BSI

Bundesamt für Sicherheit in der Informationstechnik

SPEZIFIKATION ZUR ENTWICKLUNG INTEROPERABLER VERFAHREN UND KOMPONENTEN NACH SIGG/SIGV

SIGNATUR-INTEROPERABILITÄTSSPEZIFIKATION

SIGI

ABSCHNITT A4

ZEITSTEMPEL

STAND: 31. MÄRZ 1999

VERSION 3.0

Godesberger Allee 183, 53175 Bonn - Postfach 20 03 63, 53133 Bonn
Telefon: (0228) 9582 - 0, Telefax: (0228) 9582 - 400
Internet: www.bsi.bund.de

ABSCHNITT A4

ZEITSTEMPEL

Fritz Bauspieß, Jobst Biester

Secorvo Security Consulting GmbH
Albert-Nestler-Straße 9, D-76131 Karlsruhe

Tel. +49 721 6105-452
Fax +49 721 6105-455

E-Mail: info@secorvo.de
http://www.secorvo.de

Inhaltsübersicht

Abkürzungen

ASN.1	Abstract Syntax Notation 1
BER	Basic Encoding Rules
BSI	Bundesamt für Sicherheit in der Informationstechnik
CER	Canonical Encoding Rules
CMS	Cryptographic Message Syntax
DER	Distinguished Encoding Rules
E-Mail	Electronic Mail
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
ITU	International Telecommunication Union
ITU-T	ITU - Telecommunication Sector
MIME	Multipurpose Internet Mail Extensions
OID	Object Identifier
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
RFC	Request for Comments
S/MIME	Secure MIME
SigG	Signaturgesetz
SigI	Signatur-Interoperabilitätsspezifikation
SigV	Signaturverordnung
SMTP	Simple Mail Transfer Protocol
TSA	Time Stamp Authority
TCP	Transport Control Protocol
TDA	Temporal Data Authority
TSA	Time Stamp Authority
TSP	Time Stamp Protocol
URI	Universal Resource Identifier
UTC	Universal Time Code
WWW	World Wide Web
ZS	Zertifizierungsstelle

1 Zusammenfassung

Der Zeitstempeldienst ist eine unverzichtbare Komponente einer Zertifizierungstelle (ZS), da die vom Zeitstempeldienst ausgestellten Zeitstempel unverzichtbare Beweismittel bei der Verwendung digitaler Signaturen nach dem Signaturgesetz (SigG) sind. Zeitstempel dienen allgemein dem Nachweis des Zeitpunktes eines Ereignisses. Ein Zeitstempel im Sinne des Signaturgesetzes ist eine mit einer digitalen Signatur versehene Bescheinigung einer ZS, daß ihr bestimmte digitale Daten zu einem bestimmten Zeitpunkt vorgelegen haben (§ 2 Abs. 4 SigG).

Die vorliegende Spezifikation enthält die Anforderungen an den Zeitstempeldienst und die Applikationen[1], die erfüllt werden müssen, damit der Nutzer den Zeitstempeldienst zweckentsprechend in Übereinstimmung mit SigG und der Signaturverordnung (SigV) verwenden kann und die Interoperabilität zwischen den beteiligten Instanzen gewährleistet wird. Die Spezifikation enthält darüber hinaus weitere optionale Anteile und Empfehlungen.

Die Spezifikation berücksichtigt den internationalen Standard für den Zeitstempeldienst einer Internet-PKI der PKIX-Arbeitsgruppe, der in [PKIX-TSP 98] veröffentlicht ist. Aus den in diesem Standard spezifizierten Anforderungen und aus den Anforderungen aus SigG/SigV werden die Anforderungen an den Zeitstempeldienst und die Applikationen abgeleitet.

Auch die beschriebenen Abläufe zwischen den Instanzen, die verwendeten Datenstrukuren und die Transportprotokolle entsprechen im wesentlichen dem genannten internationalen Standard.

Dieser Standard ist jedoch als Interoperabilitätsspezifikation nur bedingt geeignet, da er keine Aussage darüber enthält, welche der Anteile der umfangreichen Spezifikation zu realisieren sind. Die vorliegende Spezifikation trifft hier eindeutige Regelungen, die die Interoperabilität gewährleisten.

Die weiteren Kapitel der Spezifikation haben folgenden Inhalt:

- Kapitel 2: Definitionen der verwendeten Begriffe.
- Kapitel 3: Überblick über den Zweck eines Zeitstempels.
- Kapitel 4: Gestaltungsmerkmale, soweit sie für die vorliegende Spezifikation von Bedeutung sind und Abgrenzung zu anderen Dienstleistungen.
- Kapitel 5: Überblick über die Abläufe bei einem Zeitstempelantrag.
- Kapitel 6: Formate der Nachrichten, die zwischen den Instanzen ausgetauscht werden.
- Kapitel 7: Transportprotokolle, die zum Austausch der Nachrichten verwendet werden.
- Kapitel 8: Datenstruktur für die gemeinsame Speicherung von digitalen Daten und Zeitstempeln und Vorschlag für Dateinamenserweiterungen.
- Kapitel 9: Literaturverzeichnis.
- Anlage A: Verwendete ASN.1 Definitionen in alphabetischer Ordnung.
- Anlage B: Objektbezeichner.

[1] Applikation = Komponente auf Nutzerseite

2 Begriffsdefinitionen

Die folgenden Begriffe haben in der vorliegenden Spezifikation die hier definierte Bedeutung:

- **Applikation (Application)**

  Die Applikation ist die technische Komponente, die der Nutzer verwendet, um digitale Zeitstempelanträge an den Zeitstempeldienst zu richten und Antworten des Zeitstempeldienstes entgegenzunehmen und auszuwerten. Anstelle von Applikation werden häufig auch die Begriffe Client oder Anwenderinfrastruktur verwendet.

- **Digitale Daten als Element des Zeitstempels**

  Gemäß § 2 Abs. 4 SigG können Zeitstempel für beliebige digitale Daten beantragt werden. Es bestehen somit keine Beschränkungen hinsichtlich der Art der Daten. Insbesondere findet keine Beschränkung auf digital signierte Daten statt, auch wenn dies der Hauptanwendungsbereich ist.

  Im Zeitstempel sind die digitalen Daten stets in Form von Hashwerten enthalten, die von den Nutzern mittels starker Hashfunktionen generiert werden.[2]

- **Nutzer**

  Der Zeitstempeldienst generiert Zeitstempel auf Antrag einer Nutzers. Nutzer kann gemäß § 9 SigG jedermann sein. Der Zeitstempeldienst darf seine Dienstleistung nicht auf einen bestimmten Personenkreis beschränken.[3]

- **Signaturgesetz-konform**

  Die vorliegende Spezifikation enthält Anforderungen an Applikationen und den Zeitstempeldienst, die erfüllt werden müssen, damit der Nutzer den Zeitstempeldienst zweckentsprechend in Übereinstimmung mit dem Signaturgesetz verwenden kann und die Interoperabilität gewährleistet wird (Mininalanforderungen). Die Spezifikation enthält darüber hinaus weitere optionale Anteile und Empfehlungen.

  Ein Zeitstempeldienst und eine Applikation wird als Signaturgesetz-konform im Sinne der vorliegenden Spezifikation bezeichnet, wenn alle Minimalanforderungen erfüllt werden.

- **Starke Hashfunktionen**

  Eine Hashfunktion bildet binäre Daten beliebiger Länge auf einen binären String fester Länge ab, der Hashwert genannt wird. Da der Hashwert in der Regel wesentlich kürzer ist als die Ausgangsdaten, findet eine Komprimierung statt. Dies hat zwangsläufig zur Folge, daß mehrere binäre Daten auf den gleichen Hashwert abgebildet werden.

  Eine starke Hashfunktion muß kollisionsresistent sein, d.h. es muß praktisch unmöglich sein, zwei verschiedene binäre Daten zu finden, die den gleichen Hashwert haben.[4]

---

2 Die Begründung hierfür wird in Kapitel 4.2 gegeben.

3 In der Begründung zu § 9 SigG wurde angegeben: „Einen Zeitstempel kann jedermann verlangen, der Daten erzeugt oder dem fremde Daten vorliegen, bei denen er aus Beweisgründen ein Interesse daran hat“ (vgl. Kapitel 6.5.1 [MKAT 97]). Wie bei den Auskünften des Verzeichnisdienstes hat jedermann einen Anspruch auf einen Zeitstempel. Insbesondere kann der Zeitstempeldienst im Allgemeinen nicht davon ausgehen, daß er nur Zeitstempelanträge von Personen erhält, zu denen bereits eine Vertragsbeziehung besteht.

4 Eine Übersicht der geeigneten Krypto-Algorithmen ist im Bundesanzeiger veröffentlicht (s. § 17 Abs. 2 SigV). Z.Z. sind die Hashfunktionen SHA-1 und RIPEMD-160 zugelassen, die bis Ende 2003 als geeignet angesehen werden (s. [BAZ140298]).

- **Unterstützen**

  Der Begriff „Unterstützen“ wird verwendet, um den Begriff „Signaturgesetz-konform“ hinsichtlich der Datenformate zu beschreiben. Die Forderung nach Unterstützung eines definierten Datenformats bedeutet, daß das Datenformat erkannt und ausgewertet bzw. generiert werden können muß. Wenn die Unterstützung eines Datenformates gefordert wird, gehört dies stets zu den Minimalanforderungen.

- **Zeitstempel (Time Stamp Token)**

  Ein Zeitstempel besteht entsprechend Kapitel 1 [PKIX-TSP 98] in der Regel aus drei Elementen, einer Zeitangabe, digitalen Daten und einer digitalen Signatur. Durch die gemeinsame Signatur der digitalen Daten und der Zeitangabe werden diese Elemente miteinander verknüpft. Das Ziel dieser Verknüpfung ist die Nachweis, daß die digitalen Daten zum angegebenen Zeitpunkt existiert haben.

  Ein Zeitstempel kann jede Art von digitalen Daten enthalten, auch wenn der Hauptanwendungszweck die Zeitstempelung digital signierter Daten ist. Ein Zeitstempel gemäß [PKIX-TSP 98] setzt auch nicht voraus, daß neben der Zeitangabe überhaupt digitale Daten signiert werden. In diesem Sonderfall liefert der Zeitstempel lediglich eine digital signierte Zeitangabe, die z.B. zum Abgleich der lokalen Zeit verwendet werden kann.

  Ein Zeitstempel muß stets von einer vertrauenswürdigen Instanz ausgestellt werden. Bei Zeitstempeln nach Signaturgesetz muß diese vertrauenswürdige Instanz eine ZS sein (s. § 2 Abs. 4 SigG).

  Die Definition des Zeitstempels in § 2 Abs.2 SigG setzt voraus, daß der ZS die digitalen Daten vorgelegt werden. Es darf sich somit insbesondere nicht um digitale Daten der ZS selbst handeln, deren Existenz zu einem bestimmten Zeitpunkt durch eine Zeitangabe gesichert werden soll. Aus diesem Grund sind z.B. die Auskünfte des Verzeichnisdienstes gemäß § 5 Abs. 1 S. 2 SigG keine Zeitstempel, obwohl sie digitale Daten und eine Zeitangabe enthalten, den Zeitpunkt der Generierung der Auskunft.[5]

- **Zeitstempelantrag (Time Stamp Request)**

  Der Zeitstempeldienst generiert Zeitstempel auf Antrag des Nutzers.

- **Zeitstempeldienst (Time Stamp Authority)**

  Der Zeitstempeldienst ist der Dienst einer Zertifizierungsstelle, dessen Aufgabe die Generierung von Zeitstempeln ist. Jede Zertifizierungsstelle muß über einen Zeitstempeldienst verfügen. Der Zeitstempeldienst erbringt eine Pflichtdienstleistung nach § 9 SigG.

  Mit dem Begriff Zeitstempeldienst wird auch die technische Einrichtung zur Generierung von Zeitstempeln bezeichnet.

---

[5] Da dem Verzeichnisdienst implizites Vertrauen entgegengebracht wird, stets die korrekte Zeit zu verwenden, ist ein Zeitstempel nicht erforderlich. Bei Verwendung des Begriffs Zeitstempel in einem weiteren Sinn wird zwischen sog. äußeren Zeitstempeln (den Zeitstempeln im Sinne der vorliegenden Spezifikation) und inneren Zeitstempeln (Zeitangaben in digitalen Daten der ZS selbst) unterschieden.

- **Zeitdatendienst (Temporal Data Authority)**

  Der Zeitdatendienst ist in Kapitel 1 [PKIX-TSP 98] definiert. Seine Aufgabe ist die Bereitstellung zusätzlicher zeitbezogener Daten, die vom Zeitstempeldienst auf Antrag in den Zeitstempel einbezogen werden. Durch die Aufnahme zeitbezogener Daten in den Zeitstempel können digitale Daten mit bestimmten, nicht exakt vorhersagbaren Ereignissen wie z.B. Börsen- oder Wetterdaten verknüpft werden.

  Ein Zeitdatendienst wird vom Signaturgesetz nicht gefordert und gehört daher nicht zu den Pflichtdienstleistungen einer Signaturgesetz-konformen ZS. Die vorliegende Spezifikation berücksichtigt den Zeitdatendienst als optionale Sicherheitskomponente. Eine ZS muß jedoch keinen Zeitdatendienst anbieten. Ein Nutzer hat auch keinen Anspruch darauf, daß der Zeitstempeldienst einer ZS Zeitdaten in einen beantragten Zeitstempel einbezieht.

3 Zweck des Zeitstempels

Ein Signaturgesetz-konformer Zeitstempeldienst muß seine Dienstleistung den Nutzern in der Form erbringen, daß der Beantragung eines Zeitstempels angestrebte Zweck erreicht wird. Der Zweck des Zeitstempels wird in § 4 Abs. 1 Nr. 5 SigV allgemein beschrieben. Ein Zeitstempel sollte beantragt werden, soweit „für die Verwendung signierter Daten ein Zeitpunkt von erheblicher Bedeutung sein kann“.

Der Zweck des Zeitstempels ist jedoch nicht auf digitale Signaturen beschränkt. Zeitstempel können immer dann zu Beweiszwecken verwendet werden, wenn der Zeitpunkt strittig ist, zu dem ein bestimmtes Ereignis eingetreten ist. Beispiele hierfür sind der Nachweis der Einhaltung eines Abgabetermins oder Laboraufzeichnungen im Falle eines Patentstreites.

Der Zweck des Zeitstempel wird im folgenden konkretisiert. Es wird dargestellt, wie ein Zeitstempel den Empfänger einer digital signierten Nachricht dagegen schützt, daß er die Echtheit der Nachricht zwar zum Zeitpunkt des Empfangs, aber nicht mehr zu einem späteren Zeitpunkt beweisen kann. Es wird auch dargestellt, wie der Zeitstempel den Absender der Nachricht davor schützt, daß der Empfänger sie zu Unrecht als ungültig zurückweist. Anschließend wird die normale Nutzung des Zeitstempeldienstes beschrieben.

3.1 Schutz des Empfängers einer Nachricht

Eine digitale Signatur kann den Empfänger einer Nachricht dagegen schützen, daß ihre Echtheit vom Absender erfolgreich bestritten werden kann. Der tatsächliche Absender soll durch seine Signatur an die Erklärung gebunden sein, die in der Nachricht enthalten ist.

Der Nachweis der Echtheit wird vom Empfänger der Nachricht durch Prüfung der Gültigkeit der digitalen Signatur geführt. Der Empfänger muß darauf vertrauen können, daß das festgestellte positive Ergebnis der Gültigkeitsprüfung zu jedem späteren Zeitpunkt reproduzierbar ist.[6] Deshalb muß die Reproduzierbarkeit nachhaltig auch noch zu einem Zeitpunkt gegeben sein, der außerhalb des Gültigkeitszeitraums des Zertifikats für den Schlüssel liegt, mit dem die digitale Signatur generiert wurde. Sie darf auch nicht dadurch verloren gehen, daß das Zertifikat durch Sperrung ungültig geworden ist.

Die geforderte Reproduzierbarkeit des Ergebnisses der Gültigkeitsprüfung ist ohne einen Zeitstempel in der Regel nicht nachhaltig gewährleistet, da sich der tatsächliche Zeitpunkt der

6 Falls die Nachricht z.B. rechtserheblich ist, will es sie ggf. zu einem späteren Zeitpunkt als Beweismittel vor Gericht vorlegen können.

Generierung der digitalen Signatur ohne einen Zeitstempel nicht zuverlässig nachweisen läßt.[7] Der Absender der Nachricht könnte deshalb z.B. im Falle einer zwischenzeitlichen Sperrung seines Signaturschlüssel-Zertifikats wegen Kompromittierung des Schlüssels unwiderlegbar behaupten, daß die Signatur nicht vor ihm sondern von einer anderen Person stammt (also unecht ist). Dieser Einwand kann in der Regel zur dann widerlegt werden, wenn der Absender durch den Zeitstempel nachweisen kann, daß die Signatur bereits vor dem Sperrzeitpunkt erfolgt ist.[8]

Der Empfänger einer Nachricht sollte sich daher einen Zeitstempel beschaffen, wenn er diese ggf. später zu Beweiszwecken benötigt. Der Zeitstempel hilft ihm, den Nachweis des Zeitpunktes der Signaturbildung und damit mittelbar der Echtheit der Signatur zu führen.

Durch den Zeitstempel bescheinigt die ZS, daß ihr die signierten Daten zu einem bestimmten Zeitpunkt vorgelegen haben, also zu dem Zeitpunkt existent waren. Da die ZS eine vertrauenswürdige Instanz ist, ist der Zeitstempel geeignet, den Beweis für die Existenz zu einem definierten Zeitpunkt zu erbringen.[9]

Falls zu dem im Zeitstempel bescheinigten Zeitpunkt die Signatur bei einer Prüfung als gültig ausgewiesen wird, kann der Empfänger unter Hinweis auf den Zeitstempel jederzeit die Gültigkeit der Signatur beweisen.

3.2 Schutz des Absenders einer Nachricht

Ein Zeitstempel kann auch den Absender einer Nachricht dagegen schützen, daß der Empfänger diese als ungültig zurückweist. Falls der Signaturschlüssel des Absenders auf Grund einer Kompromittierung gesperrt werden muß, nachdem er die Nachricht generiert hat aber bevor der Empfänger die Gültigkeit der Nachricht geprüft hat, wird der Empfänger sie zurückweisen, wenn er nicht sicher ist, daß die Nachricht vor dem Sperrzeitpunkt generiert wurde. Ein Zeitstempel bietet dem Empfänger diese Sicherheit. Der Empfänger wird die Nachricht nicht zurückweisen, falls das Ausstellungsdatum durch einen Zeitstempel gesichert ist, der vor dem Sperrzeitpunkt liegt.

Falls der Absender sicher sein will, daß der Empfänger seine Nachricht nicht ggf. als ungültig zurückweist, kann er sich einen Zeitstempel beschaffen und die Nachricht zusammen mit dem Zeitstempel und einer Quittungsanforderung an den Empfänger senden. Nach Eingang der Quittung ist der Absender sicher, daß anschließende Sperrungen seines Signaturschlüssel-Zertifikates keine Auswirkungen auf die Prüfung der Gültigkeit der Signatur der Nachricht durch den Empfänger haben. Der Empfänger kann dann nicht mehr mit Erfolg bestreiten, eine gültige Nachricht erhalten zu haben.

---

7 Der Nachweis dieses Zeitpunktes läßt sich nur bei vertrauenswürdigen Instanzen dadurch führen, daß er Teil der durch den Absender signierten Daten ist (s. Kapitel 4.2.4 [BSI-SIG 99]). Andernfalls kann ein Verifizierer im Allgemeinen nicht sicher sein, daß der angegebene Zeitpunkt korrekt ist. Rückdatierungen können nicht ausgeschlossen werden.

8 Der Ersteller einer digitalen Signatur könnte dieses Beweisproblem gezielt ausnutzen, um die Folgen einer von ihm abgegebenen Erklärung nicht eintreten zu lassen. Er könnte die Sperrung seines Signaturschlüssel-Zertifikates nach einer bewußten Aufdeckung seines privaten Schlüssels veranlassen und anschließend behaupten, die digitale Signatur sei unecht. Diese Bedrohung besteht in ähnlicher Weise bei allen Authensierungsverfahren, z.B. bei der Verwendung von EC-Karten an Geldautomaten.

9 Bei Zertifizierungsstellen nach Signaturgesetz kann vorausgesetzt werden, daß mit hinreichender Sicherheit ausgeschlossen ist, daß eine solche Bescheinigung rückdatiert oder gefälscht ist.

3.3 Normale Nutzung des Zeitstempels

In der vorliegenden Spezifikation wird zwischen der normalen Nutzung des Zeitstempels und der Nutzung des Zeitstempels im Falle einer Kompromittierung des vom Zeitstempeldienst verwendeten Signaturschlüssels unterschieden. Eine normale Nutzung setzt auch voraus, daß die vom Zeitstempeldienst verwendeten Kryptoverfahren zum Zeitpunkt der Prüfung des Zeitstempels gemäß § 17 Abs. 2 SigV als geeignet angesehen werden können.[10]

Im folgenden wird die normale Nutzung für den Fall beschrieben, daß der Absender einer Nachricht einen Zeitstempel beantragt. Die normale Nutzung umfaßt folgende Schritte:

- Der Absender signiert die Nachricht
- Der Absender erhält auf Antrag einen Zeitstempel für die Nachricht vom Zeitstempeldienst
- Der Absender prüft den Zeitstempel (und archiviert die Nachricht zusammen mit dem Zeitstempel für eigene Zwecke)
- Der Absender sendet Nachricht und Zeitstempel zusammen an den/die Empfänger
- Der Empfänger prüft, ob Zeitstempel und Nachricht zusammengehören
- Der Empfänger prüft, ob die digitale Signatur des Zeitstempels zu dem im Zeitstempel ausgewiesenen Zeitpunkt gültig war
- Der Empfänger prüft, ob die digitale Signatur der Nachricht zu dem im Zeitstempel ausgewiesenen Zeitpunkt gültig war

Falls der Empfänger alle Schritte mit positivem Ergebnis durchlaufen hat, ist die Authentizität der Nachricht für ihn nachgewiesen und der Absender kann die Echtheit der Nachricht nicht mit Erfolg bestreiten.

Die normale Nutzung umfaßt die folgenden Schritte, falls der Empfänger der Nachricht einen Zeitstempel beantragt:

- Der Empfänger prüft die Gültigkeit der Nachricht bezogen auf den aktuellen Zeitpunkt (optional)
- Der Empfänger erhält auf Antrag einen Zeitstempel für die Nachricht vom Zeitstempeldienst
- Der Empfänger prüft, ob die digitale Signatur des Zeitstempels zu dem im Zeitstempel ausgewiesenen Zeitpunkt gültig war
- Der Empfänger prüft, ob die digitale Signatur der Nachricht zu dem im Zeitstempel ausgewiesenen Zeitpunkt gültig war

Falls der Empfänger alle Schritte mit positivem Ergebnis durchlaufen hat, ist die Authentizität der Nachricht für ihn nachgewiesen und der Absender kann die Echtheit der Nachricht nicht mit Erfolg bestreiten.

4 Gestaltung des Zeitstempeldienstes

Die vollständige Beschreibung des Zeitstempeldienstes ist nicht Gegenstand dieser Spezifikation. Die Gestaltungsmerkmale werden deshalb nur insoweit beschrieben, als sie für die vorliegende Spezifikation von Bedeutung sind. Weitere Gestaltungsmerkmale oder andere Dienste

---

[10] Die nicht normale Nutzung des Zeitstempels wird in Kapitel 4.1, „Abgrenzung der Spezifikation“ beschrieben.

im Zusammenhang mit dem Zeitstempeldienst werden ausschließlich zum Zwecke der Abgrenzung der Spezifikation erwähnt.

4.1 Abgrenzung der Spezifikation

Die vorliegende Spezifikation beschränkt sich im wesentlichen auf die Pflichtdienstleistungen eines Zeitstempeldienstes, wie sie von SigG/SigV gefordert werden. Die Nutzer benötigt neben den im Gesetz definierten Pflichtdienstleistungen ggf. weitere Dienstleistungen einer vertrauenswürdigen Instanz, um die Ziele der Nutzung des Zeitstempels in allen Fällen zu erreichen. Eine solche Instanz ist der sog. Notariatsdienst (Notary Authority), der nicht Gegenstand des Signaturgesetzes ist.

Falls kein Fall einer normalen Nutzung eines Zeitstempels vorliegt (vgl. Kapitel 3.3), benötigt der Nutzer weitere Dienstleistungen, die nur die ZS erbringen kann. Diese Dienstleistungen sind nicht Gegenstand der Spezifikation, werden jedoch ebenfalls beschrieben.

Keine Pflichtdienstleistung eines Zeitstempeldienstes ist die Prüfung der digitalen Daten (als Element des Zeitstempels). Zwar ist ein Zeitstempel wertlos, wenn er sich auf digitale Signaturen bezieht, die zum Zeitpunkt der Generierung des Zeitstempels nicht gültig sind. Es ist jedoch nicht Aufgabe der Zeitstempeldienstes, eine Gültigkeitsprüfung oder eine andere Prüfung der digitalen Daten (als Element des Zeitstempels) durchzuführen.[11] Eine solche Prüfung kann jeder jederzeit selbst durchführen, der über die digitale Signatur verfügt oder er kann z.B. einen Notariatsdienst mit der Prüfung beauftragen.

Es ist auch keine aus SigG/SigV ableitbare Pflichtdienstleistung des Zeitstempeldienstes, die Gültigkeit der von ihm ausgestellten Zeitstempels nachträglich zu überprüfen.[12] In Fällen der nicht normalen Nutzung des Zeitstempels, die im folgenden beschrieben werden, ist der Nutzer allerdings auf Dienstleistungen der ZS angewiesen.

Ein nicht normaler Fall der Nutzung eines Zeitstempels liegt vor, wenn der Signaturschlüssel des Zeitstempeldienstes[13] kompromittiert wurde. Auch wenn der Zeitstempeldienst alle geforderten Sicherheitsmaßnahmen beachtet, so kann dieser Fall doch nicht völlig ausgeschlossen werden.

Mit einem kompromittierten Zeitstempelschlüssel kann ein Angreifer unechte Zeitstempel generieren. Durch die Sperrung eines kompromittierten Zeitstempelschlüssels kann erreicht werden, daß diese unechten Zeitstempel bei einer Gültigkeitsprüfung erkannt werden, falls die Zeitangabe im Zeitstempel auf einen späteren Zeitpunkt als den Sperrzeitpunkt verweist. Der Angreifer wird deshalb stets einen unechten Zeitstempel für einen Zeitpunkt vor dem Sperrzeitpunkt generieren. Falls die Prüfregeln für die Gültigkeit von Zeitstempeln denen der Gültigkeit anderer digitaler Signaturen entsprechen würden, müßte der Verifizierer einen solchen Zeitstempel akzeptieren. Damit hätte der Angreifer sein Ziel erreicht.

Die normale Nutzung eines Zeitstempels ist deshalb im Falle der Kompromittierung eines Zeitstempelschlüssels ausgeschlossen. Da der Verifizierer nicht erkennen kann, ob der

---

11 Daraus folgt aus datenschutzrechtlichen Gründen, daß es dem Zeitstempeldienst nicht erlaubt ist, die digitalen Daten zu untersuchen, für den der Nutzer einer Zeitstempel beantragt. (Eine entsprechende Anforderung an den Zeitstempeldienst findet sich in Kapitel 2.1 [PKIX-TSP 98].)

12 Selbstverständlich muß der vom Zeitstempeldienst ausgestellte Zeitstempel gültig sein. Auch ist es die interne Aufgabe der Revision, dies zu prüfen. Es handelt sich jedoch nicht um eine Dienstleistung.

13 Der Zeitstempeldienst muß stets über einen eigenen Signaturschlüssel verfügen, der ausschließlich für die Signatur von Zeitstempeln verwendet wird. Diese Anforderung findet sich übereinstimmend im ersten Satz von Kapitel 2.3 [PKIX-TSP 98], in Kapitel 2.3.9.3 [BSI-ZERT 99] und in A-TSS 8 in Kapitel 6.5.2 [MKAT 97].

Zeitstempel echt ist oder nicht, kann er sich auf den Zeitstempel nicht mehr verlassen. Alle mit dem kompromittierten Schlüssel generierten Zeitstempel haben ihren Beweiswert verloren.[14] Der Verifizierer benötigt eine zusätzliche Information einer vertrauenswürdigen Instanz, die ihm die Echtheit des Zeitstempels bestätigt, also eine weitere Dienstleistung.

Die Bestätigung der Echtheit eines Zeitstempels ist keine der im Signaturgesetz erwähnten Dienstleistungen einer ZS. Allerdings kann keine andere Instanz diese Dienstleistung qualitativ gleichwertig erbringen.

Falls ein Notariatsdienst alle Nachrichten zusammen mit den Zeitstempeln archiviert, kann er vor der Archivierung prüfen, ob der Zeitstempelschlüssel als kompromittiert ausgewiesen ist oder nicht. Nur wenn der Schlüssel zu diesem Zeitpunkt nicht gesperrt ist, darf er von der Echtheit der Zeitstempels ausgehen und die Archivierung durchführen. Auf diese Weise kann der Notariatsdienst sicherstellen, daß das Archiv nur echte Zeitstempel enthält.

Dies gilt jedoch nur unter der Prämisse, daß keine unerkannt kompromittierten Zeitstempelschlüssel existieren. Im Falle unerkannt kompromittierter Zeitstempelschlüssel kann das Archiv unechte Zeitstempel enthalten, ohne daß der Notariatsdienst dies erkennen könnte.

Prinzipiell kann nur der Zeitstempeldienst selbst in diesem Fall, echte von unechten Zeitstempeln unterscheiden. Unecht sind alle Zeitstempel, die tatsächlich nicht vom Zeitstempeldienst generiert wurden. Da die Anforderung an den Zeitstempeldienst besteht, eine einmal beschreibbare Protokollierungskomponente zu verwenden, mit der alle erzeugten Zeitstempel nachvollzogen werden können (vgl. Maßnahme M-TTS 9 in Kapitel 6.5.4.2.3 [MKAT 97]), muß der Zeitstempeldienst dazu auch in der Lage sein.

Aus den genannten Gründen ist es erforderlich, daß der Zeitstempeldienst die Echtheit eines Zeitstempels auf Anfrage bestätigt.[15] Während ein Zeitstempel auf einen elektronischen Antrag hin automatisch generiert wird, ist ein automatisiertes Verfahren für die Bestätigung der Echtheit eines Zeitstempels nicht erforderlich. Dementsprechend enthält die vorliegende Spezifikation kein Protokoll für eine automatische Echtheitsanfrage für Zeitstempel.

Die normale Nutzung eines Zeitstempels ist nicht nur im Falle einer Schlüsselkompromittierung ausgeschlossen, sondern auch, wenn die bei der Erzeugung verwendeten Algorithmen als nicht mehr geeignet angesehen werden.

Als Schutz dagegen sieht das Gesetz die erneute digitale Signatur gemäß § 18 SigV vor. Die Nachricht und der/die zugehörigen Zeitstempel können dazu zusammen mit einem neuen Zeitstempel versehen werden. Bei einer Nutzung des Zeitstempels muß danach auch dieser Zeitstempel geprüft werden.

Die Generierung erneuter digitaler Signaturen ist kein Zeitstempeldienst. Sie ist ein eigener Dienst, der im Dokument „Mehrfachsignaturen“ beschrieben wird, das Teil der Gesamtspezifikation ist.

Die normale Nutzung des Zeitstempels ist auch dann ausgeschlossen, wenn sich herausstellt, daß die verwendeten Algorithmen bereits zu einem Zeitpunkt, zu dem sie noch als geeignet angesehen wurden, tatsächlich ungeeignet waren. Dies Wahrscheinlichkeit hierfür ist

---

14 Der Absender einer digital signierten Nachricht könnte z.B. fälschlich behaupten, daß der vom Empfänger präsentierte Zeitstempel nachträglich als unechter Zeitstempel für seine Nachricht generiert wurde und er die Nachricht zu einem späteren Zeitpunkt als dem durch den unechten Zeitstempel ausgewiesen signiert hat. Falls es darauf ankommen sollte, daß die Signatur zu dem durch den Zeitstempel ausgewiesenen früheren Zeitpunkt erzeugt worden ist, müßte der Empfänger dann beweisen können, daß die Behauptung des Absenders falsch ist und der Zeitstempel tatsächlich echt ist.

15 Ob eine entsprechende Verpflichtung der ZS aus dem Gesetz abgeleitet werden kann, soll hier dahingestellt bleiben.

allerdings äußerst gering, da gemäß §17 Abs.2 SigV nur solche Algorithmen als geeignet ausgewiesen werden, bei denen dies nach menschlichem Ermessen ausgeschlossen werden kann.

Auch bei der nach [BAZ140298] geforderten ausschließlichen Verwendung starker Hash-Algorithmen kann jedoch nicht völlig ausgeschlossen werden, daß zu einem Zeitstempel zwei verschiedene Datensätze vorgelegt werden, die bei Verwendung der gleichen Hashfunktion den gleichen Hashwert haben. Es ist dann bei normaler Nutzung des Zeitstempels nicht entscheidbar, für welchen der Datensätze der Zeitstempel beantragt wurde.

Entscheidbar ist dies nur dann, wenn die digitalen Daten zusammen mit dem Zeitstempel bei einer vertrauenswürdigen Instanz archiviert werden. Eine Archivierung digitaler Daten für den Nutzer ist eine Dienstleistung, die ein Notariatsdienst erbringt. Sie gehört nicht zu den Pflichtdienstleistungen eines Zeitstempeldienstes.

4.2 Gestaltungsmerkmale der Spezifikation

In diesem Kapitel werden allgemeine Gestaltungsmerkmale beschrieben, die für die Spezifikation von Bedeutung sind.

Unterschiedliche Ausprägungen des Zeitstempeldienstes

Entsprechend [PKIX-TSP 98] kann es unterschiedliche Ausprägungen des Zeitstempeldienstes geben. Der Nutzer kann im Antrag angeben, welche Art von Zeitstempel er wünscht.[16] Zeitstempel können sich z.B. dadurch unterscheiden, welche Sicherungsmaßnahmen ein Zeitstempeldienst realisiert hat, um die Qualität des Zeitstempels garantieren zu können. Da SigG/SigV nur Mindestanforderungen enthalten, können sich Zeitstempeldienste auch dazu verpflichten, höheren Anforderungen gerecht zu werden.

Ein Beispiel für eine weitere Sicherungsmaßnahme ist eine Mehrfachsignatur eines Zeitstempeldienstes. Eine ZS könnte sich entsprechend ihrer Policy verpflichten, einen Zeitstempel auf Antrag mit zwei digitalen Signaturen zu versehen. Die in der vorliegenden Spezifikation verwendete Syntax läßt dies zu.

Nutzeridentifizierung

Der Zeitstempeldienst muß die Identität des Nutzers nicht kennen, um seine Aufgabe erfüllen zu können. Nach der in Kapitel 2 gegebenen Definition enthält ein Zeitstempel keinen Identifikator für den Nutzer, der den Zeitstempel beantragt hat. Das datenschutzrechtliche Kriterium der Erforderlichkeit analog § 12 Abs. Satz1 SigG ist deshalb stets zu prüfen, wenn der Zeitstempeldienst die Nutzer identifizieren will.

Der Zeitstempeldienst darf die Nutzer identifizieren, falls er für seine Dienstleistung ein Entgelt verlangen will. In diesem Fall hat er ein berechtigtes Interesse daran, die Identität des Nutzers in Erfahrung zu bringen, um die erbrachten Dienstleistungen in Rechnung stellen zu können. In diesem Fall kann der Zeitstempeldienst verlangen, daß der Nutzer seine Identität preisgibt.

Ausnahmsweise könnte auch der Nutzer wünschen, daß der Zeitstempeldienst seine Identität im Zeitstempel bescheinigt und so einen individualisierten Zeitstempel generiert.[17] Dafür

---

16 Zeitstempelarten werden durch Angaben im Feld „reqPolicy“ unterschieden (s. Kapitel 6.1).

17 Ein individualisierter Zeitstempel kann für den Schutz des Absenders vorteilhaft sein, wenn der Absender nachweisen kann, daß der Empfänger die Nachricht zusammen mit einem Zeitstempel erhalten hat. Falls der Empfänger dadurch einen Vorteil erreichen könnte, daß der Absender nicht beweisen kann, den Zeitstempel tatsächlich beigefügt zu haben, kann er selbst (anonym) einen Zeitstempel beschaffen und später behaupten, diesen Zeitstempel vom Absender erhalten zu haben.

besteht jedoch keine Notwendigkeit, da der Nutzer den mit einem individualisierten Zeitstempel angestrebten Zweck auf andere Art erreichen kann.[18] Individualisierte Zeitstempel sind weder nach [PKIX-TSP 98] noch nach SigG/SigV vorgesehen und deshalb auch nicht Gegenstand der vorliegenden Spezifikation.

Da der Zeitstempeldienst verlangen kann, daß der Nutzer sich identifiziert, wird in der vorliegenden Spezifikation neben dem normalen anonymen Zeitstempelantrag ein digital signierter Antrag definiert. Es wird davon ausgegangen, daß ein Nutzer in der Regel über die Möglichkeit verfügt, digitale Signaturen zu erzeugen.

Für die seltenen Fälle, in denen der Nutzer ausnahmsweise nicht über die Möglichkeit verfügt, digitale Signaturen zu erzeugen (weil er z.B. seine Chipkarte verloren hat) muß der Zeitstempeldienst ggf. ein alternatives Verfahren anbieten. Andernfalls wäre eine unzulässige Beschränkung des Nutzerkreises zu befürchten (vgl. Definition des „Nutzers“ in Kapitel 2). Ein Zeitstempeldienst darf einen Antrag auf einen Zeitstempel nicht allein deshalb ablehnen, weil der Nutzer sich nicht mittels digitaler Signatur identifizieren kann. Das alternative Verfahren muß jedoch nicht automatisiert sein.

Die vorliegende Spezifikation umfaßt ein Signatur-Verfahren zur Authentisierung der Nutzer bei Zeitstempelanträgen (s. Kapitel 6.5). Alternative Verfahren sind nicht Gegenstand der Spezifikation.

Zeit und zeitbezogene Daten

Jeder Zeitstempel muß eine Zeitangabe enthalten, die die Tageszeit wiedergibt. An die Qualität dieser Zeitangabe werden hohe Anforderungen gestellt. Gemäß § 16 Abs. 5 SigV muß sie exakt die gesetzliche Zeit zum Zeitpunkt der Erzeugung des Zeitstempels wiedergeben.

Der Zeitstempeldienst nach Signaturgesetz muß Zugriff auf eine authentische Quelle für die gesetzliche Zeit haben. Falls er den Zugriff verloren hat ist der Zeitstempeldienst nicht verfügbar. Diese Tatsache muß er dem Nutzer mitteilen, der einen Zeitstempelantrag gestellt hat.

Im Interesse des Nutzers muß der Zeitstempeldienst eine bestimmte Antwortzeit garantieren. Antwortenzeiten von bis zu einer Minute sind vertretbar. Der Zeitstempeldienst muß den Nutzer in einer Antwort und einen Zeitstempelantrag ggf. darauf hinweisen, daß er die garantierte Antwortzeit nicht einhalten kann und die voraussichtliche Dauer des Problems angeben. Der Nutzer kann sich dann entscheiden, abzuwarten, bis der Zeitstempeldienst wieder funktionsfähig ist, oder einen anderen Zeitstempeldienst beauftragen.

Entsprechend [PKIX-TSP 98] wird der Zeitdatendienst als optionaler Sicherheitsdienst in der Spezifikation berücksichtigt. Falls der Zeitstempeldienst eine Schnittstelle zu einem Zeitdatendienst hat, kann der Nutzer in seinem Antrag angeben, welcher Zeitdatendienst mit der Generierung zusätzlicher Zeitdatenstempel beauftragt werden soll.

Seriennummern

Entsprechend [PKIX-TSP 98] wird die optionale Möglichkeit vorgesehen, die Zeitstempel mit einer Seriennummer zu versehen. Diese Seriennummer kann verwendet werden, um Zeitstempel in der Zeitstempeldokumentation leichter identifizieren zu können und kann der

---

Falls nun der Absender stets individualisierte Zeitstempel versendet und dies dem Empfänger bekannt sein muß, würde es dem Empfänger schwerfallen, mit dieser Behauptung vor Gericht Erfolg zu haben.

[18] Der Absender einer Nachricht mit Zeitstempel kann vom Empfänger eine Quittung fordern (vgl. Kapitel 4.1.2, „Quittungsanforderung“ [BSI-SIG 99]).

Unterstützung der Beweissicherung des Zeitstempeldienstes dienen.[19] Ein Signaturgesetz-konformer Zeitstempeldienst muß von dieser Option keinen Gebrauch machen. Falls er Seriennummern verwendet, muß er allerdings dafür sorgen, daß diese nicht doppelt vergeben werden können.

Digitale Daten als Element des Zeitstempels

Entsprechend [PKIX-TSP 98] ist niemals die Nachricht selbst, sondern stets ein Komprimat der Nachricht in Form eines Hashwertes Element des Zeitstempels. Dieser Hashwert wird stets vom Nutzer selbst generiert. Der Zeitstempeldienst bildet den Zeitstempel dann aus diesem Hashwert, einer Zeitangabe und der Signatur. Gegenstand der vorliegenden Spezifikation sind ausschließlich Zeitstempel dieser Art.

Prinzipiell könnte auch eine andere Art eines Zeitstempel verwendet werden. Statt des Komprimats der Nachricht könnte die Nachricht selbst in den Zeitstempel einbezogen werden. Aus der Legaldefinition des Zeitstempels in § 2 Abs. 4 SigG läßt sich nicht ableiten, daß nur eine der beiden genannten Arten von Zeitstempeln Signaturgesetz-konform ist.

Die Einbeziehung der Nachricht selbst in den Zeitstempel würde jedoch keinen Vorteil bieten. Da der Zeitstempel eine digitale Signatur ist, kann er effektiv nur den Hashwert der Nachricht mit einer authentischen Zeitangabe verbinden. Die Nachricht wird nur mittelbar über ihren Hashwert durch einen Zeitstempel geschützt.

Die Einbeziehung der Nachricht würde jedoch zu gravierenden Nachteilen führen. Es kann nicht davon ausgegangen werden, daß alle Nachrichten, die zeitgestempelt werden sollen, offen übertragen werden können. Die Zeitstempel-Protokolle müßten deshalb eine vertrauliche Kommunikation mit dem Zeitstempeldienst ermöglichen. Auch in diesem Fall würde für den Zeitstempeldienst selbst potentiell die Möglichkeit bestehen, von den vertraulichen Nachrichten Kenntnis zu nehmen. Der Zeitstempeldienst müßte deshalb besonders effektive Sicherheits-maßnahmen ergreifen, um eine unerlaubte Kenntnisnahme der Nachrichten durch das Betriebspersonal zuverlässig zu verhindern.[20]

Falls nicht die Nachricht selbst, sondern nur ihr Hashwert in den Zeitstempel einbezogen werden soll, gibt es wiederum zwei Möglichkeiten. Der Hashwert kann durch den Nutzer selbst oder durch den Zeitstempeldienst generiert werden. Aus der Legaldefinition des Zeitstempels in § 2 Abs. 4 SigG läßt sich auch hier nicht ableiten, daß nur eine der beiden genannten Varianten Signaturgesetz-konform ist.

Die Generierung des Hashwertes durch den Zeitstempeldienst würde keine Vorteile, aber gravierende Nachteile bieten.[21] Die vorliegende Spezifikation geht deshalb stets davon aus, daß der Hashwert durch den Nutzer generiert wird.

---

19 Als weiterer Zweck der Seriennummer wird in Kapitel 2.4 [PKIX-TSP 98] angegeben, daß Zeitstempel eindeutig sind. Die Eindeutigkeit eines Zeitstempels muß jedoch vom Zeitstempeldienst nicht garantiert werden.

20 Ein weiterer Nachteil wäre, daß der Zeitstempel in der Regel wesentlich umfangreicher wäre, wenn er die Nachricht umfassen würde.

21 Als Vorteil könnte angesehen werden, daß beim Zeitstempeldienst als einer vertrauenswürdigen Instanz im Gegensatz zum Nutzer nicht zu befürchten ist, daß ungeeignete Hashfunktionen verwendet werden. Das Signaturgesetz sieht zwar vor, daß der Nutzer nur geprüfte Komponenten verwendet. Bei der Konfiguration dieser Komponenten können jedoch Fehler gemacht werden. Falls eine Hashfunktion nicht mehr als geeignet angesehen wird muß der Nutzer seine Komponente so konfigurieren, daß diese Hashfunktion nicht mehr verwendet wird. Dies kann der Nutzer unterlassen.

Es ist auch noch die Frage zu entscheiden, welche Daten über ihren Hashwert in den Zeitstempel einzubeziehen sind. Entsprechend [PKIX-TSP 98] soll sich der Hashwert stets auf die gesamte Nachricht beziehen und nicht nur auf die digitale Signatur der Nachricht.

Ein wesentlicher Unterschied zwischen den beiden Varianten besteht bei Mehrfachsignaturen. Während bei der hier bevorzugten Variante nur ein Zeitstempel für die gesamte Nachricht erforderlich ist, müßten andernfalls ggf. mehrere Zeitstempel beschafft werden, für jede digitale Signatur einer. Dies würde trotz erhöhtem Aufwand keinen Vorteil bieten.

Da der Zeitstempeldienst nicht prüfen kann, ob sich der Zeitstempelantrag auf die gesamte Nachricht oder nur auf eine digitale Signatur bezieht, ist die letztgenannte Variante durch die vorliegende Spezifikation prinzipiell nicht ausgeschlossen.[22] Allerdings enthält der Zeitstempel keine Information darüber, auf welchen Teil der Nachricht sich der Zeitstempel bezieht. Dies ist nicht erforderlich, da stets implizit davon ausgegangen wird, daß sich der Zeitstempel auf die gesamte Nachricht bezieht. Bei einer Beschränkung auf einen Teil der Nachricht müßte der Nutzer dem Empfänger des Zeitstempels zusätzlich explizite Information zur Verfügung stellen, damit er den Zeitstempel prüfen kann, ohne diese Information erraten zu müssen.

Prüfung der verwendeten Hashfunktion

Ein Zeitstempel kann für den Nutzer wertlos sein, wenn er eine ungeeignete Hashfunktion zur Generierung des Hashwertes verwendet hat. Entsprechend [PKIX-TSP 98] ist deshalb vorgesehen, daß der Zeitstempeldienst die verwendete Hashfunktion auf ihre Eignung prüft.[23]

SigG/SigV fordern eine solche Prüfung nicht explizit. Es ist deshalb fraglich, ob diese Prüfung zu den Pflichtdienstleistungen eines Signaturgesetz-konformen Verzeichnisdienstes gehört.[24] Dies muß dahingestellt bleiben, da diese Frage hier nicht abschließend geklärt werden kann.

Allerdings wird dringend empfohlen, daß der Zeitstempeldienst eine solche Prüfung durchführt. Dies gilt auch dann, wenn aus SigG/SigV keine gesetzliche Anforderung hierfür abgeleitet werden kann. Durch die Verwendung ungeeigneter Hashfunktionen kann das Vertrauen in die Sicherheit des Verfahrens insgesamt untergraben werden. Dabei ist es unerheblich, welche Instanz die ungeeignete Hashfunktion verwendet hat.

Im Falle der Verwendung ungeeigneter Hashfunktionen durch den Nutzer sollte der Zeitstempeldienst den Antrag entsprechend [PKIX-TSP 98] daher stets zurückweisen und den Antragsteller auffordern, einen neuen Antrag unter Verwendung einer geeigneten Hashfunktion zu stellen.

Möglichen Bedrohungen kann jedoch dadurch begegnet werden, daß der Zeitstempeldienst die vom Nutzer verwendete Hashfunktion prüft (s. u.). Außerdem würde die Verwendung einer ungeeigneten Hashfunktion vom Empfänger eines Zeitstempels sofort festgestellt. Wesentliche Vorteile bietet die Generierung des Hashwertes durch den Zeitstempeldienst somit nicht.

Dem stehen jedoch die bereits beschriebenen wesentlichen Nachteile der Übermittlung der Nachricht an den Zeitstempeldienst gegenüber.

22 Diese Variante wurde in der Begründung zu § 9 SigG beschrieben (vgl. Kapitel 6.5.1 [MKAT 97]). Dort wird zurecht darauf hingewiesen, daß es bei signierten Daten ausreichend ist, wenn sich der Zeitstempel nur auf die digitale Signatur bezieht, da diese die gesamten signierten Daten umfaßt.

23 Die für den Zeitstempelantrag verwendete Datenstruktur enthält ein Feld für den OID der verwendeten Hashfunktion. Der Zeitstempeldienst muß prüfen, ob der Nutzer einen OID angegeben hat, der eine geeignete Hashfunktion identifiziert, d.h. eine Hashfunktion, die gemäß § 17 Abs. 2 SigV veröffentlicht ist. Falls der Nutzer einen unzulässigen OID verwendet hat, muß der Zeitstempeldienst den Antrag zurückweisen.

24 Möglicherweise würde der Zeitstempeldienst gegen eine Unterrichtungspflicht analog § 6 SigG verstoßen, wenn er einen Antragsteller nicht darauf hinweist, daß er eine ungeeignete Hashfunktion verwendet hat, obwohl er dies wußte oder hätte wissen müssen.

5 Abläufe

Die folgende Abbildung gibt einen Überblick über die Abläufe für einen Antrag auf einen Zeitstempel :

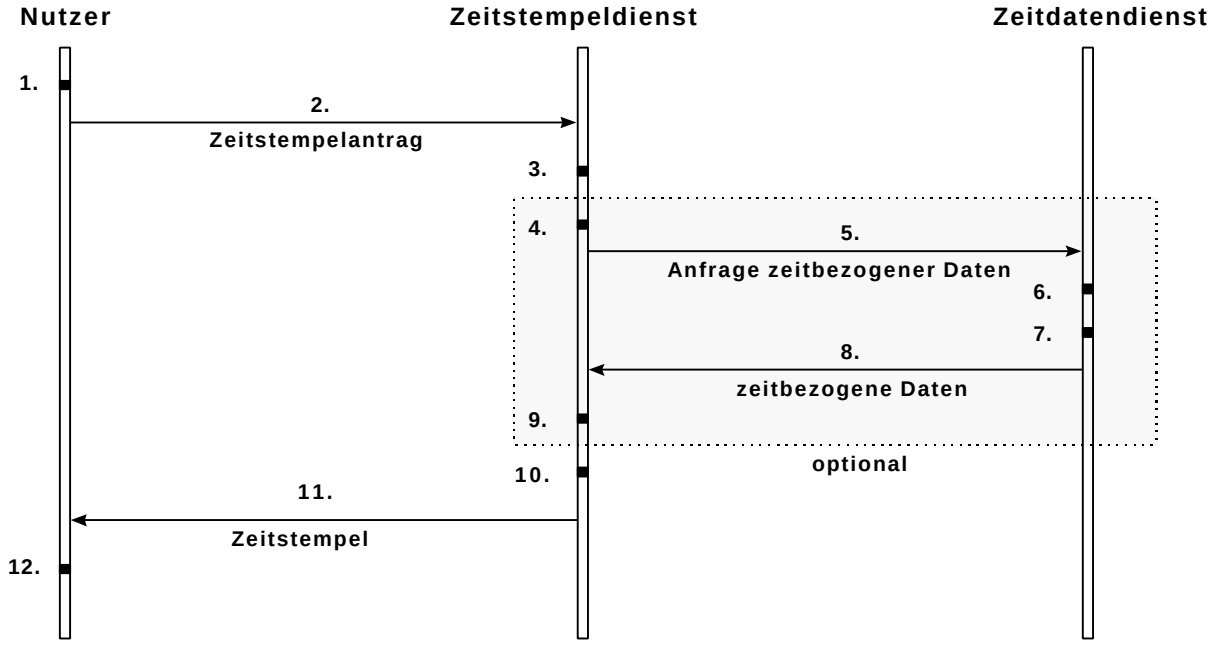

Abbildung 1: Abläufe beim einem Antrag für einen Zeitstempel

Der Gesamtablauf setzt sich aus bis zu 12 Teilschritten zusammen, wobei die Teilschritte vier bis neun optional sind, da sie den Zeitdatendienst betreffen, dessen Realisierung nicht vom Signaturgesetz gefordert wird.

1. Der Ablauf beginnt stets damit, daß der Nutzer einen digitalen Zeitstempelantrag (Time Stamp Request) generiert. Der Antrag kann folgende optionale Daten enthalten[25]:
   - Den Hashwert der digitalen Daten, für die ein Zeitstempel generiert werden soll, falls der Antragsteller nicht lediglich eine Zeitangabe benötigt.
   - Angaben über die Art des Zeitstempels (Policy-Angabe).
   - Angaben zu den Zeitdatendiensten, die Zeitdaten beisteuern sollen.
   - Einen Integer-Wert (Nonce), der der Zuordnung des Antrags zum Zeitstempel dient.
2. Anschließend sendet der Nutzer den Zeitstempelantrag an den Zeitstempeldienst (Time Stamp Authority - TSA).
3. Die TSA prüft den Antrag auf Vollständigkeit und inhaltliche Korrektheit. Ein Antrag muß dem Nachrichtenformat der vorliegenden Spezifikation entsprechen und ggf. den Antragsteller erkennen lassen, falls diese Information zu Abrechnungszwecken benötigt wird. Die inhaltliche Prüfung beschränkt sich darauf, den OID für die verwendete Hashfunktion zu untersuchen[26] und den Nutzer ggf. zu authentisieren.

---

25 Diese Daten werden in Kapitel 6.1, „Zeitstempelantrag“, genauer beschrieben.

26 Der Zeitstempeldienst hat zu prüfen, ob der OID zu einer Hashfunktion gehört, die gemäß §17 Abs. 2 Satz 1 SigV als geeignet angesehen und im Bundesanzeiger veröffentlicht ist.

4. Die TSA generiert entsprechend den Angaben zu den Zeitdatendiensten des Zeitstempelantrags Anfragen für zeitgebundene Daten (Temporal Data Request).
   Die Anfragen können folgende optionale Daten enthalten:
   - Den Hashwert der digitalen Daten aus dem Zeitstempelantrag, falls der Antragsteller nicht lediglich eine Zeitangabe benötigt.
   - Den Integer-Wert des Zeitstempelantrags, der der Zuordnung des Antrags zum Zeitstempel dient.
5. Die TSA sendet die Anfragen an die TDA (Temporal Data Authority).
6. Die TDA prüft die Anfrage auf Vollständigkeit und inhaltliche Korrektheit. Die Anfrage muß dem Nachrichtenformat der vorliegenden Spezifikation entsprechen und ggf. den Antragsteller erkennen lassen, falls diese Information zu Abrechnungszwecken benötigt wird.
   Die inhaltliche Prüfung beschränkt sich darauf, den OID für die verwendete Hashfunktion zu untersuchen und die TSA ggf. zu authentisieren.
7. Die TDA generiert die zeitgebundenen Daten (Temporal Data Token). Die zeitgebundenen Daten bestehen aus folgenden Informationen:
   - Die zeitgebundenen Daten in der Form, in der sie vom Zeitdatendienst bereitgestellt werden.
   - Der Name der TDA.
   - Die Nonce aus der Anfrage, falls vorhanden.
   - Der Hashwert aus der Anfrage, soweit vorhanden.
   - Eine optionale Seriennummer.
   - Die Signatur der TDA über diese Daten.
8. Die TDA sendet die zeitgebundenen Daten an die TSA.
9. Die TSA prüft die Daten auf Vollständigkeit und inhaltliche Korrektheit. Die zeitgebundenen Daten müssen dem Nachrichtenformat der vorliegenden Spezifikation entsprechen. Die inhaltliche Prüfung umfaßt:
   - Prüfung der Gültigkeit der digitalen Signatur.
   - Prüfung, ob die signierten zeitgebundenen Daten mit den Daten aus der Anfrage übereinstimmen.
   - Prüfung, ob der Name der TSA, der Hashwert und der Hashalgorithmus korrekt angegeben wurden.
   - Prüfung, ob die Nonce mit der Nonce in der Anfrage übereinstimmt.
10. Die TSA generiert den Zeitstempel. Der Zeitstempel besteht aus folgenden Informationen:[27]
    - Die Zeitangabe.
    - Die Policy-Angabe aus dem Zeitstempelantrag.
    - Der Status des Zeitstempelantrags.
    - Der Name der TSA.

[27] Diese Informationen werden in Kapitel 6.2 genauer beschrieben.

- Die Nonce aus dem Zeitstempelantrag, falls vorhanden.
- Der Hashwert aus dem Zeitstempelantrag, soweit vorhanden.
- Eine optionale Seriennummer.
- Die zeitgebundenen Daten, soweit vorhanden.
- Ein optionales Freitextfeld.
- Die Signatur der TSA über diese Daten.

11. Die TSA sendet den Zeitstempel an den Nutzer.
12. Der Nutzer prüft den Zeitstempel auf Vollständigkeit und inhaltliche Korrektheit. Der Zeitstempel muß dem Nachrichtenformat der vorliegenden Spezifikation entsprechen. Die inhaltliche Prüfung umfaßt:
    - Prüfung der Gültigkeit der digitalen Signatur des Zeitstempeldienstes.
    - Prüfung, ob der Zeitstempel dem Antrag entspricht.
    - Prüfung, ob der Name der TSA, der Hashwert und der Hashalgorithmus korrekt angegeben wurden.
    - Prüfung, ob die Nonce mit der Nonce in der Anfrage übereinstimmt.

6 Nachrichtenformate

Für den Zeitstempeldienst werden in den folgenden Kapiteln die vier Nachrichtenformate für Zeitstempelantrag, Zeitstempel, Anfrage zeitbezogener Daten und Zeitdatenstempel spezifiziert. Die Nachrichtenformate für digital signierte Anträge werden in Kapitel 6.5 beschrieben.

6.1 Zeitstempelantrag

Ein Zeitstempelantrag (Time Stamp Request) hat folgendes Format:

```
TimeStampReq          ::= SEQUENCE  {
     version                INTEGER { v1(0) },
     reqPolicy              PolicyInformation OPTIONAL,
     tdas                   SEQUENCE OF GeneralName OPTIONAL,
     nonce                  INTEGER OPTIONAL[28]
     messageImprint         MessageImprint OPTIONAL }
```

Das Versionsfeld (version) gibt die Version der Syntax an. Der Identifier „v1“ mit dem Integer-Wert „0“ bezeichnet die erste Version der Syntax des Zeitstempelantrags.

Über das optionale Policy-Feld (reqPolicy) kann der Nutzer die Policy für den gewünschten Zeitstempel angegeben. Durch die Policy wird die Verfahrensweise bei der Erstellung eines Zeitstempels bestimmt. Sie wird durch einen Objektbezeichner identifiziert und kann ihrerseits aus weiteren Kennzeichnern bestehen.

---

[28] In der PKIX-Spezifikation des Zeitstempeldienstes (vgl. Kapitel 2.4 [PKIX-TSP 98]) ist das Feld nicht optional. Es scheint sich dabei um ein Redaktionsversehen zu handeln, da bei jeder weiteren Referenzierung dieses Feldes stets darauf hingewiesen wird, daß das Feld auch fehlen kann.

Es wird die folgende Syntax verwendet:[29]

```
PolicyInformation     ::= SEQUENCE  {
     policyIdentifier     ReqPolicyId
     policyQualifier      SEQUENCE SIZE (1..MAX) OF
                          PolicyQualifierInfo OPTIONAL }

ReqPolicyId           ::= OBJECT IDENTIFIER

PolicyQualifierInfo   ::= SEQUENCE  {
     policyQualifierId    PolicyQualifierId
     qualifier            ANY DEFINED BY policyQualifierId }

PolicyQualifierId     ::= OBJECT IDENTIFIER
```

Da die Verfahrensweise bei der Erstellung des Zeitstempels durch die ZS festgelegt wird, werden die Objektbezeichner hierfür ebenfalls durch die ZS definiert. In der vorliegenden Spezifikation wird nur ein Objektbezeichner definiert, durch den zum Ausdruck gebracht wird, daß die Verfahrensweise den Minimalanforderungen an Zeitstempel gemäß SigG/SigV genügt. Für diesen Objektbezeichner gibt es keine weiteren Kennzeichner.

Der OID für das in der vorliegenden Spezifikation beschriebene Signaturgesetz-konforme Verfahren, das die Minimalanforderungen erfüllt, ist:

```
Id-sigi                   OBJECT IDENTIFIER ::= { 1 3 36 8 }
Id-sigi-sigts             OBJECT IDENTIFIER ::= { 1 3 36 8 X[30]}
Id-sigi-sigts-sigconform  OBJECT IDENTIFIER ::= { 1 3 36 8 X 1}
```

Das Zeitdatenfeld (tdas) enthält die Namen der Zeitdatendienste, deren zeitbezogene Daten in den Zeitstempel einbezogen werden sollen. Für die Zeitdatendienste wird kein spezielles Namensformat vorgegeben.[31] Es wird empfohlen, das Namensformat „registeredID“ zu verwenden, bei dem ein Name durch einen registrierten OID identifiziert wird.[32]

Das Feld „nonce“ (kurz für „number n once“) kann der Nutzer als eindeutige Referenz für den Zeitstempelantrag verwenden. Falls der Nutzer den gleichen Wert niemals zweimal verwendet, kann er den Zeitstempelantrag und den korrespondierenden Zeitstempel über diese Referenz eindeutig zusammenführen. Der Nutzer ist jedoch nicht verpflichtet, eine Nonce anzugeben.[33]

---

29 Die Syntax entspricht im wesentlichen der Syntax zur Angabe der Verfahrensweise bei der Erstellung von Zertifikaten (vgl. Kapitel 2.3.9.4 [BSI-ZERT 99]).

30 Der Wert für „sigts“ ist noch festzulegen.

31 „GeneralName“ ermöglicht eine Auswahl aus einer Menge verschiedener Namensformate (vgl. Kapitel 2.3.9.6 [BSI-ZERT 99].

32 Die Bestimmung der von Zeitdatendiensten bereitgestellten zeitbezogenen Daten ist nicht Gegenstand der vorliegenden Spezifikation. Dementsprechend werden auch Namen für die Zeitdatendienste nicht vergeben. Jeder Zeitdatendienst bestimmt seinen Namen selbst.

33 Da der Wert für die Nonce von jedem Nutzer frei gewählt werden kann, kann der Zeitstempeldienst nicht davon ausgehen, daß die Werte verschiedener Zeitstempelanträge eindeutig sind. Der Zeitstempeldienst muß keine Prüfung der Nonce durchführen.

Das optionale Feld „messageImprint“ besteht aus dem verwendeten Hashalgorithmus und dem Hashwert. Es wird folgende Syntax verwendet:

```
MessageImprint                ::= SEQUENCE  {
     hashAlgorithm                AlgorithmIdentifier,
     hashedMessage                OCTET STRING  }

AlgorithmIdentifier           ::= SEQUENCE  {
     algorithm                    OBJECT IDENTIFIER
     parameters                   ANY DEFINED BY algorithm OPTIONAL }
```

Die optionalen Felder „reqPolicy“ und „tdas“ müssen von Signaturgesetz-konformen Applikationen und Zeitstempeldiensten nicht unterstützt werden. Applikationen müssen jedoch in der Lage sein, Zeitstempelanträge mit allen sonstigen Feldern zu generieren. Zeitstempeldienste müssen diese Felder auswerten können.

Falls der Zeitstempeldienst den Nutzer identifizieren will, muß der Zeitstempelantrag digital signiert werden. Digital signierte Anträge werden in Kapitel 6.5 beschrieben.

6.2 Zeitstempel

Ein Zeitstempel (time stamp token) ist eine kryptographische Nachricht vom Typ „signierte Daten“ (signed data). Dieser Nachrichtentyp ist in Kapitel 5 [BSI-SIG 99], „Signaturaustauschformat“, beschrieben und beruht auf Kapitel 5 [CMS 98]. Die in [BSI-SIG 99] enthaltenen Regelungen für kryptographische Nachrichten vom Typ „signierte Daten“ gelten auch für Zeitstempel, soweit nichts anderes bestimmt ist.

Die allgemeine Syntax für kryptographische Nachrichten ist danach:

```
ContentInfo               ::= SEQUENCE  {
     contentType                OBJECT IDENTIFIER
     content                    [0] EXPLICIT ANY DEFINED BY contentType
}
```

Die kryptographische Nachricht assoziiert den zu schützenden Inhalt (content) mit einer Typangabe (contentType) in Form eines OIDs.

Die Syntax für einen Zeitstempel gemäß Kapitel 2.4 [PKIX-TSP 98] ist:

```
TimeStampToken ContentInfo    ::= SEQUENCE {
     contentType                   OBJECT IDENTIFIER,
     content                       [0] SEQUENCE  {
          version                       CMSVersion[34],
          digestAlgorithms              digestAlgorithmIdentifiers[35],
          ContentInfo                   SEQUENCE {,
               contentType                   OBJECT IDENTIFIER,
               content                       TSTInfo  }
          certificates                  [0] IMPLICIT CertificateSet
                                        OPTIONAL,
          signerInfos                   SignerInfos  }  }
```

[34] In Kapitel 2.4 [PKIX-TSP 98] wird an dieser Stelle der Typ „INTEGER“ angegeben. Dies führt zwar zum gleichen Ergebnis, ist aber nicht konsistent mit Kapitel 5 [CMS 98].

[35] In Kapitel 2.4 [PKIX-TSP 98] wird an dieser Stelle der Typ „AlgorithmIdentifier“ angegeben. Dies führt zwar in der Regel zum gleichen Ergebnis, ist allerdings inkonsistent, da die Spezifikation an sich Mehrfach-Signaturen erlaubt, die unterschiedliche Hashfunktionen verwenden können. Außerdem wird durch den Typ „AlgorithmIdentifier“ nicht zum Ausdruck gebracht, daß es sich um einen OID für eine Hash-Funktion handelt.

Der OID für Nachrichten vom Typ signed data ist:

```
id-signedData OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840)
                                     rsadsi(113549) pkcs7(7) 2 }
```

Das Versionsfeld (version) bezeichnet in Übereinstimmung mit [CMS 98] die Version der Syntax. Es sind folgende Werte definiert:

```
CMSVersion ::= INTEGER  { v0(0), v1(1), v2(2), v3(3), v4(4) }
```

Der Identifier „v3“ mit dem Integer-Wert „3“ bezeichnet die Version der Syntax, die dafür vorgesehen ist, andere als uninterpretierte binäre Daten zu signieren. Für Zeitstempel ist daher stets diese Versionsnummer zu verwenden.

Das Feld für die Hash-Algorithmen (digestAlgorithms) dient ausschließlich dem Zweck, die Verifikation eines Zeitstempels in einem „Durchgang“ zu ermöglichen.[36] Es werden folgende Datenstrukturen verwendet:

```
DigestAlgorithmIdentifiers ::= SET OF DigestAlgorithmIdentifier

DigestAlgorithmIdentifier  ::= AlgorithmIdentifier[37]
```

Die Syntax für dem Zeitstempel erlaubt Mehrfachsignaturen. Signaturgesetz-konforme Zeitstempeldienste müssen jedoch keine Mehrfachsignaturen unterstützten. In der Regel besteht die Menge der Identifier somit nur aus einem Element.

Die Felder „contentType“ und „content“ enthalten den eigentlichen Zeitstempel, d.h. die Datenstruktur „TSTInfo“, und einen OID zur Identifizierung des Datentyps „Zeitstempel“[38].

Ein Zeitstempel wird durch folgenden OID identifiziert:

```
Id-sigi-sigts-tsttoken  OBJECT IDENTIFIER ::= { 1 3 36 8 X 2}
```

Die Datenstruktur „TSTInfo“ wird in Kapitel 6.2.1 definiert.

Das optionale Zertifikatsfeld (certificates) enthält eine Menge von Zertifikaten. Eine Notwendigkeit für die Verwendung dieses Feldes besteht nicht. Es kann davon ausgegangen werden, daß alle Zertifikate des Zertifizierungspfades aus Zertifikatsverzeichnissen abrufbar sind.

Falls das Feld verwendet wird, sollte es alle Signaturschlüssel-Zertifikate des Zertifizierungspfades von der Wurzel-Zertifizierungsstelle bis zur ZS, die das Zertifikat für den Zeitstempeldienst erstellt hat, enthalten.[39] Sinnvoll ist dies jedoch nur dann, wenn Verifizierer des Zeitstempels auf Abfragen des Verzeichnisdienstes voraussichtlich verzichten werden. Andernfalls bietet die Verwendung des Feldes keine Vorteile.

---

36 Während der Auflösung der Datenstruktur kann bereits der Hashwert gebildet werden, der später bei der Verifikation benötigt wird.

37 Die Datenstruktur „AlgorithmIdentifier“ ist in Kapitel 6.1 definiert.

38 Da dieses Feld nicht in die Signatur eingeschlossen wird, ist es vom Verifizierer nicht zu verwenden. Verwendet werden muß statt dessen das signierte Attribut vom Typ „ContentType“, das den gleichen Inhalt hat (s. Kapitel 6.2.4). Das Feld „contentType“ ist somit an sich überflüssig, darf jedoch nicht ausgelassen werden, da es nicht optional ist.

39 Das Signaturschlüssel-Zertifikat des Zeitstempeldienstes, bzw. eine Referenz darauf, wird stets als signiertes Attribut in die Signatur eingeschlossen (s. Kapitel 6.2.4). Die zusätzliche Aufnahme dieses Zertifikates in das Feld „certificates“ ist daher überflüssig.

Das Informationsfeld (signerInfos) enthält eine Menge von Informationen über den Ersteller der Zeitstempelsignatur (s. Kapitel 6.2.4).

Bis auf das optionale Feld „certificates“ müssen alle Felder von Applikationen und dem Zeitstempeldienst unterstützt werden. Mehrfachsignaturen müssen nicht unterstützt werden.

6.2.1 TSTInfo

Die Datenstruktur „TSTInfo“ ist wie folgt definiert:

```
TSTInfo                  ::= SEQUENCE  {
     version                     INTEGER { v1(0) },
     policy                      PolicyInformation,
     status                      PKIStatusInfo,
     tsa                         GeneralName,
     tstTime                     TSTTime,
     tdaTokens                   SEQUENCE OF TemporalDataToken OPTIONAL,
     nonce                       INTEGER OPTIONAL,
     messageImprint              MessageImprint OPTIONAL,
     serialNumber                INTEGER OPTIONAL,
     tsaFreeData                 OCTET STRING OPTIONAL }
```

Das Versionsfeld (version) gibt die Version der Syntax an. Der Identifier „v1“ mit dem Integer-Wert „0“ identifiziert die erste Version.

Über das Policy-Feld (Policy) gibt der Zeitstempeldienst durch die Datenstruktur „Policy Information“ (s. Kapitel 6.1) an, unter welcher Policy der Zeitstempel generiert wurde. Falls der Nutzer eine bestimmte Policy im Zeitstempelantrag vorgegeben hat, so ist diese vom Zeitstempeldienst zu verwenden und im Zeitstempel einzutragen. Falls der Nutzer im Antrag keine Policy vorgegeben hat, ist die Policy „Id-sigi-sigts-sigconform“ einzutragen (s. Kapitel 6.1).

Über das Statusfeld (status) wird der Status des Zeitstempelantrages angegeben (s. Kapitel 6.2.2).

Das Namensfeld (tsa) enthält den Namen des Zeitstempeldienstes. Jeder Zeitstempeldienst muß einen Namen vom Typ „distinguished name“ haben[40], der den gleichen Aufbau wie der technische Name der ZS hat, sich jedoch unterscheiden muß, da der Zeitstempeldienst über ein eigenes Zertifikat verfügt. Der Aufbau der technischen Namen, der für alle Instanzen gleich ist, ist in Kapitel 2.3.4 [BSI-ZERT 99] beschrieben.

Das Zeitfeld (tstTime) enthält den Zeitpunkt der Generierung des Zeitstempels (s. Kapitel 6.2.3).

Das optionale Feld für zeitbezogene Daten von Zeitdatendiensten (tdaTokens) enthält die Folge der zeitbezogenen Daten, die in den Zeitstempel integriert sind.[41]

Das Referenzfeld (nonce) enthält den Integerwert, den der Nutzer im Zeitstempelantrag angegeben hat. Falls der Nutzer keinen Wert angegeben hat, bleibt das Feld leer.

Das Feld „messageImprint“ enthält den verwendeten Hash-Algorithmus und den Hashwert, die der Nutzer im Zeitstempelantrag angegeben hat. Falls der Nutzer keine Werte angegeben hat, bleibt das Feld leer (vgl. Kapitel 6.1).

---

40 Dies ist eine Beschränkung gegenüber PKIX. In Kapitel 2.4. [PKIX-TSP 98] wird die Verwendung beliebiger Namen freigestellt. Dies wäre jedoch nicht mit dem in [BSI-ZERT 99] definierten Zertifikatsformat vereinbar. Jede Instanz wird ausschließlich durch seinen technischen Namen identifiziert.

41 Das Format der zeitbezogenen Daten wird in Kapitel 6.4 beschrieben.

Das optionale Seriennummernfeld (serialNumber) kann eine Seriennummer enthalten (s. Kapitel 4.2).

Über das optionale Freitextfeld (tsaFreeData) kann der Zeitstempeldienst Daten an den Nutzer versenden. Das Feld sollte nicht verwendet werden.[42]

Konforme Zeitstempeldienste und Applikationen müssen alle Felder bis auf „tdaToken", „serialNumber" und „tsaFreeData" unterstützen.

6.2.2 Das Statusfeld

Das Statusfeld enthält folgende Datenstrukturen (vgl. Kapitel 3.2.3 [PKIX-CMP 98]):

```
PKIStatusInfo         ::= SEQUENCE {
     status               PKIStatus,
     statusString         PKIFreeText     OPTIONAL,
     failInfo             PKIFailureInfo  OPTIONAL }
```

Der Status eines Zeitstempelantrags wird durch einen der folgenden Integer-Werte angezeigt:[43]

```
PKIStatus                ::= INTEGER {
      granted                  (0),
      -- Der Zeitstempel wurde erteilt.
      rejection                (2),
      -- Der Zeitstempel wurde nicht erteilt.
      waiting                  (3),
      -- Diese Statusinformation kann als Eingangsbestätigung oder
      -- zur Anzeige von Verzögerungen dienen. }
```

Ein Zeitstempel enthält den Status-Wert „0" (granted), wenn alle Antragsvoraussetzungen für die Erteilung des Zeitstempels erfüllt sind und der Zeitstempel deshalb erteilt werden.

Die Spezifikation [PKIX-CMP 98] sieht den Status-Wert „1" (grantedWithMods) für den Fall vor, daß der Nutzer als Zeitstempel etwas anderes erhält als das, was er beantragt hat. Von dieser Variante darf der Zeitstempeldienst jedoch keinen Gebrauch machen, so daß dieser Statuswert ausscheidet.[44]

Der Status-Wert „2" (rejection) gibt an, daß der Zeitstempelantrag nicht erteilt werden kann. Gründe hierfür können z.B. ein falsches Format oder eine ungeeigneter Hashfunktion sein.

Der Status-Wert „3" (waiting) kann vom Zeitstempeldienst generell verwendet werden, um dem Nutzer anzuzeigen, daß der Zeitstempelantrag eingegangen ist. Eine solche Quittung erscheint jedoch überflüssig, da der Zeitstempeldienst ohnehin innerhalb der garantierten kurzen Antwortzeit antworten muß. Der Status-Wert ist vom Zeitstempeldienst zu verwenden, falls eine voraussichtliche Überschreitung der garantierten Antwortzeit angezeigt werden muß.

---

42 Zu beachten ist, daß der Nutzer nicht verpflichtet ist, die Daten auszuwerten und daß keinesfalls nutzerbezogene Daten auf diese Art in den Zeitstempel aufgenommen werden dürfen.

43 Es wird die Struktur aus Kapitel 3.2.3 [PKIX-CMP 98] verwendet, wobei nur die Statuswerte wiedergegeben werden, die für den Zeitstempeldienst von Bedeutung sind.

44 Der Zeitstempeldienst muß dem Antrag entsprechen, falls die Voraussetzungen dafür gegeben sind. Andernfalls muß er den Antrag ablehnen. Er darf jedoch nicht einen Zeitstempel generieren, den der Nutzer gar nicht beantragt hat.

Die Status-Werte „2“ und „3“ (rejection und waiting) müssen durch folgende Datenstruktur weiter konkretisiert werden:

```
PKIFailureInfo       ::= BIT STRING {
     badAlg              (0),
     -- ungeeignete Algorithmen verwendet.
     badMessageCheck     (1),
     -- die Gültigkeitsprüfung des Authentifikators für den Nutzer
     -- liefert einen Fehler (s. Kapitel 6.5).
     badRequest          (2),
     -- Die vom Nutzer gewünschte Transaktion ist nicht erlaubt oder
     -- wird nicht unterstützt.
     BadCertID           (4),
     -- Das Zertifikat zur Identifikation des Nutzers konnte nicht
     -- gefunden werden (s. Kapitel 6.5).
     badDataFormat       (5),
     -- Der Zeitstempelantrag ist syntaktisch fehlerhaft.
     timeNotAvailable    (14),
     -- Ein Zeitstempel kann nicht generiert werden, da die
Zeitquelle
     -- nicht zur Verfügung steht.
     tdaNotAvailable     (15),
     -- Der gewünschte Zeitstempel kann nicht generiert werden, da
     -- mindestens ein Zeitdatendienst nicht zur Verfügung steht.  }
```

Durch diese Datenstruktur können nicht alle denkbaren Fehlerfälle berücksichtigt werden. Die Datenstruktur ist jedoch stets dann verwendet werden, wenn einer der beschriebenen Fehlerfälle vorliegt. Auch in diesem Fall muß jedoch über die folgende Freitext-Nachricht der Fehler bzw. die voraussichtliche Dauer einer Verzögerung angegeben werden:

```
PKIFreeText          ::= SEQUENCE SIZE (1..MAX) OF UTF8String

UTF8String           ::= [Universal 12] IMPLICIT OCTET STRING
```

Alle Elemente des Statusfeldes müssen von Applikationen und dem Zeitstempeldienst unterstützt werden.

6.2.3 Das Zeitfeld

Das Zeitfeld (tstTime) enthält den Zeitpunkt der Generierung des Zeitstempels. Es wird folgendes Format verwendet:

```
TSTTime                  ::= SEQUENCE  {
     genTime                  GeneralizedTime,
     milliseconds             INTEGER (0..999) OPTIONAL  }
```

Für die Zeitangabe wird stets GeneralizedTime in dem Format verwendet, das in Kapitel 2.3.5 [BSI-ZERT 99] spezifiziert ist (YYYYMMDDHHMMSSZ). Wie bei allen Zeitangaben im Rahmen der Interoperabilitätsspezifikation wird auch hier Zulu-Zeit verwendet.

Die Granularität von einer Sekunde ist ausreichend. Optional können jedoch auch Millisekunden verwendet werden.

Das Zeitfeld muß von Applikationen und dem Zeitstempeldienst unterstützt werden. Das gilt jedoch nicht für das Teilfeld „milliseconds“.

6.2.4 Das Signaturfeld

Das Signaturfeld (signerInfos) enthält eine Menge von Informationen über den Ersteller der Signatur des Zeitstempels. Es wird folgende Syntax aus Kapitel 5.3 [PKIX-CMP 98] verwendet:

```
SignerInfos             ::= SET OF SignerInfo

SignerInfo              ::= SEQUENCE {
     version                   CMSVersion,
     issuerAndSerialNumber     IssuerAndSerialNumber,
     digestAlgorithm           DigestAlgorithmIdentifier,
     signedAttrs               [0] IMPLICIT SignedAttributes OPTIONAL,
     signatureAlgorithm        SignatureAlgorithmIdentifier,
     signature                 SignatureValue,
     unsignedAttrs             [1] IMPLICIT UnsignedAttributes OPTIONAL
}
```

Die Syntax sieht Mehrfachsignaturen für Zeitstempel vor. Das Feld „signerInfo“ kann deshalb mehrfach vorkommen. Ein Signaturgesetz-konformer Zeitstempeldienst muß jedoch keine Mehrfachsignaturen erzeugen können. In der Regel besteht die Menge „SET OF SignerInfo“ somit nur aus einem Element.

Das Versionsfeld (version) gibt die Version der Syntax an. Entsprechend [CMS 98] ist stets der Identifier „v1“ mit dem Integer-Wert „1“ zu verwenden.

Das Feld „issuerAndSerialNumber“ identifiziert das Signaturschlüssel-Zertifikat und damit den Signaturschlüssel, mit dem der Zeitstempel signiert wurde.[45] Es wird folgende Datenstruktur verwendet:

```
IssuerAndSerialNumber     ::= SEQUENCE {
     issuer                    Name,
     serialNumber              CertificateSerialNumber }
```

Das Ausstellerfeld (issuer) enthält den technischen Namen der ZS wie in Kapitel 2.3.4 [BSI-ZERT 99] beschrieben. Das Seriennummernfeld (serialNumber) enthält die Seriennummer wie in Kapitel 2.3.2 [BSI-ZERT 99] beschrieben.

Das Feld „digestAlgorithm“ enthält den OID für die verwendete Hashfunktion. Syntax und Inhalt des Feldes müssen mit dem Feld „digestAlgorithms“ übereinstimmen, das bereits in Kapitel 6.2 beschrieben ist.

---

45 Siehe auch Fußnote zu diesem Feld in Kapitel 5 [BSI-SIG 99].

Da dieses Feld nicht in die Signatur eingeschlossen wird, ist es vom Verifizierer nicht zu verwenden. Verwendet werden muß statt dessen das signierte Attribut vom Typ „AttrRef“, das den gleichen Inhalt hat, bzw. das signierte Attribut „Certificate“, das das Signaturschlüssel-Zertifikat enthält (s.u. Feld „signedAttrs“). Das Feld „issuerAndSerialNumber“ ist somit an sich überflüssig, darf jedoch nicht ausgelassen werden, da es nicht optional ist.

Das Feld „signedAttrs“ enthält Attribute, die in die Signatur einbezogen werden.[46] Signaturgesetz-konforme Zeitstempel müssen die folgenden vier Attribute enthalten, die in Kapitel 6 [BSI-SIG 99] beschrieben sind:

- Typ (Content Type)
- Hashwert (Message Digest)
- Signaturschlüssel-Zertifikat des Signierers bzw. Referenz darauf
- Hashverfahren (Digest Algorithm)

Das Attribut vom Typ „ContentType“ ist stets zu verwenden (vgl. Kapitel 6.1.1 [BSI-SIG 99]). Es enthält den OID für den Datentyp „Zeitstempel“. Es ist der gleiche OID zu verwenden, der bereits oben in Kapitel 6.2 als Identifikator für Zeitstempel beschrieben wurde.[47]

Das Attribut vom Typ „Message Digest“ ist aus technischen Gründen, die mit der Signaturbildung zusammen hängen, stets zu verwenden (vgl. Kapitel 6.1.2 [BSI-SIG 99]).

Ein Attribut vom Typ „Certificate“ bzw. „CertRef“ ist ebenfalls stets zu verwenden (vgl. Kapitel 6.1.3 und 6.1.4 [BSI-SIG 99]). Das Attribut spezifiziert das Zertifikat des Zeitstempeldienstes bzw. eine Referenz auf dieses Zertifikat.

Auch das Attribut vom Typ „Digest Algorithm“ ist stets zu verwenden (vgl. Kapitel 6.1.7 [BSI-SIG 99]). Das Attribut spezifiziert das vom Zeitstempeldienst im Rahmen der Signaturbildung verwendete Hashverfahren.

Weitere Attribute sind für Zeitstempel nicht erforderlich, da ein Zeitstempel ein Spezialfall einer digitalen Signatur ist. Zu einem Signaturschlüssel-Zertifikat gibt es keine Attribut-Zertifikate die ggf. in die Signatur einbezogen werden müßten. Es kann auch nicht empfohlen werden, weitere Attribute wie z.B. „Signaturdatum und Zeit“, „Quittungsanforderung“ oder „automatisch erstellte Signatur“ zu verwenden.[48]

Das Feld „signatureAlgorithm“ enthält den Algorithmus, mit dem der Zeitstempel signiert wurde. Es wird folgende Datenstruktur verwendet:

```
SignatureAlgorithmIdentifier ::= AlgorithmIdentifier
```
[49]

Das Signaturfeld (signature) enthält die Signatur als Ergebnis der Anwendung des Signatur-Algorithmus und des privaten Schlüssels auf die zu signierenden Daten. Signiert werden die Datenstruktur „TSTInfo“ und die o.g. Attribute. Die Signatur wird folgendermaßen kodiert:

```
SignatureValue ::= OCTET STRING
```

---

46 In [CMS 98] wird dieses Feld als optional angesehen, da es dem Aussteller einer digitalen Signatur freigestellt wird, Attribute in die digitale Signatur einzubeziehen. In der Tabelle 1 in Kapitel 4 [BSI-SIG 99] wird jedoch ausgewiesen, daß einige Attribute bei Signaturgesetz-konformen Signaturen stets Teil der Nachricht sein müssen. Die für Zeitstempel relevanten Attribute müssen auch stets in die Signatur einbezogen werden.

47 Der OID wird somit stets an zwei verschiedenen Stellen in den Zeitstempel eingetragen. Die Eintragung in das Feld „signedAtts“ ist erforderlich, um den OID in die digitale Signatur einzubeziehen.

48 „Signaturdatum und Zeit“ sind Teil der Datenstruktur „TSTInfo“, die bei einem Zeitstempel stets in die digitale Signatur einbezogen sind. Eines eigenen Attributes hierfür bedarf es daher nicht. Eine Quittungsanforderung ist aufgrund der garantierten kurzen Antwortzeit ebenfalls nicht erforderlich. Da Zeitstempel stets automatisch erstellt werden, muß diese Tatsache nicht eigens in einem Attribut ausgewiesen werden. Das Attribut „automatisch erstellte Signatur“ hat somit bei Zeitstempeln keine Bedeutung.

49 Die Datenstruktur „AlgorithmIdentifier“ ist in Kapitel 6.1 definiert.

Das Feld „unsignedAttrs“ ist in [PKIX-CMP 98] dafür vorgesehen, Attribute aufzunehmen, die nicht in die Signatur einbezogen werden sollen. In [BSI-SIG 99] ist nur das Attribut „Gegenzeichnung“ definiert, das in diese Klasse fällt. Gegenzeichnungen sind für Zeitstempel jedoch ohne Bedeutung.

Bis auf das Feld „unsignedAttrs“ müssen alle Felder von Applikationen und Zeitstempeldienst unterstützt werden. Bei den „signedAttrs“ müssen nur die o.g. obligatorischen Attribute unterstützt werden. Die Anmerkungen in Kapitel 6 [BSI-SIG 99] zu diesen Attributen sind zu beachten.

6.3 Anfrage zeitbezogener Daten

Eine Anfrage nach zeitbezogenenen Daten (temporal data request) hat folgendes Format:

```
TemporalDataReq                ::= SEQUENCE  {
     version                       INTEGER  { v1(0) },
     nonce                         INTEGER OPTIONAL,
     messageImprint                MessageImprint OPTIONAL }
```

Das Versionsfeld (version) gibt die Version der Syntax an. Der Identifier „v1“ mit dem Integer-Wert „0“ bezeichnet die erste Version der Syntax für die Anfrage.

Das Feld „nonce“ muß vorhanden sein, falls es im Zeitstempelantrag vorhanden ist. Der Wert muß mit dem Wert im Zeitstempelantrag übereinstimmen.

Das optionale Feld „messageImprint“ muß vorhanden sein, wenn es auch im Zeitstempelantrag vorhanden ist. Der Wert muß mit dem Wert im Zeitstempelantrag übereinstimmen.

Falls der Zeitdatendienst den Zeitstempeldienst idenfizieren will, muß die Anfrage digital signiert werden. Digital signierte Anfragen werden in Kapitel 6.5 beschrieben.

Die Anfrage zeitbezogener Daten muß von einem Signaturgesetz-konformen Zeitstempeldienst nicht unterstützt werden.

6.4 Zeitbezogene Daten

Bei Zeitdatenstempeln (temporal data token) handelt es sich um kryptographische Nachrichten vom Typ signierte Daten (signed data). Dieser Nachrichtentyp ist in Kapitel 5 [BSI-SIG 99], „Signaturaustauschformat“, beschrieben und beruht auf Kapitel 5 [CMS 98]. Die in [BSI-SIG 99] enthaltenen Regelungen für kryptographische Nachrichten vom Typ „signierte Daten“ gelten auch für Zeitdatenstempel, soweit nichts anderes bestimmt ist.

Zeitbezogene Daten haben die folgende Struktur:

```
TemporalDataToken ContentInfo  ::= SEQUENCE  {
     contentType                   OBJECT IDENTIFIER,
     content                       [0] SEQUENCE  {
          version                       CMSVersion[50],
          digestAlgorithms              digestAlgorithmIdentifiers[51],
          contentInfo                   SEQUENCE  {
              contentType                   OBJECT IDENTIFIER,
              content                       TDTInfo  }
          certificate                   [0] Certificate,
          signerInfos                   SignerInfos  }  }
```

Das Versionsfeld (version) gibt die Version der Syntax an. Es ist der Identifier „v3“ mit dem Integer-Wert „3“ anzugeben (vgl. Kapitel 6.2).

Das Feld für die Hash-Algorithmen (digestAlgorithms) dient ausschließlich dem Zweck, die Prüfung eines Zeitstempels in einem „Durchgang“ zu ermöglichen.[52]

Die Felder contentType und content enthalten die eigentlichen zeitbezogenen Daten, d.h. die Datenstruktur TDTInfo, und einen OID zur Identifizierung dieses Datentyps.

Zeitbezogene Daten werden durch folgenden OID identifiziert:

```
Id-sigi-sigts-tdttoken  OBJECT IDENTIFIER ::= { 1 3 36 8 X 3}
```

Die Datenstruktur „TDTInfo“ wird unten spezifiziert.

Das optionale Zertifikatsfeld (certificates) enthält eine Menge von Zertifikaten. Eine Notwendigkeit für die Verwendung dieses Feldes besteht nicht. Es kann davon ausgegangen werden, daß alle Zertifikate des Zertifizierungspfades aus Zertifikatsverzeichnissen abrufbar sind.

Falls das Feld verwendet wird, sollte es alle Signaturschlüssel-Zertifikate des Zertifizierungspfades von der Wurzel-Zertifizierungsstelle bis zur ZS, die das Zertifikat für den Zeitstempeldienst erstellt hat, enthalten.[53] Sinnvoll ist dies jedoch nur dann, wenn Verifizierer des Zeitstempels auf Abfragen des Verzeichnisdienstes voraussichtlich verzichten werden. Andernfalls bietet die Verwendung des Feldes keine Vorteile.

Das Informationsfeld (signerInfos) enthält eine Menge von Informationen über den Ersteller der Signatur der zeitbezogenen Daten (siehe Kapitel 6.2.4).

---

50 In Annex C5 [PKIX-TSP 98] wird an dieser Stelle der Typ „INTEGER“ angegeben. Dies führt zwar zum gleichen Ergebnis, ist aber nicht konsistent mit Kapitel 5 [CMS 98].

51 In Anhang C.5 [PKIX-TSP 98] wird an dieser Stelle der Typ „AlgorithmIdentifier“ angegeben. Dies führt in der Regel zum gleichen Ergebnis, ist allerdings inkonsistent, da die Spezifikation an sich Mehrfach-Signaturen erlaubt, die unterschiedliche Hashfunktionen verwenden können. Außerdem wird durch den Typ „AlgorithmIdentifier“ nicht zum Ausdruck gebracht, daß es sich um einen OID für eine Hash-Funktion handelt.

52 Die Datenstrukturen sind in Kapitel 6.2 beschrieben.

53 Das Signaturschlüssel-Zertifikat des Zeitstempeldienstes, bzw. eine Referenz darauf, wird stets als signiertes Attribut in die Signatur eingeschlossen (s. Kapitel 6.2.4). Die zusätzliche Aufnahme dieses Zertifikates in das Feld „certificates“ ist daher überflüssig.

Die Datenstruktur „TSTInfo“ ist wie folgt definiert:

```
TDTInfo                    ::= SEQUENCE  {
     version                      INTEGER { v1 (0) },
     nonce                        INTEGER  OPTIONAL[54],
     temporalData                 TemporalData,
     messageImprint               MessageImprint OPTIONAL,
     serialNumber                 INTEGER OPTIONAL  }
```

Das Versionsfeld (version) gibt die Version der Syntax an. Der Identifier „v1“ mit dem Integer-Wert „0“ bezeichnet die erste Version der Syntax für die zeitbezogenen Daten.

Das Referenzfeld (nonce) enthält den Integerwert, den der Nutzer im Zeitstempelantrag angegeben hat. Falls der Nutzer keinen Wert angegeben hat, bleibt das Feld leer.

Das Zeitdatenfeld (temporalData) enthält die zeitbezogenen Daten in folgendem Format:

```
TemporalData               ::= SEQUENCE {
     format                       OBJECT IDENTIFIER,
     rawdata                      ANY DEFINED BY format  }
```

Der OID für das Format der zeitbezogenen Daten ist vom Zeitdatendienst registrieren zu lassen.

Das Feld „messageImprint“ enthält den verwendeten Hash-Algorithmus und den Hashwert aus dem Zeitstempelantrag. Falls in der Anfrage keine Werte angegeben sind, bleibt das Feld leer.

Das optionale Seriennummernfeld (serialNumber) kann eine Seriennummer enthalten (s. Kapitel 6.2.1).

Zeitbezogene Daten müssen von einem Signaturgesetz-konformen Zeitstempeldienst nicht unterstützt werden.

6.5 Digital signierte Anträge und Anfragen

Digital signierte Anträge und Anfragen sind kryptographische Nachrichten vom Typ signierte Daten (signed data). Dieser Nachrichtentyp ist in Kapitel 5 [BSI-SIG 99], „Signaturaustausch-format“, beschrieben und beruht auf Kapitel 5 [CMS 98]. Die in [BSI-SIG 99] enthaltenen Regelungen für kryptographische Nachrichten vom Typ „signierte Daten“ gelten auch für digital signierte Anträge und Anfragen, soweit nichts anderes bestimmt ist.

Ein signierter Zeitstempelantrag (bzw. eine digital signierte Anfrage zeitbezogener Daten) wird im folgenden als „signedTSreq“ (bzw. „signedTDreq“) bezeichnet. Die in Kapitel 6.1 (bzw. Kapitel 6.3) beschriebenen Datenstrukturen „TimeStampReq“ (bzw. „TemporalDataReq“) sind in diese Nachrichten eingebettet.

[54] Die Kennzeichnung des Feldes als optional fehlt in Anhang C.5 [PKIX-TSP 98].

Für den signierten Zeitstempelantrag ergibt sich folgende Datenstruktur:

```
signedTSreq ContentInfo      ::= SEQUENCE {
     contentType                 OBJECT IDENTIFIER,
     content                     [0] SEQUENCE  {
          version                     CMSVersion,
          digestAlgorithms            digestAlgorithmIdentifiers[55],
          ContentInfo                 SEQUENCE {,
               contentType                 OBJECT IDENTIFIER,
               content                     TimeStampReq }
          certificates                [0] IMPLICIT CertificateSet
                                      OPTIONAL,
          signerInfos                 SignerInfos  }  }
```

Alle Felder sind bereits in Kapitel 6.2 beschrieben. Bis auf das Feld „certificates“ müssen alle Felder von Applikationen unterstützt werden. Der Zeitstempeldienst kann auf die Unterstützung verzichten, falls die Nutzer nicht identifiziert werden sollen.

Der Zeitstempeldienst kann anhand des Attributs „Certificate“ bzw. „CertRef“ des signierten Zeitstempelantrags das Zertifikat des Antragstellers bestimmen. Im Zertifikat ist der „distinguished name“ des Antragstellers enthalten, der ihn eindeutig identifiziert.

7 Transportprotokolle

Für den Transport von Zeitstempelanträgen und Zeitstempeln (sowie von Anfragen zeitbezogener Daten und zeitbezogener Daten) kommen eine Vielzahl von Protokollen in Betracht. Da vom Zeitstempeldienst nicht erwartet werden kann, eine unbestimmte Vielzahl von Protokollen zu implementieren, muß eine Auswahl getroffen werden.[56]

Der Zeitstempeldienst soll sowohl mit Online- als auch mit Offline-Protokollen erreichbar sein.[57] Offline-Protokolle sind für Zeitstempel geeignet, da der Nutzer insbesondere dann, wenn er als Empfänger einer Nachricht einen Zeitstempel beantragt, auf die Ausstellung des Zeitstempels nicht warten muß.[58] Die anschließende Archivierung der Nachricht zusammen mit dem Zeitstempel ist in der Regel nicht zeitkritisch.[59]

---

55 In Kapitel 2.4 [PKIX-TSP 98] wird an dieser Stelle der Typ „AlgorithmIdentifier“ angegeben. Dies führt in der Regel zum gleichen Ergebnis, ist allerdings inkonsistent, da die Spezifikation an sich Mehrfach-Signaturen erlaubt, die unterschiedliche Hashfunktionen verwenden können. Außerdem wird durch den Typ „AlgorithmIdentifier“ nicht zum Ausdruck gebracht, daß es sich um einen OID für eine Hash-Funktion handelt.

56 In die Auswahl müssen keine Sicherheitsprotokolle wie z.B. S-HTTP, SSL, TSL oder SET einbezogen werden, da die zu übertragenden Daten bereits in ausreichend gesicherter Form vorliegen.

57 Ein Protokoll wird im folgenden als Online-Protokoll bezeichnet, wenn der Zeitraum zwischen der Übermittlung des Zeitstempelantrags bis zur Entgegennahme des Zeitstempels im wesentlichen nur von der Bearbeitungszeit des Zeitstempeldienstes abhängig ist. Das setzt voraus, daß die Laufzeiten für den Transport der Nachrichten gegenüber der Bearbeitungszeit nicht ins Gewicht fallen.

58 Es kann die Prüfung des Zeitstempels auf einen späteren Zeitpunkt verschieben.

59 Deshalb steht die Verwendung von Offline-Protokollen für den Zeitstempeldienst nicht im Widerspruch zu Kapitel 2.4 [BSI-DIR 99], in dem E-Mail als für den Verzeichnisdienst nicht geeignet angesehen wird.

Das Simple Mail Transfer Protocol (SMTP) zum Transport von E-Mail ist aufgrund der weiten Verbreitung und der Verfügbarkeit von Proxies für Firewalls ein besonders geeignetes Offline-Protokoll.

Neben dem Transport von E-Mail muß ein Zeitstempeldienst Online-Protokolle unterstützten. Insbesondere dann, wenn der Zeitstempel vom Absender einer Nachricht beantragt wird und zusammen mit der Nachricht versendet werden soll, kann die Beschaffung einer Zeitstempels zeitkritisch sein.

Ein geeignetes Online-Protokoll ist das Hypertext Transfer Protocol (HTTP). Die Verwendung von HTTP [RFC 2068 97] erlaubt eine einfache Erstellung von Software für den Zugriff auf Zeitstempeldienste unter Verwendung erprobter Programmbibliotheken. Das Protokoll ist weit verbreitet und Proxies für Firewalls sind in der Regel verfügbar.

Ein weiteres geeignetes Protokoll ist das File Transfer Protokoll (FTP). Diesem Protokoll kommt neben HTTP, das FTP umfaßt, kaum noch eine eigenständige Bedeutung zu. Aus diesem Grund wird nicht gefordert, daß der Zeitstempeldienst eine eigene Schnittstelle für FTP-Nachrichten bereitstellt.

Speziell für den Transport von PKI-Nachrichten wird in Kapitel 5.2 [PKIX-CMP 98] ein direktes TCP-basiertes Protokoll spezifiziert. Dieses Protokoll zeichnet sich durch seine Einfachheit aus. Die ausgetauschten Nachrichten beschränken sich auf das absolute Minimum, so daß dieses Protokoll aus Kostengründen vorteilhaft sein kann. Der Entwicklungsaufwand für die Erstellung von Software für dieses Protokoll ist äußerst gering.

Die Spezifikation umfaßt somit ein Offline-Protokoll (für E-Mail) und zwei Online-Protokolle (HTTP und TCP-basiert). Ein Zeitstempeldienst muß aus Gründen der Interoperabilität alle diese Protokolle realisieren, um Zeitstempelanträge entgegennehmen und Zeitstempel versenden zu können. Die Software der Nutzers muß jedenfalls ein Online-Protokoll realisieren. Da alle Protokolle im konkreten Anwendungsfall Vor- und Nachteile haben können, empfiehlt sich die Implementierung aller Protokolle.

7.1 E-Mail

Alle der in Kapitel 6 spezifizierten Nachrichtenformate können per E-Mail ausgetauscht werden. Die Nachrichtenformate müssen so konvertiert werden, daß sie über einfache Transportmechanismen für Internet-Mail übertragen werden können.

Das folgende einfache MIME-Objekt dient diesem Zweck:

```
Content-Type: application/timestamp
Content-Transfer-Encoding: base64

<< ASN.1-DER-kodierte Nachricht, die base64 kodiert ist >>
```

Die Aufgabe der Kopfzeile „Content-Type“ ist es, die Daten des Rumpfes so genau zu beschreiben, daß sie auf Empfängerseite automatisch weiterverarbeitet werden können. Durch die Typangabe „application/timestamp“[60] wird angegeben, daß es sich um Nachrichten im Zusammenhang mit Zeitstempeln handelt. Eine weitere Unterscheidung der Nachrichtenformate ist nicht erforderlich.

Die auszutauschenden Nachrichten werden zunächst ASN.1-DER codiert.[61] Die so kodierten Nachrichten können als binäre Daten ohne eine weitere Kodierung nur über 8-Bit-transparente

---

60 Vgl. Kapitel 5 [MIME1 96] und Kapitel 4.5.3 [MIME2 96].

61 Die Kodierung der in Kapitel 6 spezifizierten ASN.1-Formate nach den „Distinguished Encoding Rules“ (DER) [ITU-T X.690 94] ist eindeutig.

Übertragungsmedien ausgetauscht werden. Es ist deshalb eine Transportkodierung (Content-Transfer-Encoding) vorzunehmen, die die Abhängigkeit vom Transportmedium aufhebt. Die Transportkodierung „Base64“ leistet dies. Sie ist in Kapitel 6.8 [MIME1 96][62] definiert.

Das so definierte MIME-Objekt ist um die Angabe der verwendeten MIME-Version[63] zu ergänzen und wird dann in einen RFC 822-Nachrichtenkopf (vgl. [RFC 822 82]) integriert. Der Rumpf der Nachricht enthält die kodierten Nutzdaten.

7.2 HTTP

Alle in Kapitel 6 spezifizierten Nachrichtenformate können per HTTP ausgetauscht werden. Die Nachrichten werden so in ein MIME-Objekt intergriert, daß sie über allgemeine Verbindungen zwischen Browsern und WWW-Servern übertragen werden können.

Das folgende einfache MIME-Objekt dient diesem Zweck:

```
Content-Type: application/timestamp

<< ASN.1-DER kodierte Nachricht >>
```

Die Aufgabe der Kopfzeile „Content-Type“ ist es, wie bei E-Mail, die Daten des Rumpfes so genau zu beschrieben, daß sie auf Empfängerseite automatisch weiterverarbeitet werden können.[64]

HTTP-Zeitstempelanträge enthalten in der ersten Zeile (Request-Line) die verwendete Methode (GET oder POST), einen Universal Resource Identifier (URI), der auf den Prozeß zur Generierung des Zeitstempels verweist, und die Protokoll-Version (vgl. Kapitel 5 [HTTP 97]). Der URI ist dabei entweder lokal in der Applikation gespeichert oder kann durch Verwendung einer der in Anhang II zu [BSI-ZERT 98] beschriebenen Methoden abgeleitet wird.

Auf die erste Zeile folgen das o.g. Feld „Content-Type“ und dem Rumpf, d.h. dem DER-kodierten Antrag (vgl. Kapitel 7 [HTTP 97]).

Ein HTTP-Zeitstempel besteht ebenfalls aus Kopfzeilen und dem DER-kodierten Zeitstempel. Die erste Zeile (Status-Line) gibt den Status des Antrags an (vgl. Kapitel 6 [HTTP 97]. Die Kopfzeile „Content-Type“ identifiziert das MIME-Objekt.

7.3 TCP-basiertes Protokoll

Alle in Kapitel 6 spezifizierten Nachrichtenformate können über ein direktes TCP-basiertes Protokoll übertragen werden. Der Nutzer[65] übermittelt einen Zeitstempelantrag und erhält den Zeitstempel entweder sofort oder ruft ihn später beim Zeitstempeldienst ab (polling).

Der Zeitstempeldienst muß einen Prozeß installieren, der Nachrichten über einen wohldefinierten Port (Portnummer 309) entgegennimmt.

---

62 Die Kodierung ist fast identisch mit der in PEM [RFC 1421 93] beschriebenen Kodierung.

63 Vgl. Kapitel 4 [MIME1 96].

64 Im Gegensatz zu E-Mail ist eine base64-Kodierung bei HTTP nicht erforderlich.

65 Bei der Beschreibung der Protokolls werden der Einfachheit halber nur die Instanzen Nutzer und Zeitstempeldienst verwendet. Das Protokoll kann jedoch ebenso für die Kommunikation zwischen Zeitstempeldienst und Zeitdatendienst verwendet werden.

Die Nachrichten werden wie folgt kodiert:[66]

```
length (32-Bits), flag (8-Bits), value
```

Das Längenfeld (length) enthält die Anzahl der Oktette des Restes der Nachricht, das Flag gibt den Typ der Nachricht an und das Wertefeld (value) enthält die Nachricht selbst.

Es werden folgende Nachrichtentypen definiert:

Nachrichtentyp	Flag	Nachricht
msgReq	„00“ H	DER-kodierter Zeitstempelantrag
pollRep	„01“ H	Polling-Referenz; Zeitpunkt für nächstes Polling
pollReq	„02“ H	Polling-Referenz
finalMsgreq	„05“ H	DER-kodierter Zeitstempel
errorMsgRep	„06“ H	Lesbare Fehlermeldung

Das TCP-basierte Protokoll soll nicht nur für den Zeitstempeldienst, sondern für alle Dienste verwendet werden können, die einen Nachrichtenaustausch zwischen Nutzer und ZS erfordern. In der vorliegenden Spezifikation des Zeitstempeldienstes werden nur die Nachrichtentypen beschrieben, die tatsächlich verwendet werden.[67]

Nachdem der Nutzer den Zeitstempelantrag als Nachricht vom Typ „msgReq“ an den Zeitstempeldienst versandt hat, erhält er vom Zeitstempeldienst entweder den DER-kodierten Zeitstempel (Nachrichtentyp „finalMsgReq“[68]), bzw. eine Fehlermeldung, oder eine Polling-Referenz (Nachrichtentyp „pollRep“).

Es ist von der Bearbeitungszeit des Zeitstempelantrags abhängig, ob der Nutzer auf den Antrag hin sofort den Zeitstempel erhält. Falls die Generierung des Zeitstempels längere Zeit in Anspruch nimmt, erhält der Nutzer statt des Zeitstempels eine Polling-Referenz, mit der er den Zeitstempel später abfragen kann. Zusammen mit der Polling-Referenz erhält er eine Zeitangabe, die ihm anzeigt, wann sein Zeitstempel voraussichtlich abrufbar sein wird.[69]

Die Polling-Referenz besteht aus 32-Bits. Die Werte für die Polling-Referenz müssen verschieden sein, wenn ein Nutzer mehrere Anträge stellt. Weitere Anforderungen an die Werte bestehen nicht.

Der Zeitpunkt für das nächste Polling wird als Integer-Wert der Länge 32-Bits angegeben. Der Integer-Wert entspricht der UNIX-Konvention und gibt die Anzahl der Sekunden seit dem 1. Januar 1970 wieder, wobei zeitzonenunabhängig Universal Time Code (UTC) verwendet wird.

Eine Nachricht vom Typ „errorMsgRep“ ist eine Fehlermeldung. Sie wird zum Beispiel dann gesendet, wenn die Polling-Referenz ungültig ist oder der Zeitstempel bereits gesendet wurde.

---

66 Vgl. Kapitel 5.2 [PKIX-CMP 98].

67 Aus diesem Grunde fehlen die Flags „03“ und „04“ H in der Tabelle.

68 Ein Zeitstempel als Antwort auf einen Antrag wird stets in einer Nachricht übermittelt. Die Nachricht wird als „final“ bezeichnet, da es keine Teilnachrichten gibt.

69 Da Zeitstempel stets innerhalb der garantierten kurzen Antwortzeit zur Verfügung gestellt werden müssen, kommt dieser Variante in der Regel keine wesentliche Bedeutung zu. Da das Protokoll jedoch im Rahmen der Gesamtspezifikation auch für andere Dienste verwendet werden soll, wird diese Variante vom Protokoll allgemein berücksichtigt. Es bleibt dem Zeitstempeldienst überlassen, von dieser Variante Gebrauch zu machen oder nicht.

Die Nachricht muß eine für den Nutzer lesbare Form haben und die Art des Fehlers erkennen lassen. Für die Nachricht ist das Format „UTF8String“ zu verwenden (vgl. Kapitel 6.2.2).

8 Assoziierung von digitalen Daten und Zeitstempeln

Ein Zeitstempel ist ohne die gesicherten Daten, deren Hashwert er enthält, bedeutungslos. Deshalb wird ein Verfahren benötigt, daß es den Nutzern erlaubt, die digitalen Daten zusammen mit den Zeitstempeln sicher zu speichern. Das Verfahren kann insbesondere auch verwendet werden, wenn die signierten Daten zusammen mit dem Zeitstempel und einer Quittungsanforderung versendet werden sollen (vgl. Kapitel 3.2).

Das im folgenden beschriebene Verfahren ist optional, da eine entsprechende Anforderung aus SigG/SigV nicht abgeleitet werden kann. Eine Implementierung des Verfahrens in Applikationen wird jedoch empfohlen.

Die signierten Daten werden in eine weitere Datenstruktur vom Typ signierte Daten (signed data) eingebettet. Diese Datenstruktur enthält auch den Zeitstempel in Form eines signierten Attributs. Die signierten Daten und der zugehörige Zeitstempel werden dann signiert, wodurch die Integrität gesichert wird. Beide Teile werden so gesichert miteinander verbunden.

Dieses Verfahren ist im Anhang A [PKIX-TSP 98] beschrieben. Dort wird ein Zeitstempel-Attribut definiert. Allerdings fehlt die Zuweisung eines OIDs für das Attribut.

Der OID zur Identifizierung des Attributs für den Zeitstempel ist:

```
Id-sigi-sigts-tstattrib  OBJECT IDENTIFIER ::= { 1 3 36 8 X 4}
```

Im folgenden werden mögliche Anwendungen der Assoziierung beschrieben.

Falls die digitalen Daten mit der Zeitstempel assoziiert werden, um sie in einer einzigen Datenstruktur archivieren so können, ist diese von der Person zu signieren, die für die Archivierung zuständig ist. Die Signatur wird ausschließlich für die Zwecke der Archivierung verwendet. Die Prüfung der Signatur soll nicht die Prüfung der Daten und des Zeitstempels ersetzen. Aufgabe der Signatur ist es nur, die Daten und den Zeitstempel integritätsgeschützt zusammenzuhalten.

Falls die Archivierung durch eine vertrauenswürdige Instanz wie z.B. einem Notariatsdienst erfolgt (vgl. Kapitel 4.1), kann es sinnvoll sein, in die Signatur als weiteres Attribut den Signaturzeitpunkt aufzunehmen, um den Zeitpunkt der Vorlage bei der vertrauenswürdigen Instanz dadurch belegen zu können.[70]

Falls die digitalen Daten mit dem Zeitstempel assoziiert werden, um sie an den Empfänger der Nachricht zu versenden, wird die gemeinsame Datenstruktur in der Regel durch den Absender selbst signiert. Der Zweck der Signatur besteht in diesem Fall insbesondere darin, eine Quittungsanforderung in die Signatur einbeziehen zu können. Die Quittungsanforderung bezieht sich dann sowohl auf die digitalen Daten, als auch auf den Zeitstempel (vgl. Kapitel 4.1).

Im folgenden werden optionale Dateinamenserweiterungen spezifiziert, deren Verwendung empfohlen wird. Für Zeitstempel wird „.tst“ (für timestamp), für die oben spezifizierte Datenstruktur wird „.sts“ (für signed timestamp structure) empfohlen.

---

[70] Es muß dafür jedoch davon ausgegangen werden, daß diese Instanz implizites Vertrauen genießt, nur korrekte Zeitangaben zu machen.

9 Literatur

[BAZ140298] Bundesanzeiger vom 14. Februar 1998, Nr.31, pp. 1787-1788

[BSI-DIR 99] BSI; Spezifikation zur Entwicklung interoperabler Verfahren und Komponenten nach SigG/SigV; Verzeichnisdienst; Stand 31.01.1999

[BSI-SIG 99] BSI; Spezifikation zur Entwicklung interoperabler Verfahren und Komponenten nach SigG/SigV; Signatur; Stand März 1999

[BSI-ZERT 99] BSI; Spezifikation zur Entwicklung interoperabler Verfahren und Komponenten nach SigG/SigV; Zertifikate; Stand 31.01.1999

[CMS 98] S/MIME Working Group; Cryptographic Message Syntax; (work in progress) Stand: Oktober 1998

[HTTP 97] RFC 2068; Hypertext Transfer Protocol - HTTP/1.1; Januar 1997

[ITU-T X.690 94] ITU-T X.690: Information Technology - ASN.1 Encoding Rules - Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER); 1994

[MIME1 96] RFC 2045; Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies; November 1996

[MIME2 96] RFC 2046; Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types; November 1996

[MKAT 97] Regulierungsbehörde für Telekommunikation und Post; Maßnahmenkatalog für digitale Signaturen; Version 1.0; November 1997

[PKIX-CMP 98] Internet X.509 Public Key Infrastructure; Certificate Management Protocols; (work in progress) Stand: May 1998

[PKIX-TSP 98] Internet X.509 Public Key Infrastructure; Time Stamp Protocols; (work in progress) Stand: 23. September 1998

[RFC 822 82] RFC 822; Standard for the Format of ARPA Internet Text Messages; 1982

[RFC 1421 93] RFC 1421; Privacy Enhancement for Internet Electronic Mail: Part I: Message Encryption and Authentication Procedures; 1993

Anhang A: ASN.1 Definitionen

```
AlgorithmIdentifier      ::= SEQUENCE  {
     algorithm               OBJECT IDENTIFIER
     parameters              ANY DEFINED BY algorithm OPTIONAL }

CMSVersion ::= INTEGER  { v0(0), v1(1), v2(2), v3(3), v4(4) }

ContentInfo              ::= SEQUENCE  {
     contentType             OBJECT IDENTIFIER
     content                 [0] EXPLICIT ANY DEFINED BY contentType
}
DigestAlgorithmIdentifier  ::= AlgorithmIdentifier

DigestAlgorithmIdentifiers ::= SET OF DigestAlgorithmIdentifier

IssuerAndSerialNumber    ::= SEQUENCE {
     issuer                  Name,
     serialNumber            CertificateSerialNumber }

MessageImprint           ::= SEQUENCE  {
     hashAlgorithm           AlgorithmIdentifier,
     hashedMessage           OCTET STRING  }

PKIFailureInfo           ::= BIT STRING {
     badAlg                  (0),
     -- ungeeignete Hash- oder Signaturfunktion verwendet.
     badMessageCheck         (1),
     -- die Gültigkeitsprüfung des Authentifikators für den Nutzer
     -- liefert einen Fehler.
     badRequest              (2),
     -- Die vom Nutzer gewünschte Transaktion ist nicht erlaubt oder
     -- wird nicht unterstützt.
     BadCertID               (4),
     -- Das Zertifikat zur Identifikation des Nutzers konnte nicht
     -- gefunden werden.
     badDataFormat           (5),
     -- Der Zeitstempelantrag ist syntaktisch fehlerhaft.
     timeNotAvailable        (14),
     -- Ein Zeitstempel kann nicht generiert werden, da die
Zeitquelle
     -- nicht zur Verfügung steht.
     tdaNotAvailable         (15),
     -- Der gewünschte Zeitstempel kann nicht generiert werden, da
     -- mindestens ein Zeitdatendienst nicht zur Verfügung steht.  }

PKIStatus                ::= INTEGER  {
      granted                (0),
      -- Der Zeitstempel wurde erteilt.
      rejection              (2),
      -- Der Zeitstempelantrag wurde nicht erteilt.
      waiting                (3),
      -- Diese Statusinformation kann als Eingangsbestätigung oder
      -- zur Anzeige von Verzögerungen dienen. }

PKIStatusInfo            ::= SEQUENCE {
     status                  PKIStatus,
     statusString            PKIFreeText     OPTIONAL,
     failInfo                PKIFailureInfo  OPTIONAL }
```

```
PolicyInformation         ::= SEQUENCE  {
     policyIdentifier         ReqPolicyId
     policyQualifier          SEQUENCE SIZE (1..MAX) OF
                              PolicyQualifierInfo OPTIONAL }

PolicyQualifierId         ::= OBJECT IDENTIFIER

PolicyQualifierInfo       ::= SEQUENCE  {
     policyQualifierId        PolicyQualifierId
     qualifier                ANY DEFINED BY policyQualifierId }

ReqPolicyId               ::= OBJECT IDENTIFIER

SignatureAlgorithmIdentifier ::= AlgorithmIdentifier

SignatureValue            ::= OCTET STRING

SignerInfo                ::= SEQUENCE {
     version                  CMSVersion,
     issuerAndSerialNumber    IssuerAndSerialNumber,
     digestAlgorithm          DigestAlgorithmIdentifier,
     signedAttrs              [0] IMPLICIT SignedAttributes OPTIONAL,
     signatureAlgorithm       SignatureAlgorithmIdentifier,
     signature                SignatureValue,
     unsignedAttrs            [1] IMPLICIT UnsignedAttributes
OPTIONAL}

SignerInfos               ::= SET OF SignerInfo

TDTInfo                   ::= SEQUENCE  {
     version                  INTEGER  { v1(0) },
     nonce                    INTEGER OPTIONAL,
     temporalData             TemporalData,
     messageImprint           MessageImprint OPTIONAL,
     serialNumber             INTEGER OPTIONAL  }

TemporalData              ::= SEQUENCE {
     format                   OBJECT IDENTIFIER,
     rawdata                  ANY DEFINED BY format  }

TemporalDataReq           ::= SEQUENCE  {
     version                  INTEGER  { v1(0) },
     nonce                    INTEGER OPTIONAL,
     messageImprint           MessageImprint OPTIONAL }

TimeStampReq              ::= SEQUENCE  {
     version                  INTEGER { v1(0) },
     reqPolicy                PolicyInformation OPTIONAL,
     tdas                     SEQUENCE OF GeneralName OPTIONAL,
     nonce                    Integer OPTIONAL
     messageImprint           MessageImprint OPTIONAL }

TemporalDataToken ContentInfo  ::= SEQUENCE  {
     contentType                 OBJECT IDENTIFIER,
     content                     [0] SEQUENCE  {
          version                     CMSVersion,
          digestAlgorithms            digestAlgorithmIdentifiers,
          contentInfo                 SEQUENCE  {
```

```
            contentType                 OBJECT IDENTIFIER,
            content                     TDTInfo  }
        certificate                 [0] Certificate,
        signerInfos                 SignerInfos  }  }

TimeStampToken ContentInfo     ::= SEQUENCE {
     contentType                    OBJECT IDENTIFIER,
     content                        [0] SEQUENCE  {
          version                        CMSVersion,
          digestAlgorithms               digestAlgorithmIdentifiers,
          ContentInfo                    SEQUENCE {,
               contentType                    OBJECT IDENTIFIER,
               content                        TSTInfo }
          certificates                   [0] IMPLICIT CertificateSet
                                         OPTIONAL,
          signerInfos                    SignerInfos  }  }

TSTInfo                  ::= SEQUENCE  {
     version                    INTEGER  { v1(0) },
     policy                     PolicyInformation,
     status                     PKIStatusInfo,
     tsa                        GeneralName,
     tstTime                    TSTTime,
     tdaTokens                  SEQUENCE OF TemporalDataToken OPTIONAL,
     nonce                      INTEGER OPTIONAL,
     messageImprint             MessageImprint OPTIONAL,
     serialNumber               INTEGER OPTIONAL,
     tsaFreeData                OCTET STRING OPTIONAL }

TSTTime                  ::= SEQUENCE  {
     genTime                    GeneralizedTime,
     milliseconds               INTEGER (0..999) OPTIONAL  }
```

Anhang B: Objektbezeichner

```
Id-sigi                    OBJECT IDENTIFIER ::= { 1 3 36 8 }

Id-sigi-sigts              OBJECT IDENTIFIER ::= { 1 3 36 8 X[71]}

Id-sigi-sigts-sigconform   OBJECT IDENTIFIER ::= { 1 3 36 8 X 1}

Id-sigi-sigts-tsttoken     OBJECT IDENTIFIER ::= { 1 3 36 8 X 2}

Id-sigi-sigts-tdttoken     OBJECT IDENTIFIER ::= { 1 3 36 8 X 3}

Id-sigi-sigts-tstattrib    OBJECT IDENTIFIER ::= { 1 3 36 8 X 4}

id-signedData OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840)
                                      rsadsi(113549) pkcs7(7) 2 }
```

[71] Der Wert für „sigts“ ist noch festzulegen.