

Intervall-qualifizierte Zeitstempel

Detlef Hühnlein

secunet Security Networks AG
Sudetenstraße 16, D-96247 Michelau
detlef.huehnlein@secunet.com

Zusammenfassung

Dieser Beitrag erläutert die Konstruktion Intervall-qualifizierter (IQ) Zeitstempel, die in vielen Anwendungsfällen als kostengünstige Alternative zu qualifizierten Zeitstempeln gemäß §2 Nr. 14 des deutschen Signaturgesetzes dienen können. Hierbei wird ein zum Zeitpunkt t_i erstellter IQ-Zeitstempel mit zwei zum Zeitpunkt T_1 bzw. T_2 erstellten qualifizierten Zeitstempeln verknüpft, so dass bewiesen werden kann dass $T_1 < t_i < T_2$.

1 Einleitung

Im Rahmen der elektronischen Abwicklung von Geschäftsprozessen werden Zeitstempel zur verbindlichen Verknüpfung elektronischer Daten mit Zeitattributen eingesetzt. Muss die mit den Nutzdaten verknüpfte Zeitinformation hohe Beweiskraft, z. B. bei Streitfällen vor Gericht, entfalten, so ist der Einsatz qualifizierter Zeitstempel gemäß §2 Nr. 14 [SigG] geboten. Ein solcher qualifizierter Zeitstempel ist eine „Bescheinigung eines Zertifizierungsdiensteanbieters“ (ZDA), der die anspruchsvollen Anforderungen des deutschen Signaturgesetzes (§§ 4 bis 14 und §17 oder §23 SigG) und der Signaturverordnung erfüllt, dass ihm „bestimmte elektronische Daten zu einem bestimmten Zeitpunkt“ vorgelegen haben. Ein wichtiges Einsatzgebiet qualifizierter Zeitstempel ist die langfristige Datensicherung gemäß §17 [SigV]. Deshalb darf erwartet werden, dass der Bedarf an qualifizierten Zeitstempeln mit der weiteren Verbreitung der qualifizierten elektronischen Signatur signifikant steigt. Für das Ausstellen von qualifizierten Zeitstempeln werden typischerweise transaktionsabhängige Gebühren erhoben, die sich bei einer großen Anzahl an benötigten Zeitstempeln als signifikanter Kostenfaktor erweisen. Deshalb wäre es wünschenswert, Zeitstempel mit ähnlich hohem Beweiswert, aber deutlich geringeren Kosten zu ermöglichen.

Bei den hier vorgestellten IQ-Zeitstempeln wird dies dadurch realisiert, dass nicht für jedes zeitzustempelnde Dokument bei einem ZDA ein qualifizierter Zeitstempel angefordert wird, sondern diese kostenintensive externe Dienstleistung nur sporadisch, beispielsweise einmal täglich, in Anspruch genommen wird und als vertrauenswürdiger Bezugspunkt für die Ausstellung selbsterzeugter Zeitstempel dient. Durch den geschickten Einsatz einer kryptographischen Hashfunktion, deren Einwegigkeit eine relative zeitliche Ordnung zwischen den verschiedenen (qualifizierten und selbsterzeugten) Zeitstempeln induziert, kann – unter übli-

chen kryptographischen Annahmen – bewiesen werden, dass der IQ-Zeitstempel in der Zeit zwischen zwei bestimmten qualifizierten Zeitstempeln erstellt wurde. Somit kann durch das tägliche Anfordern eines einzigen qualifizierten Zeitstempels das Erstellungsdatum von beliebig vielen organisationsinternen Zeitstempeln mit dem hohen Beweiswert qualifizierter Zeitstempel versehen werden. Damit kann bei den meisten Applikationen der Einsatz kostenintensiver qualifizierter Zeitstempel durch IQ-Zeitstempel ersetzt werden. Die kurze Wirtschaftlichkeitsbetrachtung in Abschnitt 3.4 zeigt, dass sich eine Investition in Systeme zur Erstellung von IQ-Zeitstempeln bereits nach einem Jahr amortisiert, sofern täglich etwa 400 Zeitstempel benötigt werden.

Die vorliegende Arbeit ist folgendermaßen gegliedert: Nachdem in Abschnitt 2 die nötigen Grundlagen zusammengetragen wurden, widmet sich Abschnitt 3 den hier vorgeschlagenen Intervall-qualifizierten Zeitstempeln. Die wesentlichen Aspekte dieser Arbeit werden schließlich in Abschnitt 4 zusammengefasst. Im Anhang finden sich einige Informationen zur Syntax von Zeitstempeln in CMS [RFC3369] und TSP [RFC3161].

2 Grundlagen

In diesem Abschnitt sollen einige in dieser Arbeit verwendeten Begriffe und zugehörige Grundlagen zu selbsterzeugten und qualifizierten Zeitstempeln zusammengetragen werden.

2.1 Begriffsbestimmungen

„*Zeitstempel*“ sind digitale Daten, mit denen die Existenz bestimmter Daten vor einem bestimmten Zeitpunkt bewiesen werden kann (vgl. [ISO-18014]).

Der „*Beweiswert*“ eines Zeitstempels ist proportional zur Schwierigkeit, einen Augenscheinsbeweis gemäß §§371 - 372 ZPO zu erschüttern oder gar zu widerlegen – je schwieriger es für die Gegenpartei ist, den Beweis zu erschüttern oder zu widerlegen, desto höher ist der Beweiswert.

Zeitstempel werden von einem „*Zeitstempeldienst*“ erzeugt, der entweder organisationsintern oder von einer vertrauenswürdigen dritten Partei betrieben wird.

Tritt diese dritte Partei als „*Zertifizierungsdiensteanbieter*“ gemäß Signaturgesetz auf und erfüllt sie mindestens die Anforderungen der §§4 – 14 und §17 oder §23 SigG und SigV, so handelt es sich um „*qualifizierte Zeitstempel*“ gemäß §2 Nr. 14 SigG.

Da nicht-qualifizierte Zeitstempel von beliebigen organisationsinternen Zeitstempeldiensten selbst erzeugt werden können, bezeichnen wir sie in dieser Arbeit als „*selbsterzeugte Zeitstempel*“.

„*Intervall-qualifizierte Zeitstempel*“ sind selbsterzeugte Zeitstempel von denen bewiesen werden kann, dass sie im Zeitintervall zwischen zwei bestimmten qualifizierten Zeitstempeln ausgestellt worden sind.

2.2 Selbsterzeugte und qualifizierte Zeitstempel

Die qualitativen Unterschiede zwischen selbsterzeugten und qualifizierten Zeitstempeln, die insbesondere auch den Beweiswert der Zeitstempel (vgl. Abschnitt 3.3) beeinflussen, ergeben

sich anhand der minimalen¹ in SigG und SigV definierten Anforderungen, die ein Anbieter qualifizierter Zeitstempel² erfüllen muss:

- Nachweisliche Zuverlässigkeit und Fachkunde (§4 SigG und §5 SigV)
- Sicherheitskonzept (§4 SigG und §2 SigV)
- Dokumentation (§10 SigG und §8 SigV)
- Haftung (§11 SigG)
- Deckungsvorsorge (§12 SigG und §9 SigV)
- Geprüfte³ technische Komponenten, die die Fälschung oder Verfälschung von Zeitstempeln ausschließen und eine Herstellererklärung oder Bestätigung aufweisen (§17 SigG, §15 SigV und Anlage 1 SigV)

Da bei organisationsinternen Zeitstempeldiensten auf die meisten dieser anspruchsvollen – und in der Umsetzung vergleichsweise kostenintensiven – Anforderungen grundsätzlich verzichtet werden könnte, ist es wenig verwunderlich, dass selbsterzeugte Zeitstempel in aller Regel wesentlich kostengünstiger erstellt werden können, als qualifizierte Zeitstempel. Insbesondere entfallen bei den selbsterzeugten Zeitstempeln die transaktionsabhängigen Gebühren pro Zeitstempel, mit denen ein Zertifizierungsdiensteanbieter die zusätzlichen Investitionen und Betriebsaufwände auf die einzelnen Transaktionen umlegt.

Deshalb ist es – unter wirtschaftlichen Gesichtspunkten, insbesondere bei einer großen Anzahl an benötigten Zeitstempeln – wünschenswert, qualifizierte Zeitstempel durch selbsterzeugte Zeitstempel zu ersetzen. Da der Beweiswert selbsterzeugter Zeitstempel aber unter Umständen sehr gering ist, könnte dies in Streitfällen zu signifikanten Problemen führen. Hat ein Zeitstempel, dessen Zweck per Definition der Beweis der Existenz bestimmter Daten zu einem bestimmten Zeitpunkt ist, keinen Beweiswert, so ist er als Zeitstempel selbstverständlich wertlos. Deshalb ist die Verwendung selbsterzeugter Zeitstempel statt qualifizierter Zeitstempel nur dann ratsam, wenn der Beweiswert der Zeitstempel unter dieser Substitution nicht, oder nicht wesentlich, leidet.

Die wesentliche Errungenschaft der hier vorgestellten Intervall-qualifizierten Zeitstempel ist, dass der Beweiswert dieser speziellen selbsterzeugten Zeitstempel beinahe dem Beweiswert qualifizierter Zeitstempel gleich kommt. Insbesondere kann von einem IQ-Zeitstempel bewiesen werden, dass er in einem Zeitintervall erzeugt wurde, das durch zwei qualifizierte Zeitstempel definiert wird.

3 Intervall-qualifizierte Zeitstempel

In diesem Abschnitt wird gezeigt, wie durch den geschickten Einsatz einer kryptographischen Hashfunktion und wenigen qualifizierten Zeitstempeln beliebig viele IQ-Zeitstempel erzeugt werden können.

¹ Bei der freiwilligen Akkreditierung eines Zeitstempeldienstes, oder von Produkten zum Betrieb eines solchen, sind weiterhin §15 Abs. 1 bzw. Abs. 7 SigG zu beachten.

² Stellt ein Zertifizierungsdiensteanbieter auch qualifizierte Zertifikate aus, so hat dieser zusätzlich insbesondere die §§5 – 8 und 14 SigG und die zugehörigen Regularien aus SigV zu beachten.

³ Für nähere Informationen zur Prüfungspflicht bei einer Herstellererklärung sei auf [HüKn03] Abschnitt 2.1.3 verwiesen.

Nach der Skizze der zugrundeliegenden Ideen in Abschnitt 3.1 werden die IQ-Zeitstempel in Abschnitt 3.2 präzise spezifiziert. In Abschnitt 3.3 wird die Sicherheit dieser Zeitstempel und der daraus resultierende Beweiswert untersucht. Betrachtungen zur Effizienz und Wirtschaftlichkeit dieser Zeitstempel finden sich in Abschnitt 3.4.

3.1 Zugrundeliegende Ideen

Ein Zeitstempeldienst TSS erzeugt einen Zeitstempel QS typischerweise, indem die Konkatination aus bestimmten Daten d und einem Zeitattribut t mit dem privaten Schlüssel sk_{TSS} signiert wird:

$$QS = Sig_{TSS} (d / t , sk_{TSS}) \quad (1)$$

Durch diesen Zeitstempel TS wird dokumentiert, dass die Daten d zum Zeitpunkt t beim Zeitstempeldienst TSS vorgelegen haben. Ist das verwendete Signaturverfahren sicher, so dass keine Signaturen gefälscht werden können und ist TSS hinreichend vertrauenswürdig, so dass stets die aktuelle Zeit t zur Produktion solcher Zeitstempel verwendet wird, dann beweist TS , dass d bereits vor dem Zeitpunkt t existiert hat.

Sei $h: \{0,1\}^* \rightarrow \{0,1\}^n$ eine kryptographische Hashfunktion, so dass es bei gegebenem $h(x)$ praktisch unmöglich ist, x zu ermitteln (Einwegeigenschaft) und es praktisch unmöglich ist ein Paar x_1, x_2 zu finden, so dass $h(x_1) = h(x_2)$ (Kollisionsresistenz).

Dann induzieren die Einwegeigenschaft und Kollisionsresistenz von h , wie beispielsweise in Section 3.1 [Lipm99] und [BLLV98] herausgestellt, eine relative zeitliche Ordnung zwischen dem Argument und dem Funktionswert von h . Existiert der Wert $h(x)$ zum Zeitpunkt t , so impliziert die Einwegeigenschaft und die Kollisionsresistenz von h , dass das Dokument x bereits vor dem Zeitpunkt t existiert haben muss.

Sei A ein mit einem Signaturschlüsselpaar (sk_A, pk_A) ausgestattetes Subjekt (z. B. ein organisationsinterner Zeitstempeldienst) und r beliebige Daten. Sei

$$QS_1 = Sig_{TSS} (r / T_1 , sk_{TSS}), \quad (2)$$

$$S = Sig_A (h (QS_1) / m / t , sk_A) \quad (3)$$

und

$$QS_2 = Sig_{TSS} (h (S) / T_2 , sk_{TSS}). \quad (4)$$

Unterstellt man, dass TSS vertrauenswürdig ist, dann wurde die Signatur in (2) zum Zeitpunkt T_1 und die Signatur in (4) zum Zeitpunkt T_2 erstellt.

Sei t der Zeitpunkt der Erstellung der Signatur in (3). Da bei der Signatur in (3) der Hashwert $h (QS_1)$ des Zeitstempels QS_1 verwendet wird, ist

$$t > T_1. \quad (5)$$

Auf der anderen Seite fließt der Hashwert $h (S)$ der Signatur S aus (3) in den Zeitstempel aus (4) ein. Deshalb ist

$$t < T_2. \quad (6)$$

Aus (5) und (6) folgt schließlich, dass A die Signatur S in (3) im offenen Zeitintervall $] T_1, T_2 [$ erzeugt haben muss. Diese Zusammenhänge sind in Abbildung 1 veranschaulicht.

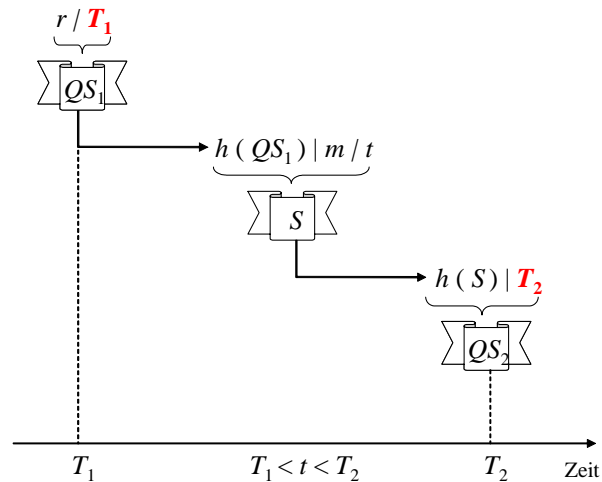


Abbildung 1: Relative zeitliche Ordnung mittels Hashfunktion

Sollen nun mehrere Signaturen S_i , $1 \leq i \leq n$, zwischen den beiden vertrauenswürdigen Zeitstempeln erzeugt werden, so wird der Zeitstempel QS_1 in jede Signatur S_i einbezogen und die verschiedenen Signaturen S_i wiederum in geeigneter Weise in den Zeitstempel QS_2 integriert. Hierfür bietet sich die Verwendung der Stapelsignatur-Strategie aus [PaBo99] an, die im Kern auf Merkle's Authentisierungsbaum [Merk80] basiert.

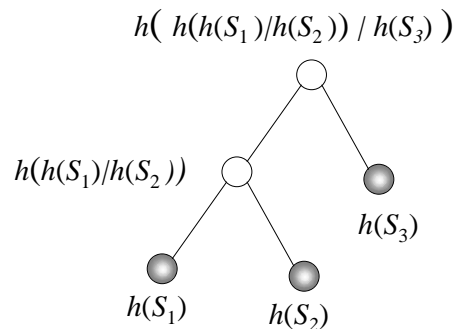


Abbildung 2: Binärer Hashbaum für Stapelsignatur mit drei Blättern

Hier werden die Signaturen S_i , wie in Abbildung 2 angedeutet, als Blätter eines binären⁴ Hashbaumes aufgefasst, wobei die Wurzel dieses Baumes schließlich im Rahmen der Erstellung von QS_2 signiert wird. Zur Verifikation der Stapelsignatur muss einfach der Pfad vom entsprechenden Blatt zur Wurzel durchlaufen und die Signatur der Wurzel überprüft werden. Um den Pfad zwischen Blatt und Wurzel durchlaufen zu können, werden die notwendigen Informationen für jedes Blatt in Form eines reduzierten Hashbaumes abgelegt. Dieser reduzierte Hashbaum besteht aus einer Folge von Wertepaaren, die aus dem benachbarten Hashwert und der relativen Position („L“ für links oder „R“ für rechts) desselben bestehen.

⁴ Grundsätzlich wäre es auch möglich, statt einem binären Baum einen nicht-binären Baum zu verwenden. Allerdings wurde in [PaBo99] Section 4.2 gezeigt, dass dies zu Lasten des für die Speicherung der Signatur benötigten Speicherplatzes gehen würde. Der geringste Speicherbedarf ist bei der Verwendung binärer Bäume zu erwarten.

Wie diese reduzierten Hashbäume gebildet werden, kann am besten anhand eines Beispiels veranschaulicht werden. Betrachtet man den Hashbaum in Abbildung 2, dann besteht der reduzierte Hashbaum für das Blatt $h(S_1)$ aus der Folge $\{ (h(S_2),R), (h(S_3),R) \}$. Für das Blatt $h(S_2)$ besteht der reduzierte Hashbaum aus der Folge $\{ (h(S_1),L), (h(S_3),R) \}$. Für das Blatt $h(S_3)$ besteht der reduzierte Hashbaum schließlich aus einem einzigen Knoten $\{ (h(h(S_1) | h(S_2)), L) \}$.

Durch die Kombination der beiden einfachen Ideen („Relative zeitliche Ordnung durch Hashfunktion“ und „Stapelsignatur mit binärem Hashbaum“) erhält man schließlich, wie in Abbildung 3 angedeutet, die Intervall-qualifizierten Zeitstempel. Analog zur obigen Konstruktion (vgl. Abbildung 1), ist auch hier leicht einzusehen, dass die Signaturen S_i nach T_1 und vor T_2 erstellt worden sind.

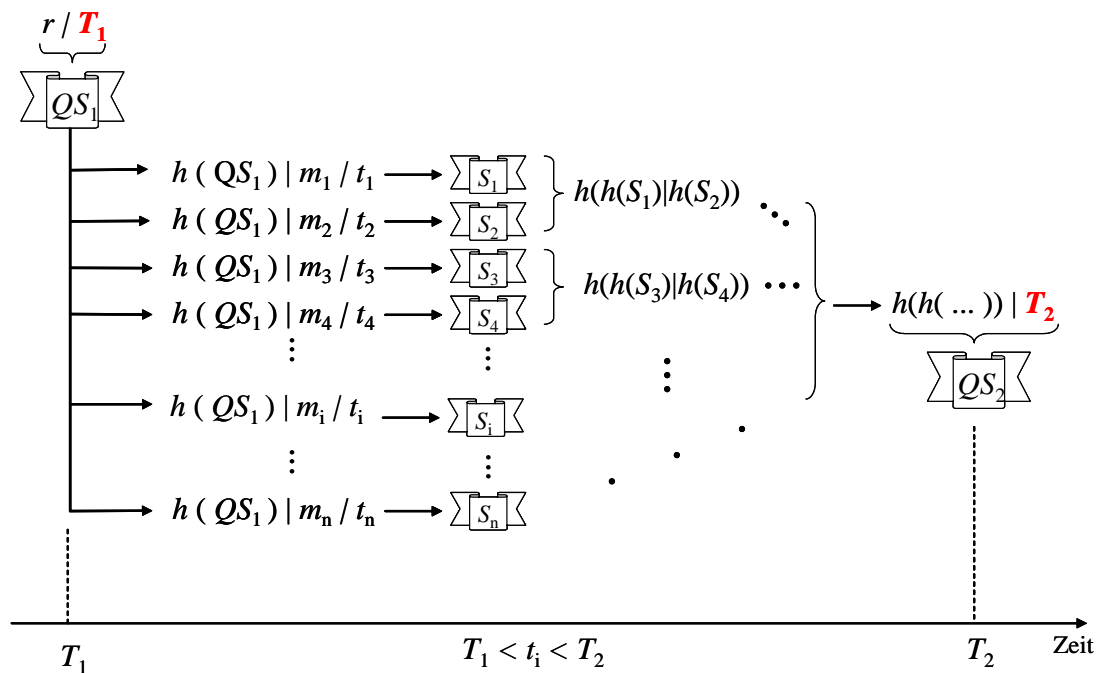


Abbildung 3: Konstruktion Intervall-qualifizierter Zeitstempel

3.2 Spezifikation der Syntax und Abläufe

In diesem Abschnitt sollen die oben skizzierten vagen Ideen weiter präzisiert werden, so dass schließlich die nötige ASN.1-Syntax und die Prozeduren zur Erzeugung und Verifikation der Intervall-qualifizierten Zeitstempel angegeben werden können.

Wir beschränken uns hier auf den Fall, dass die vertrauenswürdigen Zeitstempel QS_1 und QS_2 gemäß dem in [RFC3161] spezifizierten Time Stamping Protocol (TSP) erzeugt werden und die selbsterzeugten Zeitstempel S_i gewöhnliche Cryptographic-Message-Syntax (CMS) Signaturen [RFC3369] mit signiertem Attribut `SigningTime` sind.

Dann muss zum Einen ein erweiterter Zeitstempel definiert werden, mit dem die Stapelsignatur mit binärem Hashbaum realisiert werden kann und schließlich spezifiziert werden, wie die beiden vertrauenswürdigen Zeitstempel QS_1 und QS_2 mit den selbsterzeugten Zeitstempeln S_i verbunden werden.

Den erweiterten Zeitstempel definieren wir in Anlehnung an [BPT03]⁵ und [PaBo99] folgendermaßen:

```
EnhancedTimeStamp ::= SEQUENCE {
    tsEnhancement    TimeStampEnhancement OPTIONAL,
    timeStamp        TimeStampToken }
```

wobei

```
TimeStampEnhancement ::= SEQUENCE {
    digestAlgorithm  AlgorithmIdentifier
    reducedHashtree SEQUENCE OF Node }
```

und

```
Node ::= SEQUENCE {
    direction      BIT STRING {L (0), R (1)},
    hashvalue      OCTET STRING }
```

Hierbei haben die Bezeichner folgende Bedeutung:

- Der erweiterte Zeitstempel (`EnhancedTimeStamp`) besteht aus einer optionalen Erweiterung (`tsEnhancement`) und einem gewöhnlichen, in [RFC3161] spezifizierten, Zeitstempel-Token (`timeStamp`) (siehe Anhang).
- Die optionale Erweiterung vom Typ `TimeStampEnhancement` besteht ihrerseits aus
 - dem Bezeichner `digestAlgorithm`, der spezifiziert welche Hashfunktion zur Konstruktion des Hashbaumes verwendet wurde und
 - dem `reducedHashtree`, der wiederum aus einer Folge von Knoten besteht, die den Pfad zwischen einem Blatt und der Wurzel des Hashbaumes eindeutig festlegen. Jeder Knoten (`Node`) besteht aus den beiden Bezeichnern `direction` und `hashvalue`, die die Richtung für den nächsten Schritt auf dem Weg zur Wurzel und den Hashwert des Geschwisterknotens angeben, der zur Berechnung des nächsten Schrittes auf dem Weg zur Wurzel benötigt wird. Beispiele zur Reduktion des Hashbaumes in Abbildung 2 finden sich in Abschnitt 3.1.

Wie in Abbildung 4 angedeutet, geschieht die Erzeugung eines in Abbildung 3 dargestellten Intervall-qualifizierten Zeitstempels in folgenden drei Schritten:

1. Der IQ-Zeitstempel-Dienst erhält von einem ZDA einen qualifizierten Zeitstempel QS_1 .
2. Dieser qualifizierte Zeitstempel QS_1 fließt als signiertes Attribut (`PrevStamp`) in die Zeitstempel S_i ein, die der IQ-Zeitstempel-Dienst für die Clients ausstellt.
3. Die Zeitstempel S_i , $1 \leq i \leq n$, fließen in einen erweiterten Zeitstempel QS_2 ein, der – mit dem individuellen, zur speziellen Signatur S_i gehörigen, `reducedHashtree` – als unsigniertes Attribut (`NextStamp`) in S_i integriert wird. Dies geschieht in folgenden Teilschritten:
 - 3.1. Aus den S_i , $1 \leq i \leq n$, wird – wie in Abbildung 2 angedeutet – ein Binärbaum konstruiert.
 - 3.2. Für die Wurzel des Binärbaumes wird mittels TSP ein Zeitstempel angefordert.

⁵ In [BPT03] wird die völlig generische Syntax `reducedHashtree ::= SEQUENCE OF {SEQUENCE OF OCTET STRING} OPTIONAL` vorgeschlagen, mit der auch beliebige (nicht-binäre) Bäume unterstützt werden könnten. Allerdings sind die notwendigen Prozeduren für die Behandlung beliebiger Bäume wesentlich komplexer und deshalb für den praktischen Einsatz weniger geeignet. Deshalb wird hier vorgeschlagen, sich wie in [PaBo99] auf binäre Hashbäume zu beschränken.

- 3.3. Für jedes S_i , $1 \leq i \leq n$, wird der Binärbaum auf die relevanten Informationen reduziert. Das geschieht, indem der Baum vom Blatt S_i zur Wurzel durchlaufen wird und in jedem Schritt der Hashwert des jeweiligen Geschwisterknotens mit der zugehörigen Richtung gespeichert wird.
- 3.4. Wurde der individuelle `reducedHashtree` auf diese Art und Weise erzeugt, so kann er – zusammen mit dem für alle Blätter gültigen Zeitstempel der Wurzel – als `EnhancedTimeStamp` als unsigniertes Attribut in den selbsterzeugten Zeitstempel S_i integriert werden.

Die beiden Zeitstempelattribute

- `PrevStamp` für QS_1 , das als signiertes Attribut in S_1 eingefügt wird, und
- `NextStamp` für QS_2 , das als unsigniertes Attribut in S_i eingefügt wird, sollten jeweils als `EnhancedTimeStamp` definiert sein.

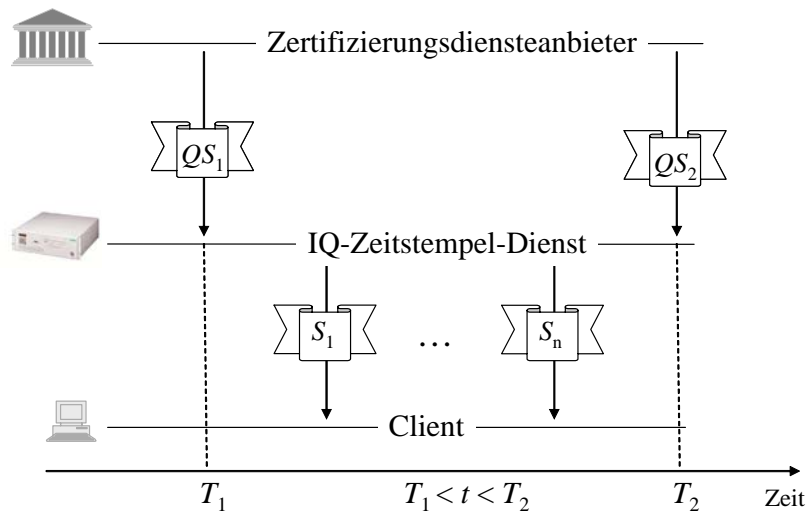


Abbildung 4: System zur Erstellung Intervall-qualifizierter Zeitstempel

Um einen Intervall-qualifizierten Zeitstempel zu überprüfen, existieren zwei verschiedene Möglichkeiten:

- *Einfache Prüfung*
Bei der einfachen Prüfung, die bei der internen Verarbeitung zumeist ausreichend ist, wird lediglich die Signatur S_i über dem `SigningTime`-Attribut verifiziert.
- *Umfassende Prüfung*
Bei der umfassenden Prüfung, die wegen des erhöhten Beweiswertes beispielsweise bei Streitfällen vor Gericht bemüht werden wird, geht man folgendermaßen vor:
 1. Auslesen des signierten Zeitstempel-Attributes `PrevStamp` aus S_i .
 2. Überprüfen der Gültigkeit der Signatur an `PrevStamp`.
 3. Überprüfung der Gültigkeit der Signatur an S_i .
 4. Auslesen des unsignierten Zeitstempel-Attributes `NextStamp` aus S_i .
 5. Überprüfen der Gültigkeit der Signatur am erweiterten Zeitstempel `NextStamp`. Das geschieht in folgenden Teilschritten:

- 5.1. Durchwandern des reduzierten Hash-Baumes vom Blatt (S_i) zur Wurzel. Das geschieht, indem $j:=0$ und $H_0:=h(S_i)$ gesetzt wird und für die komplette Folge der Knoten (Node) in `reducedHashtree` folgende Schritte ausgeführt werden:

$j:=j+1$

IF (Node.direction = „L“)

THEN $H_j:=h(\text{Node.hashvalue} | H_{j-1})$

ELSE $H_j:=h(H_{j-1} | \text{Node.hashvalue})$

- 5.2. Überprüfen, ob der `MessageImprint` im Zeitstempel mit H_j übereinstimmt.

- 5.3. Überprüfen, ob die Signatur am Zeitstempel für H_j gültig ist.

6. Überprüfen, ob $T_1 < t_i < T_2$.

Der Intervall-qualifizierte Zeitstempel ist genau dann gültig, wenn alle Prüfungen (in 2., 3., 5. und 6.) erfolgreich waren.

3.3 Sicherheit und Beweiswert

In diesem Abschnitt sollen Sicherheitsaspekte der hier vorgeschlagenen Intervall-qualifizierten Zeitstempel und damit eng verknüpfte Aspekte des Beweiswertes vor Gericht betrachtet werden.

Hierzu gehen wir in drei Schritten vor: In Abschnitt 3.3.1 finden sich generelle Betrachtungen zum Beweiswert von Zeitstempeln. Abschnitt 3.3.2 betrachtet den Beweiswert qualifizierter Zeitstempel. In Abschnitt 3.3.3 wird schließlich die Sicherheit und der Beweiswert der hier vorgeschlagenen Intervall-qualifizierten Zeitstempel näher untersucht.

3.3.1 Generelles zum Beweiswert von Zeitstempeln

Gemäß der Definition in Abschnitt 2.1 muss bei der Betrachtung des Beweiswertes eines Zeitstempels hinterfragt werden, wie schwierig es sein würde einen Beweis durch Augenschein gemäß §371 ff ZPO, der sich auf den Zeitstempel stützt, zu erschüttern oder gar zu widerlegen.

In der Praxis (siehe Anhang) erfolgt das Ausstellen von (qualifizierten oder selbsterzeugten) Zeitstempeln zumeist durch die elektronische Signatur (des Hashwertes) der Nutzdaten und einer Zeitangabe. Deshalb ist also insbesondere zu untersuchen, ob

1. die Signatur gefälscht sein könnte und ob
2. die durch die Signatur eingeschlossene Zeitangabe mit der zum Zeitpunkt der Signaturerstellung aktuellen Zeit übereinstimmt.

Bei der ersten Frage muss nach der Art der verwendeten Signatur unterschieden werden.

Wird eine qualifizierte elektronische Signatur verwendet, so kann gemäß §292a ZPO der Anschein der Echtheit der Signatur nur durch Tatsachen erschüttert werden, die ernstliche Zweifel daran begründen. Wird eine qualifizierte elektronische Signatur mit Anbieterakkreditierung verwendet, so dürfte es noch schwieriger sein, den Anschein der Echtheit zu erschüttern – in der Begründung [SigGBeg] zu §15 Abs. 1 Satz 4 SigG ist gar von einer „Art ‚Sicherheitsvermutung‘“ die Rede.

Werden lediglich fortgeschrittene oder gar einfach elektronische Signaturen zur Erstellung der Zeitstempel eingesetzt, so kann es unter Umständen sehr einfach sein, einen Anscheins-

beweis, der sich auf einen solchen Zeitstempel stützt, zu erschüttern – der Beweiswert dieser Zeitstempel wäre also eher gering.

Während die Möglichkeit der Signaturfälschung durch den Einsatz qualifizierter elektronischer Signaturen (mit Anbieterakkreditierung) praktisch ausgeschlossen werden kann, so ist es ungleich schwieriger zu beweisen, dass die im Zeitstempel angegebene Zeit mit der bei der Erstellung des Zeitstempels aktuellen Zeit übereinstimmt.

Hier wird man sich (bei einer vorab, oder auf Grund eines Streitfalles, durchgeführten Prüfung) mit dem Nachweis begnügen müssen, dass beim Zeitstempeldienst mehr oder weniger wirkungsvolle (technische, organisatorische und personelle) Sicherheitsmechanismen implementiert sind, die dafür Sorge tragen, dass stets die gesetzlich gültige Zeit zur Zeitstempelung verwendet wird.

Geht man davon aus, dass zur Erstellung von (selbsterzeugten oder qualifizierten) Zeitstempeln immer qualifizierte elektronische Signaturen mit Anbieterakkreditierung eingesetzt werden, dann hängt der Beweiswert des Zeitstempels insbesondere von der Authentizität der bei der Erzeugung verwendeten Zeitquelle und der Integrität des Gesamtsystems ab.

3.3.2 Beweiswert qualifizierter Zeitstempel

Ein „qualifizierter Zeitstempel“ ist gemäß §2 Nr. 14 SigG eine elektronische Bescheinigung eines Zertifizierungsdiensteanbieters (ZDA), dass ihm bestimmte elektronische Daten zu einem bestimmten Zeitpunkt vorgelegen haben.

Der Unterschied zwischen selbsterzeugten und qualifizierten Zeitstempeln besteht darin, dass ein ZDA, der qualifizierte Zeitstempel erstellt, die in Abschnitt 2.2 aufgelisteten Mindestanforderungen erfüllen muss. Im Hinblick auf den Beweiswert sind insbesondere die im Sicherheitskonzept, und darin referenzierten Produktdokumentationen und Prüfberichten, aufgeführten Sicherheitsmaßnahmen von Bedeutung mit denen die Integrität und Authentizität der Zeitquelle und des Gesamtsystems gewährleistet wird. Durch die Anbieterakkreditierung gemäß §15 SigG wird zudem der „Nachweis der umfassend geprüften technischen und administrativen Sicherheit“ erbracht. Deshalb dürfte es, insbesondere bei einem ZDA mit Anbieterakkreditierung, äußerst schwierig sein, den Augenscheinsbeweis zur Echtheit eines qualifizierten Zeitstempels zu widerlegen. Der qualifizierte Zeitstempel eines akkreditierten Anbieters dürfte im Streitfall also einen sehr hohen Beweiswert haben.

3.3.3 Sicherheitsaspekte und Beweiswert Intervall-qualifizierter Zeitstempel

Wie in den Abschnitten 3.1 und 3.2 näher erläutert, besteht ein Intervall-qualifizierter Zeitstempel im Wesentlichen aus drei Zeitstempeln (QS_1 , S_i und QS_2), die durch eine kryptographische Hashfunktion h , so in Beziehung gesetzt sind, dass S_i (auf Grund der Einwegigkeit und Kollisionsresistenz von h) erst nach der Erstellung von QS_1 , und QS_2 erst nach der Erstellung von S_i , erzeugt werden kann.

Sofern eine geeignete Hashfunktion h zur oben erläuterten Konstruktion der Intervall-qualifizierten Zeitstempel verwendet wurde, kann somit bewiesen⁶ werden, dass der Zeitpunkt der Erstellung der Signatur S_i zwischen der Erstellung von QS_1 und QS_2 liegen musste.

⁶ Für einen formalen Beweis hierfür verweisen wir auf Theorem 1 in [Hühn04].

Hashfunktionen, die nach dem jeweils aktuellen Stand der Wissenschaft und Technik, die Einwegigkeit und Kollisionsresistenz aufweisen, werden von der RegTP regelmäßig im Bundesanzeiger veröffentlicht. In der aktuellen Bekanntmachung [RegTPAlg] wird davon ausgegangen, dass RIPEMD-160 und SHA-1 mindestens bis zum Jahr 2008 eingesetzt werden können.

Bei Produkten, die die hier vorgestellten Intervall-qualifizierten Zeitstempel realisieren, muss außerdem noch, vorab (im Rahmen einer Prüfung und Bestätigung gemäß §15 Abs. 7 SigG) oder im Streitfall vor Gericht, nachgewiesen werden, dass die in Abschnitt 3.2 angegebenen Mechanismen tatsächlich implementiert sind und die eingesetzten Komponenten zum fraglichen Zeitpunkt in einem einwandfreien Zustand waren. Sind diese Voraussetzungen gegeben, so ist bewiesen, dass S_i zwischen QS_1 und QS_2 erstellt wurde.

Bezüglich der Intervallzugehörigkeit $T_1 < t_i < T_2$ bleibt also der hohe Beweiswert der qualifizierten Zeitstempel erhalten, wohingegen der genaue Zeitpunkt t_i der Erstellung von S_i nur mit dem geringeren Beweiswert des selbsterzeugten Zeitstempels dokumentiert ist.

Wird beispielsweise täglich ein qualifizierter Zeitstempel angefordert, so ist zwar das Datum der Intervall-qualifizierten Zeitstempel nachweislich authentisch, aber möglicherweise nicht die Uhrzeit.

3.4 Effizienz und Wirtschaftlichkeit

In diesem Abschnitt wird kurz auf praktische und ökonomische Aspekte der IQ-Zeitstempel eingegangen.

Wie sich direkt aus dem in Abbildung 3 skizzierten Aufbau der IQ-Zeitstempel erkennen lässt, wird zusätzlicher Speicherplatz für die beiden Zeitstempel QS_1 und QS_2 benötigt. Für die Speicherung eines einfachen, in [RFC3161] definierten Zeitstempels werden etwa⁷ 300 Byte benötigt. Der Speicherbedarf für den reduzierten Hashbaum hängt von der Tiefe des Baumes ab, die wiederum logarithmisch von der Anzahl n der zwischen T_1 und T_2 selbst erzeugten Zeitstempel abhängt. Bei einer Million selbsterzeugter Zeitstempel S_i müssen beispielsweise höchstens 20 ($= \lceil \log_2(10^6) \rceil$) Knoten á 21 Byte gespeichert werden – der zusätzliche Speicherbedarf pro Zeitstempel läge in diesem Fall also bei rund 1 kByte.

Für die Abschätzung des wirtschaftlichen Effektes des Einsatzes der IQ-Zeitstempel unterstellen wir, dass

- die Stückkosten für den Bezug der qualifizierten Zeitstempel abhängig von der Anzahl x der jährlich bezogenen Zeitstempel sind und sich aus der Funktion $k=1 / \log_{10}(x)$ errechnen,
- für die Bereitstellung eines Systems zur Erzeugung der IQ-Zeitstempel eine Investition in Höhe von 20.000 € nötig wird,
- pro Arbeitstag ein qualifizierter Zeitstempel angefordert wird, wobei ein Jahr 250 Arbeitstage hat.

Mit diesen Annahmen erhalten wir die folgenden Ergebnisse:

⁷ 100 Byte für TSTInfo und rund 200 Byte für eine 1024 Bit RSA CMS-Signatur (ohne Zertifikate und CRLs etc.) scheint eine hinreichend präzise Näherung darzustellen.

Anzahl x der Zeitstempel pro Jahr	Stückkosten in Euro $k=1 / \log_{10}(x)$	Kosten pro Jahr qual. Zeitstempel in Euro ($k*x$)	Anzahl der Zeitstempel pro Tag ($x / 250$)	Break-Even nach y Monaten
10	1,00 €	10,00 €	0,04	
100	0,50 €	50,00 €	0,40	
1.000	0,33 €	333,33 €	4	1.152,00
10.000	0,25 €	2.500,00 €	40	101,05
100.000	0,20 €	20.000,00 €	400	12,08
1.000.000	0,17 €	166.666,67 €	4.000	1,44
10.000.000	0,14 €	1.428.571,43 €	40.000	0,17
100.000.000	0,13 €	12.500.000,00 €	400.000	0,02

Tabelle 1: Wirtschaftlichkeit der Intervall-qualifizierten Zeitstempel

Wie in Tabelle 1 zu erkennen ist, amortisiert sich die Investition in ein System zur Erstellung Intervall-qualifizierter Zeitstempel unter den o.g. Voraussetzungen bereits nach etwa einem Jahr, sofern mindestens 400 Zeitstempel pro Tag benötigt werden.

4 Fazit

In dieser Arbeit wurde ein einfaches Verfahren vorgestellt, mit dem – unter Verwendung einer kryptographischen Hashfunktion und dem täglichen Bezug eines einzigen qualifizierten Zeitstempels – das Erstellungsdatum selbsterzeugter Zeitstempel mit dem hohen Beweiswert qualifizierter Zeitstempel versehen werden kann.

Da der zusätzliche Rechenaufwand aus wenigen Aufrufen einer Hashfunktion besteht und der zusätzlich benötigte Speicherplatz typischerweise weniger als 1 kByte beträgt, ist die Bereitstellung der IQ-Zeitstempel sehr effizient möglich.

Unter plausiblen Annahmen lässt sich zeigen, dass der Einsatz der IQ-Zeitstempel bereits bei einigen hundert Zeitstempeln pro Tag wirtschaftlicher ist, als der alleinige Bezug qualifizierter Zeitstempel.

Literatur

- [BrPo02] Brandner, R.; Pordesch, U.: *Long-term conservation of provability of electronically signed documents*, Beitrag zu ISSE, 2002
- [BPT03] Brandner, R.; Pordesch, U.; Tielemann, M.: *Archive Time-Stamps Syntax (ATS)*, Internet-Draft, Juni 2003
- [BrTe01] Bröhl, G.; Tettenborn, A.: *Das neue Recht der elektronischen Signaturen: kommentierende Darstellung von Signaturgesetz und Signaturverordnung*, Bundesanzeiger-Verlag, ISBN 3-89817-045-4, 2001
- [BLLV98] Buldas, A.; Laud, P., Lipmaa, H., Vilemson, J.: *Time-stamping with Binary Linking Schemes*, in *Advances in Cryptology - CRYPTO '98*, LNCS 1462, Springer-Verlag, 1998, SS. 486–501
- [ETSI-TSP] ETSI: *TS 101 861 – Time stamping profile*, v1.2.1, 2002, via http://docbox.etsi.org/EC_Files/EC_Files/ts_101861v010201p.pdf

- [ISIS-MTT] TeleTrusT e.V.: *ISIS-MTT-Spezifikation*, Version 1.0.2, Juli 2002, via <http://www.isis-mtt.de/>
- [HüKn03] Hühnlein, D.; Knosowski, Y.: *Aspekte der Massensignatur*, Tagungsband D·A·C·H Security 2003, IT-Verlag, 2003, ISBN 3-00-010941-2, SS. 293-307
- [Hühn04] Hühnlein, D.: *How to qualify electronic signatures and time stamps*, erscheint bei 1st European PKI Workshop, Juni 2004 und Springer Verlag
- [ISO-18014] ISO/IEC 18014-1: *Information technology - Security techniques - Time stamping services - Part 1: Framework, 2002*
- [Lipm99] Lipmaa, H.: *Secure and efficient time stamping systems*, Dissertation an der Universität Tartu, Estland, 1999, via <http://www.tcs.hut.fi/~helger/papers/thesis/thesis.pdf>
- [Merk80] Merkle, R.: *Protocols for Public Key Cryptosystems*, Proceedings of the 1980 IEEE Symposium on Security and Privacy (Oakland, CA, USA, April 1980), SS. 122-134.
- [PaBo99] Pavlovski C.; Boyd C.: *Efficient Batch Signature Generation using Tree Structures*, International Workshop on Cryptographic Techniques and E-Commerce, CrypTEC'99, City University of Hong Kong Press, SS. 70-77, via <http://sky.fit.qut.edu.au/~boydc/papers/treefinal.ps>
- [PKCS#7] RSA Labs: *PKCS #7 - Cryptographic Message Syntax Standard*, via <http://www.rsalabs.com/pkcs/pkcs-7/index.html>
- [PKCS#9] RSA Labs: *PKCS #9 - Selected Attribute Types*, via <http://www.rsalabs.com/pkcs/pkcs-9/index.html>
- [RegTPAlg] RegTP: *Geeignete Algorithmen zur Erfüllung der Anforderungen nach §17 Abs. 1 bis 3 SigG*, Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung, Bundesanzeiger Nr. 48 – S. 4202-4203 vom 11.03.2003, via http://www.regtp.de/imperia/md/content/tech_reg_t/digisign/143.pdf
- [RFC1421] Linn, J.: *Privacy Enhancement for Internet Electronic Mail: Part I: Message Encryption and Authentication Procedures*, RFC 1421, 1993, via <http://www.ietf.org>
- [RFC2315] Kaliski, B.: *PKCS #7: Cryptographic Message Syntax*, Version 1.5, RFC 2315, 1998, via <http://www.ietf.org>
- [RFC2630] Housley, R.: *Cryptographic Message Syntax (CMS)*, RFC 2630, via <http://www.ietf.org>
- [RFC3161] Adams, C.; Cain, P.; Pinkas, D.: *Internet X.509 Public Key Infrastructure – Time Stamp Protocol (TSP)*, RFC 3161, via <http://www.ietf.org>
- [RFC3369] Housley, R.: *Cryptographic Message Syntax (CMS)*, RFC 3369, via <http://www.ietf.org>
- [SigG] *Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften*, vom 16.05.2001, BGBl. 2001 Teil I Nr. 22, S. 876 ff, via <http://www.iid.de/iukdg/gesetz/SigAendG2.pdf>

[SigGBeg] *Begründung zu [SigG]*, via <http://www.iid.de/iukdg/gesetz/310102siggbegr.pdf>

[SigV] *Verordnung zur elektronischen Signatur*, vom 16.11.2001 BGBl. 2001 Teil I Nr. 59, S. 3074 ff), via <http://www.iid.de/iukdg/gesetz/SigV161101.pdf>

Anhang – Zeitstempel-Syntax in CMS und TSP

In diesem Anhang werden einige relevante Aspekte der Zeitstempel-Syntax aus CMS [RFC3369] und TSP [RFC3161] in kompakter Art und Weise zusammengetragen.

Cryptographic Message Syntax (CMS)

Das heute vielleicht am weitesten verbreitete Basisformat für kryptographisch behandelte Nachrichten ist in [RFC3369] definiert. Dieser Standard basiert⁸, wie bereits seine Vorgängerversion [RFC2630], auf [PKCS#7] bzw. [RFC2315]. PKCS#7 ist wiederum – unter gewissen Umständen⁹ – sogar mit den heute schon fast antik anmutenden PEM-Format [RFC1421] kompatibel.

In CMS werden im `ContentInfo` verschiedene Inhaltstypen unterstützt. Unter den in [RFC3369] spezifizierten Nachrichtentypen ist der Signaturtyp (`contentType` ist `id-signedData` und `content` ist `SignedData`) für Zeitstempel relevant.

```
SignedData ::= SEQUENCE {
    version          CMSVersion,
    digestAlgorithms DigestAlgorithmIdentifiers,
    encapContentInfo EncapsulatedContentInfo
    certificates     [0] IMPLICIT CertificateSet           OPTIONAL,
    crls             [1] IMPLICIT CertificateRevocationLists OPTIONAL,
    signerInfos     SignerInfos }
```

Die `EncapsulatedContentInfo` in CMS ([RFC3369] und [RFC2630]) ist definiert als

```
EncapsulatedContentInfo ::= SEQUENCE {
    econtentType    ContentType,
    eContent        [0] EXPLICIT OCTET STRING OPTIONAL }.
```

Sollen, beispielsweise zum Zweck der Erstellung von Zeitstempeln gemäß [RFC3161], strukturierte Daten signiert werden, so wird ein anderer `econtentType` mit dem strukturierten `eContent` spezifiziert.

Ein weiteres interessantes Feld ist `SignerInfos ::= SET OF SignerInfo`, das die elektronische(n) Signatur(en) enthält. Hierbei ist

```
SignerInfo ::= SEQUENCE {
    version          CMSVersion,
    sid             SignerIdentifier,
    digestAlgorithm  DigestAlgorithmIdentifier,
```

⁸ Inkompatibilitäten zwischen CMS und PKCS#7 ergeben sich lediglich, falls es sich bei den Nutzdaten nicht um den Typ `Data ::= OCTET STRING`, sondern um strukturierte Daten, wie z.B. ein `TSTInfo` Zeitstempel-Token aus [RFC3161], handelt (vgl. [RFC3369] Abschnitt 5.2.1.).

⁹ Siehe [PKCS#7] Abschnitt 9.5.

```

signedAttrs          [0] IMPLICIT SignedAttributes    OPTIONAL,
signatureAlgorithm  SignatureAlgorithmIdentifier,
signature            SignatureValue
unsignedAttrs       [1] IMPLICIT UnsignedAttributes    OPTIONAL }

```

mit

```
SignedAttributes ::= SET SIZE (1..MAX) OF Attribute
```

```
UnsignedAttributes ::= SET SIZE (1..MAX) OF Attribute
```

```
Attribute ::= SEQUENCE {
    attrType OBJECT IDENTIFIER,
    attrValues SET OF AttributeValue }

```

und

```
AttributeValue ::= ANY.
```

In [RFC3369] Abschnitt 11.3 wird ein bereits in [PKCS#9] eingeführtes zu signierendes Attribut `SigningTime` angegeben:

```
SigningTime ::= Time
```

```
Time ::= CHOICE {
    utcTime           UTCTime,
    generalizedTime  GeneralizedTime }

```

Die Verwendung dieses Attributes macht also aus einer gewöhnlichen CMS-Signatur einen Zeitstempel.

Time-Stamp Protocol (TSP)

Das vielleicht in der Praxis gebräuchlichste Protokoll für die Ausstellung von Zeitstempeln ist in [RFC3161] spezifiziert. Beispielsweise verweisen die beiden Standards [ISIS-MTT] und [ETSI-TSP] auf diesen Standard.

Im Rahmen dieses Standards wurde das Zeitstempel-Format `TimeStampToken` als ein in [RFC2630] spezifiziertes `ContentInfo` definiert, bei dem der `contentType` gleich `id-signedData` und der `content` ein `SignedData` ist. Außerdem ist der `eContentType` als `id-ct-TSTInfo` und `eContent` als `TSTInfo` definiert. Diese tatsächlichen Zeitstempel-Nutzdaten sind nun folgendermaßen definiert:

```

TSTInfo ::= SEQUENCE {
    version          INTEGER { v1(1) }.
    Policy           TSAPolicyId,
    messageImprint  MessageImprint,
    serialNumber    INTEGER
    genTime         GeneralizedTime,
    accuracy        Accuracy          OPTIONAL
    ordering        BOOLEAN           DEFAULT FALSE
    nonce           INTEGER           OPTIONAL
    tsa             [0] GeneralName   OPTIONAL
    extensions      [1] IMPLICIT Extensions OPTIONAL }

```