebene Netzwerke auf eigenen Glasfasern redundant verbunden. Insbesondere ist jedes der beiden Rechenzentren sowohl mit Gebäude A als auch mit Gebäude E jeweils über zwei auf unterschiedlichen Wegen geführten Glasfasern verbunden.

Die Server des sicheren Zeitstempeldienstes samt den daran angeschlossenen sicheren Signaturerstellungseinheiten werden ausschließlich für Zwecke des sicheren Zeitstempeldienstes verwendet.

Alle anderen Komponenten sowie alle verwendeten Räume werden auch für andere Aufgaben des BEV verwendet, welche aber mit den Aufgaben des sicheren Zeitstempeldienstes nicht unvereinbar sind:

- Die Atomuhren sowie die NTP-Server in Gebäude E dienen verschiedensten Aufgaben, bei denen exakte Zeitangaben benötigt werden. Alle diese Aufgaben haben aber die Genauigkeit des Zeitsignals sowie die Ausfallsicherheit des Gesamtsystems gemeinsam. Daher sind auch alle relevanten Komponenten redundant ausgeführt. Für das Personal, welches die Atomuhren und die NTP-Server betreut, gehört die Genauigkeit und Unverfälschtheit und die Ausfallsicherheit zu den Kernaufgaben.
- Der GPS-Empfänger wird ausschließlich für Zwecke des sicheren Zeitstempeldienstes verwendet.
- Die Netzwerkinfrastruktur zwischen den Gebäuden wird für verschiedenste Aufgaben der BEV eingesetzt. Für Zwecke des sicheren Zeitstempeldienstes werden daher zwischen den Räumen, in denen sich die Zeitgeber und deren NTP-Server befinden und den beiden Rechenzentren jeweils VPN-Tunnel eingerichtet.
- In den beiden Rechenzentren befinden sich zahlreiche Server des BEV, die verschiedenste Aufgaben wahrnehmen. Insbesondere werden die Datenbank und das Storage Area Network sowie das Backupsystem für verschiedene Zwecke des BEV verwendet. Die sicherheitsrelevanten Kernaufgaben des Zeitstempeldienstes (Überprüfung der Genauigkeit und allfälliger Ausfälle des Zeitsignals, Sicherheit des privaten Schlüssels, Überprüfung der einlangenden Zeitstempel-Requests und Ausstellung der Zeitstempel) werden daher ausschließlich auf den Servern des Zeitstempeldienstes sowie den direkt daran angeschlossenen sicheren Signaturerstellungseinheiten implementiert. Die Datenbank wird vom sicheren Zeitstempeldienst ausschließlich für die Verwaltung der Seriennummern der Zeitstempel und die Ablage der Log-Dateien verwendet.

6.3 Personelle Sicherheit

Sämtliche Aufgaben im Zusammenhang mit dem sicheren Zeitstempeldienst des BEV dürfen nur von Personen durchgeführt werden, die mit einer der im Folgenden beschriebenen Rolle ausdrücklich betraut wurden.

Da die sicherheitsrelevanten Kernaufgaben auf den Servern des Zeitstempeldienstes bzw. den daran angeschlossenen sicheren Signaturerstellungseinheiten erfolgt, wurde für die Verwaltung dieser Server eine eigene Rolle definiert, nämlich die des Schlüsselbeauftragten.

- Ein *Schlüsselbeauftragter* ist für die sichere Konfiguration der Server des Zeitstempeldienstes und der sicheren Signaturerstellungseinheiten verantwortlich. Für alle Maßnahmen auf den sicheren Signaturerstellungseinheiten selbst (Konfiguration, Schlüsselgenerierung, Löschen von Schlüsseln, siehe Kapitel 4) gilt ein Vier-Augen-Prinzip, alle anderen Maßnahmen auf den Servern können auch von einem Schlüsselbeauftragten alleine vorgenommen werden. Der Leiter des Bundesamtes ernennt vier Personen zu Schlüsselbeauftragten. Dabei wählt er zwei Personen aus dem Kreis der für IT-Sicherheit zuständigen Mitarbeiter und zwei Personen aus dem Kreis der für den Serverbetrieb zuständigen Mitarbeiter. Letztere sind für die laufende Serverwartung (insbesondere: Einspielen von Security-Patches, Überprüfung von Fehlermeldungen, Beheben von Störungen, Beaufsichtigung von externem Wartungspersonal) verantwortlich. Aufgaben, für die das Vier-Augen-Prinzip gilt, können von zwei beliebigen Schlüsselbeauftragten vorgenommen werden.

Für die übrigen Aufgaben definiert diese Policy keine eigenen Rollen, sondern es werden diese Aufgaben von Mitarbeitern der verschiedenen Abteilungen des BEV im Rahmen ihres jeweiligen Aufgabenbereiches wahrgenommen. Insbesondere sind zu nennen:

1) Mitarbeiter, die für die Betreuung der Atomuhren und der NTP-Server im Gebäude E verantwortlich sind. Zu den Kernaufgaben dieser Mitarbeiter gehört die Sicherstellung der Genauigkeit der Atomuhren und der NTP-Server.

2) Die Abteilung Informationstechnik ist verantwortlich für

- den Netzwerkbetrieb;
- den Betrieb der Server (zwei der damit befassten Mitarbeiter werden mit der Rolle eines Schlüsselbeauftragten beauftragt, siehe oben);
- die Betreuung der Fachapplikationen (einer der damit befassten Mitarbeiter wird mit der Projektbetreuung des sicheren Zeitstempeldienstes beauftragt);
- den Betrieb des Storage Area Network, die Datensicherung und die Wartung der Datenbanken;
- den Schutz der IT-Infrastruktur und der Zugänge von außen (zwei dieser Security Officer werden mit der Rolle eines Schlüsselbeauftragten betraut, siehe oben);
- die Überwachung von Servern und Applikationen und die Erstellung der Betriebsstatusberichte.

In allen genannten Rollen werden ausschließlich Personen beschäftigt, welche zuverlässig sind und das erforderliche Fachwissen und die erforderliche Erfahrung und Qualifikation aufweisen, die für die Wahrnehmung der den Rollen entsprechenden Aufgaben notwendig ist.

6.4 Physikalische Sicherheit

Mit Ausnahme der Zeitgeber (samt NTP-Servern) befinden sich alle Komponenten in den beiden Rechenzentren (insbesondere die Server des Zeitstempeldienstes, die sicheren Signaturerstellungseinheiten, die Datenbank und das Storage Area Network). Die Rechenzentren werden vom beauftragten Rechenzentrumsbetreiber gegen unbefugten Zutritt geschützt. Das BEV hat in beiden Rechenzentren eigene abgesperrte Bereiche angemietet, die nur von benannten Mitarbeitern des BEV betreten werden dürfen. Die Identitätsprüfung und Zutrittskontrolle erfolgt durch den beauftragten Rechenzentrumsbetreiber. Alle Server sowie auch die Switches für die Netzwerkverbindungen zwischen den verschiedenen Standorten des BEV befinden sich innerhalb dieses abgesperrten Bereichs.

Die Server des Zeitstempeldienstes sowie die sicheren Signaturerstellungseinheiten werden darüber hinaus so versperrt, dass Veränderungen an der Hardware nicht von allen

Zutrittsberechtigten vorgenommen werden können, sondern nur durch jene Personen, die mit der Rolle eines Schlüsselbeauftragten beauftragt werden. Insbesondere wird darauf geachtet, dass die sicheren Signaturerstellungseinheiten nicht entfernt bzw. vom Server getrennt werden können (z. B. indem als sichere Signaturerstellungseinheiten PCI-Karten verwendet werden oder indem Server und Signaturerstellungseinheit in einem gemeinsamen Behältnis versperrt werden).

Der Betreiber des Rechenzentrums ergreift Schutzmaßnahmen gegen unbefugten Zutritt, Einbruch und Diebstahl, zum Brandschutz, gegen Stromausfall und Wassereinbruch. Durch die redundante Verteilung auf zwei Rechenzentren wird darüber hinaus auch weitere Vorsorge gegen den Ausfall von Strom und Internetanbindung und gegen Elementarereignisse getroffen.

Die Atomuhren und deren NTP-Server sind in einem versperrten Raum untergebracht, zu dem nur Mitarbeiter der zuständigen Fachabteilungen sowie des beauftragten Sicherheitspersonals Zutritt haben. Der Raum ist durch eine Brandschutztüre gesichert. Im Raum befinden sich keine Arbeitsplätze, der Raum ist versperrt und wird im Rahmen von geregelten Arbeiten an den Systemen betreten. Die Schlüsselverwaltung erfolgt durch die für die Gebäudeverwaltung zuständige Abteilung.

Der GPS-Empfänger samt NTP-Server befindet sich in einem versperrten LAN-Schrank in einem versperrten Raum. Zum Raum haben nur Mitarbeiter der zuständigen Fachabteilungen sowie des beauftragten Sicherheitspersonals Zutritt, zum Schrank nur Mitarbeiter der für Netzwerktechnik und für die Betreuung des GPS- und Zeitempfängers zuständigen Fachabteilungen. Die Schlüsselverwaltung für den Raum erfolgt durch die für die Gebäudeverwaltung zuständige Abteilung, die Schlüsselverwaltung für den LAN-Schrank durch die für die Netzwerktechnik zuständiger Abteilung.

6.5 Organisatorische Sicherheitsmaßnahmen

Zu den Aufgaben der Schlüsselbeauftragten gehört die laufende Überwachung der Sicherheit der Server des Zeitstempeldienstes sowie der eingesetzten Technologien und Algorithmen. Insbesondere sind bei bekannt gewordenen Sicherheitslücken Security-Patches einzuspielen. Werden Umstände bekannt, denen zufolge einer der verwendeten Algorithmen nicht mehr als langfristig sicher erscheint, dann sind die entsprechenden Maßnahmen zur Änderung der verwendeten Algorithmen zu ergreifen (siehe oben 3.5). Besteht der Verdacht, dass eine Kompromittierung eingetreten ist oder dass Zeitstempel erstellt wurden, die um mehr als eine Sekunde von UTC abgewichen sind, dann sind die unten in 6.8 beschriebenen Maßnahmen zu ergreifen.

Im BEV ist ein dreistufiges Antivirenkonzept realisiert, welches Viren am Internet-Gateway, am Fileserver und an den Clients filtert. Die Server des Zeitstempeldienstes sowie der Datenbank werden darüber hinaus dadurch gegen Viren geschützt, dass nur ausgesuchte und auf Viren geprüfte Software installiert wird.

Datenträger werden gegen Beschädigung, Diebstahl und unbefugten Zugriff geschützt. Die Daten des sicheren Zeitstempeldienstes (Log-Dateien) werden in das allgemeine Datenbanksystem des BEV übernommen. Bei den Servern des Zeitstempeldienstes wird im Fall, dass Festplatten ausgetauscht werden, darauf geachtet, dass die Daten, insbesondere Passwörter und private Schlüssel (z. B. für den Zugriff der Software auf die sichere Signaturerstellungseinheit und für die Verwaltung der VPN-Tunnel) gelöscht oder ausgetauscht werden. Die privaten Schlüssel, mit denen Zeitstempel signiert werden, befinden sich ohnehin in eigenen Signaturerstellungseinheiten (siehe Kapitel 4).

Für alle Aufgaben im Zusammenhang mit dem sicheren Zeitstempeldienst werden klare Prozessbeschreibungen erstellt, insbesondere für die Konfiguration der Server des Zeitstempeldienstes und der sicheren Signaturerstellungseinheiten und für die Fehlerbehandlung. Die verschiedenen mit dem sicheren Zeitstempeldienst befassten

Fachabteilungen (insbesondere die für die Zeitgeber und für die Netzwerksicherheit verantwortlichen Abteilungen) haben die für den Zeitstempeldienst erforderlichen Tätigkeiten in ihre jeweiligen abteilungsinternen Dokumentationen eingearbeitet.

Im Zuge der Überwachung der Server und Applikationen und der Erstellung von Betriebsstatusberichten wird darauf geachtet, dass die Kapazität der Server und der Signaturerstellungseinheiten (insbesondere die leistbare Anzahl von Zeitstempeln pro Minute) sowie die Kapazität der Datenbank ausreichend dimensioniert ist. Im Fall, dass eine Systemerweiterung geplant werden sollte, wird der mit der Projektbetreuung des sicheren Zeitstempeldienstes betraute Mitarbeiter verständigt und ist für die Planung und das Projektmanagement der Systemerweiterung verantwortlich.

Für mögliche auftretende Fehler werden Prozessbeschreibungen zur Fehlerbehandlung erstellt. Zu diesen Fehlern gehört insbesondere der Ausfall eines von den Servern des Zeitstempeldienstes herangezogenen Zeitsignals, Fehlermeldungen betreffend die Plausibilität der Zeitsignale, Ausfälle eines Servers, Fehlermeldungen der Selbst-Tests der sicheren Signaturerstellungseinheit, Fehler beim Zugriff auf die Datenbank etc. Für Probleme der Datenbank, des Storage Area Network oder für Netzwerkprobleme werden die bereits bestehenden Prozeduren zur Fehlerbehandlung verwendet.

Die Server des Zeitstempeldienstes sowie die sicheren Signaturerstellungseinheiten werden ausschließlich für den sicheren Zeitstempeldienst eingesetzt. Für diese Komponenten werden eigene Sicherheitsmaßnahmen ergriffen, die in dieser Policy bzw. im Sicherheitskonzept für den sicheren Zeitstempeldienst des BEV beschrieben werden. Die Atomuhren und ihre NTP-Server, das Netzwerk, die Datenbank, das Storage Area Network und das Backupsystem werden gemeinsam für eine Vielzahl von Anwendungen des BEV genutzt.

6.6 Zugriffsschutz

Das interne Netzwerk des BEV wird durch Firewalls vor unbefugtem Zugriff von außen geschützt. Die sicherheitsrelevanten Netzwerkkomponenten befinden sich jeweils im Einflussbereich des BEV und werden von den Mitarbeitern der Abteilung Informationstechnik überwacht. Die Verbindung zwischen den NTP-Servern in Gebäude E und den Servern des Zeitstempeldienstes in den beiden Rechenzentren, weiters die Verbindung zwischen dem GPS-Empfänger in Gebäude A und den Servern des Zeitstempeldienstes wird zudem durch einen VPN-Tunnel geschützt.

Auf allen eingesetzten Systemen, insbesondere den Servern des Zeitstempeldienstes, den sicheren Signaturerstellungseinheiten, den NTP-Servern und der Datenbank, ist eine personen- oder rollenbezogene Anmeldung (in der Regel mittels Username und Passwort) erforderlich. Bei Personalwechsel werden alle der betreffenden Person bekannten Passwörter geändert. Insbesondere ist für alle administrativen Zugriffe auf einen der Server des Zeitstempeldienstes und für alle Vorgänge auf eine der sicheren Signaturerstellungseinheiten eine Anmeldung mittels Username und Passwort erforderlich.

Das Personal ist für seine jeweiligen Handlungen verantwortlich. Über alle sicherheitsrelevanten Vorgänge werden Protokolle oder automatisierte Event-Logs erstellt (siehe unten 6.11).

6.7 Vertrauenswürdige Systeme

Folgende Systeme sind für die Sicherheit des Zeitstempeldienstes von besonderer Bedeutung:

- Zeitgeber (Atomuhren und GPS-Empfänger)
- NTP-Server

- Server des Zeitstempeldienstes
- sichere Signaturerstellungseinheiten
- Netzwerkkomponenten, Firewall-Cluster
- Datenbankserver, Storage Area Network, Backupsysteme

Bei allen Geräten besteht das Risiko eines Ausfalls und somit einer Beeinträchtigung der Verfügbarkeit. Daher sind alle genannten Systeme redundant ausgeführt (mit Ausnahme des GPS-Empfängers, der aber seinerseits nur als Ersatz-Zeitgeber bei einem Ausfall der Verbindung zu den Atomuhren eingesetzt wird).

Weiters besteht bei allen Geräten das Risiko einer Beeinträchtigung der Integrität, z. B. durch Softwarefehler, Viren etc. Um diesem Risiko vorzubeugen, müssen Änderungen vor ihrer Implementierung auf mögliche Sicherheitsprobleme geprüft werden. Bei den Servern des Zeitstempeldienstes fällt dies in den Aufgabenbereich der Schlüsselbeauftragten, bei den anderen Systemen in den Aufgabenbereich der jeweils zuständigen Fachabteilung. Auf allen genannten Servern wird nur Software installiert, die für die jeweiligen Server benötigt wird. Auf den Servern des Zeitstempeldienstes darf nur Software installiert werden, die für den Zeitstempeldienst benötigt wird. Auf den sicheren Signaturerstellungseinheiten darf nur die von der Bescheinigung bzw. dem Gutachten der Bestätigungsstelle umfasste Softwareversion eingesetzt werden, diese muss auch so konfiguriert sein, dass ein nachträglicher Wechsel der Software nicht möglich ist, ohne dass die gespeicherten Schlüssel unwiederbringlich gelöscht werden.

Bei der sicheren Signaturerstellungseinheit muss vor allem dem Risiko vorgebeugt werden, dass der private Schlüssel die Signaturerstellungseinheit verlässt oder daraus ausgelesen werden kann. Daher werden ausschließlich technische Komponenten verwendet, welche entsprechend den in oben in 4.1 genannten Kriterien von einer Bestätigungsstelle geprüft wurden. Außerdem werden die Geräte so konfiguriert, dass ein Schlüsselexport nicht möglich ist.

Bei der Datenbank, dem Storage Area Network und dem Backupsystem muss gegen Verletzungen der Vertraulichkeit vorgebeugt werden. Dies wird durch Zutritts- und Zugriffskontrollen gewährleistet.

6.8 Elementarereignisse und Kompromittierung

Gegen Elementarereignisse wird vorgesorgt, indem alle wichtigen Komponenten doppelt ausgeführt werden. Bei einem Ausfall eines der beiden Rechenzentren kann der sichere Zeitstempeldienst samt der Datenbank für die Log-Dateien unbeeinträchtigt im anderen Rechenzentrum weiterbetrieben werden. Bei einem Ausfall der Verbindung zu den Atomuhren in Gebäude E kann das Zeitsignal von einem GPS-Empfänger in Gebäude A bezogen werden.

Da sämtliche Komponenten des sicheren Zeitstempeldienstes und der Infrastruktur, auf welcher er beruht (Netzinfrastruktur, Zeitgeber ...) sorgfältig dokumentiert werden, kann auch bei einem Totalausfall der Dienst wiederhergestellt werden.

Im Fall, dass ein privater Schlüssel verloren wird (z. B. wegen eines Ausfalls einer Signaturerstellungseinheit) wird ein neues Schlüsselpaar erstellt (siehe oben 4.4). Ein Backup der privaten Schlüssel existiert nicht (siehe oben 4.2).

Wenn festgestellt wird, dass unkorrekte Zeitstempel ausgestellt wurden (insbesondere Zeitstempel mit einer Abweichung von mehr als einer Sekunde von UTC), dann wird die auf die Zeitstempel vertrauende Öffentlichkeit darüber informiert.

Im Fall einer schwerwiegenden Beeinträchtigung (Kompromittierung) der Sicherheitsvorgaben dieser Policy wird die Ausgabe von Zeitstempeln umgehend eingestellt. Entsprechend der Schwere des Falles wird die Öffentlichkeit informiert.

Besteht die berechtigte Befürchtung, dass ein privater Schlüssel des Zeitstempeldienstes gestohlen oder gebrochen wurde, dann wird die Ausgabe von Zeitstempeln mit diesem Schlüssel umgehend eingestellt und das für den Schlüssel ausgestellte Zertifikat wird widerrufen. In einem solchen Fall erfolgt jedenfalls eine Information an die Öffentlichkeit.

Bei allen genannten Informationsmaßnahmen wird der genaue Umfang der Information entsprechend der Schwere des Falles und den Auswirkungen auf die dem BEV bekannten Nutzungen des sicheren Zeitstempeldienstes abgestimmt. Das BEV wird jedenfalls die ihm bekannten Nutzer informieren, soweit deren E-Mail-Adressen bekannt gegeben wurden. Die Information soll insbesondere Angaben zur Auswirkung des Zwischenfalls auf die Langzeitsicherheit der erstellten Zeitstempel enthalten.

6.9 Einstellung des Betriebs

Das BEV behält sich die Möglichkeit vor, den sicheren Zeitstempeldienst jederzeit ohne Angaben von Gründen einzustellen. Davon abweichend kann das BEV Service Level Agreements mit bestimmten Nutzern abschließen, in denen es eine bestimmte Verfügbarkeit über einen gewissen Zeitraum hin zusichert. Über diese vertraglichen Verpflichtungen hinaus besteht keine Verpflichtung oder Haftung für die weitere Erbringung des Dienstes.

Bei der Einstellung der Dienstes wird für alle noch gültigen Zertifikate der Server des sicheren Zeitstempeldienstes ein Widerruf veranlasst. Alle privaten Schlüssel werden unwiederbringlich gelöscht (siehe oben 4.5). Sollte das BEV für die Server des Zeitstempeldienstes eigene Zertifikate ausgestellt haben, dann würde das entsprechende Sicherheits- und Zertifizierungskonzept regeln, wie lange die Widerrufslisten für die Zertifikate online abrufbar gehalten werden (mindestens jedenfalls bis zum Ende der Gültigkeitsdauer der jeweiligen Zertifikate).

Alle bekannten Nutzer des sicheren Zeitstempeldienstes werden von der Einstellung des Betriebs verständigt. Weiters wird das BEV auf seiner Website über die Einstellung des Betriebs informieren und die für die Langzeitüberprüfung von Zeitstempeln erforderlichen Informationen (insbesondere Zertifikate) bis mindestens drei Jahre nach der Einstellung des Dienstes abrufbar halten.

Auch über die Einstellung des Betriebs hinaus wird die Dokumentation des sicheren Zeitstempeldienstes archiviert (siehe unten 6.11).

6.10 Übereinstimmung mit rechtlichen Anforderungen

Das BEV ist eine dem Bundesministerium für Wirtschaft und Arbeit nachgeordnete Bundesbehörde und hat seinen Sitz in Wien. Es unterliegt somit österreichischem Recht und der Gerichtsstand ist (soweit nicht besondere Bestimmungen zur Anwendung kommen) Wien.

Als Anbieter eines sicheren Zertifizierungsdienstes ist das BEV verpflichtet, insbesondere das Signaturgesetz und die Signaturverordnung sowie das Datenschutzgesetz 2000 in der jeweils geltenden Fassung zu beachten. Der sichere Zeitstempeldienst und alle seine Änderungen werden der Telekom-Control-Kommission als Aufsichtsstelle für elektronische Signaturen angezeigt und unterliegen deren Aufsicht.

In den Log-Dateien und bei der Nutzerverwaltung bzw. einer allfälligen Abrechnung werden personenbezogene Daten verwaltet. Diese werden durch dem Stand der Technik entsprechende Datensicherheitsmaßnahmen geschützt.

6.11 Protokollierung und Archivierung

Über die folgenden Vorgänge werden von den handelnden Personen Protokolle erstellt und gesammelt archiviert:

- Aufsetzen der Server des Zeitstempeldienstes, Installation von Software, Veränderungen an der installierten Software. Möglichst genau soll dabei auch jeweils festgehalten werden, wann solche Veränderungen wirksam wurden.
- Sämtliche nicht-automatisierten Aktionen an den sicheren Signaturerstellungseinheiten, insbesondere das Initialisieren, Konfigurieren und die Generierung von Schlüsselpaaren sowie das Löschen von Schlüsseln und die Außerbetriebnahme der Geräte. Weiters wird auch der Lebenszyklus der für diese Schlüssel ausgestellten Zertifikate dokumentiert (Informationen zur Ausstellung der Zertifikate sowie zu einem allfälligen Widerruf) und die Zertifikate werden archiviert.

Diese Protokolle werden in das allgemeine Aktensystem des BEV aufgenommen und für unbestimmte Zeit aufbewahrt.

Über die folgenden Vorgänge werden im Datenbanksystem automationsunterstützt Log-Einträge erzeugt. Diese Log-Daten werden mindestens drei Jahre lang aufbewahrt:

- Start und Stop der Software des Zeitstempeldienstes
- Fehlermeldungen der Server des Zeitstempeldienstes, insbesondere Fehlermeldungen betreffend die Zeitsynchronisation
- Log-Einträge zu jedem einzelnen erzeugten Zeitstempel, die unter anderem die Seriennummer, den genauen Zeitpunkt und den Hashwert des zeitgestempelten Dokumentes enthalten.

Das Aktensystem des BEV sowie das verwendete Datenbanksystem und die Backupstrategie des BEV schützen die protokollierten Daten wirksam gegen nachträgliche Veränderung, Datenverlust und unbefugten Datenzugriff.

Auskunft über protokollierte Log-Daten wird nur im Rahmen der Gesetze, insbesondere des Datenschutzgesetzes 2000, erteilt. Insbesondere wird Auskunft über Log-Daten zu einem bestimmten Zeitstempel nur dann erteilt, wenn ein rechtliches Interesse an der Auskunft geltend gemacht wird, etwa weil das mit dem Zeitstempel versehene Dokument Gegenstand eines Rechtsstreits ist (siehe oben 3.12).

7 Anhang

7.1 Begriffsbestimmungen und Abkürzungen

Begriff / Abkürzung	Definition, Beschreibung
A-SIT	Zentrum für sichere Informationstechnologie – Austria, http://www.a-sit.at/
ASN.1	Abstract Syntax Notation 1. In dieser Notation werden unter anderem X.509-Zertifikate codiert.
Aufsichtsstelle	In Österreich ist die Telekom-Control-Kommission mit den Aufgaben einer Aufsichtsstelle für elektronische Signaturen betraut.
BEV	Bundesamt für Eich- und Vermessungswesen
BIPM	Bureau International des Poids et Mesures
C	Country, Staat, z. B.: C=AT im Distinguished Name eines Zertifikats
CN	Common Name, z. B.: CN=Vorname Nachname im Distinguished Name eines Zertifikats
Common Criteria	Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik
CWA	CEN Workshop Agreement, ein Standard der Standardisierungsorganisation CEN
Distinguished Name	Die unter anderem in Zertifikaten und Zeitstempeln verwendete, gegliederte Namensschreibweise, z. B. in der Form C=AT, O=Name der Organisation, CN=Vorname Nachname
echt, Echtheit	Eine elektronische Signatur ist echt, wenn sie von demjenigen stammt, der als Signator angezeigt wird.
ETSI	European Telecommunications Standards Institute
FIPS	Federal Information Processing Standard
GPS	Global Positioning System, ein Satellitennetzwerk das für die genaue Ortsbestimmung entwickelt wurde, aber auch als Zeitgeber verwendet werden kann.
gültig, Gültigkeit	Zertifikate haben einen Gültigkeitszeitraum. Ein Zertifikat verliert seine Gültigkeit, wenn es widerrufen wurde. Eine elektronische Signatur ist gültig, wenn sie innerhalb des Gültigkeitszeitraums des Zertifikates, auf dem sie beruht, erstellt wurde. Die Überprüfung der Gültigkeit der Signatur ist ein wichtiger Schritt bei der Überprüfung der Echtheit.
Hashverfahren, Hashwert	Ein Hashverfahren ist eine mathematische Funktion, mit der beliebige Dokumente auf einen Wert bestimmter Länge (z. B.: 256 Bit), den Hashwert abgebildet werden können. Von einem Hashverfahren wird verlangt, dass es unumkehrbar ist (d. h. aus dem Hashwert können keine Rückschlüsse auf das Dokument gezogen werden) und dass es in der Praxis ausgeschlossen ist, dass zwei Dokumente den selben Hashwert haben. Beispiele für Hashverfahren sind SHA-256 und RIPEMD-160.
ITSEC	Kriterien für die Bewertung der Sicherheit von Informationstechnik
LAN	Local Area Network
NTP	Network Time Protocol, das am stärksten verbreitete Protokoll zur Synchronisation von Uhren über das Internet.

O	Organisation, z. B.: O=Firmenname im Distinguished Name eines Zertifikats
OID	Object Identifier. Wird in der ASN.1-Notation zur Benennung beliebiger Inhalte verwendet, z. B. als Referenz auf die Policy, auf deren Grundlage ein Zeitstempel oder ein Zertifikat ausgestellt wurde.
PCI	Peripheral Component Interconnect
Policy	Hier: ein Regelwerk, das einen Zeitstempeldienst (oder einen anderen Zertifizierungsdienst) beschreibt und zu dessen Einhaltung sich der Anbieter des Dienstes selbst verpflichtet. Meist wird die Policy veröffentlicht und in den ausgestellten Zeitstempeln (bzw. Zertifikaten) wird mit einem OID auf die jeweilige Policy verwiesen.
RFC	Request for Comments, ein Dokument mit dem ein Standard für das Internet festgelegt wurde
RIPEMD-160	RACE Integrity Primitives Evaluation Message Digest, ein Hashverfahren
RSA	Das am stärksten verbreitete asymmetrische kryptographische Verfahren zur Erstellung elektronischer Signaturen, benannt nach den Anfangsbuchstaben der Entwickler, Rivest, Shamir und Adleman.
RTR-GmbH	Rundfunk und Telekom Regulierungs-GmbH, der Geschäftsapparat der Telekom-Control-Kommission als Aufsichtsstelle für elektronische Signaturen
Schlüssel	Die Information, die bei einem kryptographischen Verfahren zur Verschlüsselung bzw. Entschlüsselung (oder zur Erstellung bzw. zum Prüfen von Signaturen verwendet wird). Bei einem aymmetrischen kryptographischen Verfahren verwendet jeder Nutzer ein Schlüsselpaar. Der private Schlüssel kann zur Erstellung von Signaturen, der öffentliche Schlüssel zur Prüfung dieser Signaturen verwendet werden.
SHA	Secure Hash Algorithm, eine Familie von Hashverfahren. Das am stärksten verbreitete Hashverfahren SHA-1 (160 Bit) wird zunehmend als nicht mehr ausreichend sicher angesehen, weshalb SHA-256, SHA-384 und SHA-512 (256, 384 bzw. 512 Bit) verwendet werden.
Signatur	Elektronische Daten, die einem elektronischen Dokument hinzugefügt werden und mit denen die Identität des Signators, d. h. des Erstellers der Signatur bescheinigt wird.
Signaturgesetz, SigG	Bundesgesetz über elektronische Signaturen (Signaturgesetz – SigG), BGBl. I Nr. 190/1999 in der geltenden Fassung
Signaturverordung, SigV	Verordnung des Bundeskanzlers über elektronische Signaturen (Signaturverordnung – SigV), BGBl. II Nr. 30/2000 in der geltenden Fassung
SZSD	Sicherer Zeitstempeldienst
TKK	Telekom-Control-Kommission, die österreichische Aufsichtsstelle für elektronische Signaturen. Die RTR-GmbH fungiert als Geschäftsapparat der TKK.
TS	Technical Standard, z. B. ETSI TS 102 023
UTC	Coordinated Universal Time, Koordinierte Weltzeit. Die mitteleuropäische Zeit weicht eine Stunde von UTC ab, die mitteleuropäische Sommerzeit zwei Stunden. UTC basiert auf Atomuhren, alle Sekunden sind gleich lang. Um Unregelmäßigkeiten der Erdrotation auszugleichen werden manchmal Schaltsekunden eingefügt oder gestrichen. Im Gegenzug dazu basiert die Universal Time (UT) auf der Erdrotation. Die Sekunden der UT haben geringfügig unterschiedliche Länge.
UTC(BEV)	Die von den Atomuhren des BEV repräsentierte Form der UTC.

VPN	Virtual Private Network
Widerruf, Widerrufsliste	Zertifikate können widerrufen werden und verlieren damit schon vor dem Ablauf ihres im Zertifikat ausgewiesenen Gültigkeitszeitraumes ihre Gültigkeit. In der Regel verbreitet ein Zertifizierungsdienst Informationen über widerrufene Zertifikate in Form der Widerrufsliste, einer Liste aller widerrufenen Zertifikate.
Wurzelzertifikat	Das oberste Zertifikat in einer Zertifikatshierarchie. Ein Wurzelzertifikat ist selbstsigniert, basiert also auf sich selbst und nicht auf einem anderen Zertifikat.
X.509	Der am weitesten verbreitete Standard zur Codierung von Zertifikaten. X.509 verwendet ASN.1 als Notation.
Zeitstempeldienst	Eine Dienstleistung, die Dokumente mit Zeitstempeln versieht, d. h. mit einer Zeitangabe und einer Signatur, welche das Dokument (bzw. seinen Hashwert) und die Zeitangabe umfasst. Ein Zeitstempel bescheinigt, dass das Dokument zu einem bestimmten Zeitpunkt bereits vorgelegen ist und danach nicht mehr verändert wurde.
Zeitstempeldienst, sicherer	Ein sicherer Zeitstempeldienst ist ein Zeitstempeldienst, der bestimmte hohe Anforderungen des Signaturgesetzes und der Signaturverordnung erfüllt, wie sie auch im vorliegenden Dokument beschrieben sind.
Zertifikat	Eine elektronische Bescheinigung, die ein bestimmtes Schlüsselpaar (und somit alle mit dem privaten Schlüssel dieses Schlüsselpaars erzeugten Signaturen bzw. Zeitstempel) einer bestimmten Person zuordnet.