**Nr. 4,** April 2009

ISSN 1862-4375

# IT·Grundschutz

Informationsdienst

*Workshops*

## Trau, schau, wem

*Seite 13*

Quelle: Stock.xchng

*NEWS*

**BSI veröffentlicht Quartalslagebericht zur IT-Sicherheit**

**PGP-Nutzer geben vertrauliche Daten im Internet preis**

**Richtlinien zum Management privilegierter Passworte nutzen**

*Seite 2*





SecuMedia
Der Verlag für Sicherheits-Informationen

# Elektronische Zeitstempel

## *Gesetzlich verankerte Absicherung für elektronische Geschäftsprozesse aller Art, Teil I*

*Judith Balfanz, Vice President Marketing, AuthentiDate International AG*

**Im Juli 1997 definierten das erste Deutsche Signaturgesetz und die Signaturverordnung die Rahmenbedingungen für elektronische Signaturen und Zeitstempel. 1999 wurden die Rahmenbedingungen überarbeitet und resultierten in der Neufassung des Deutschen Signaturgesetzes vom Mai 2001. Im ersten Teil des Artikels werden Zeitstempel und Aufgaben definiert.**

Für Unternehmen, Behörden und Organisationen wurde mit dem Signaturgesetz die Grundlage für eine rechtssichere, elektronische Kommunikation geschaffen. Um die vielfältigen Einsatzmöglichkeiten insbesondere von Zeitstempeln beurteilen zu können, ist es hilfreich sich mit einigen Grundlagen, sowie den technischen und rechtlichen Rahmenbedingungen auseinanderzusetzen.

Ein Zeitstempel ist eine elektronische Bescheinigung, welche aussagt, wann bestimmte Daten vorlagen. Er dokumentiert somit das „Wann" und „Was". Eine elektronische Signatur, häufig auch als personenbezogene Signatur bezeichnet, dokumentiert das „Wer" und „Was".

Eine besondere Stellung nehmen so genannte qualifizierte Zeitstempel von akkreditierten Anbietern ein. Diese Zeitstempel unterliegen bei ihrer Erstellung besonderen gesetzlichen Anforderungen. Sie können so für elektronische Daten einen zuverlässigen, langfristigen Schutz über mindestens 30 Jahre gesetzlich garantieren. Diese Zeitstempel sind somit ein ideales Werkzeug, um unter anderem die Einhaltung von Compliance Anforderungen für Unternehmensprozesse rechtssicher zu dokumentieren.

Da qualifizierte Zeitstempel von einem unabhängigen Dritten, dem Zertifizierungsdiensteanbieter (ZDA), erstellt werden, können sie im Vergleich zu personenbezogenen Signaturen wesentlich einfacher zur Absicherung von Prozessen verwendet werden.

So sind beispielsweise keine spezielle gesetzeskonforme Hard- oder Software beim Anwender selbst und keine manuelle Interaktion des Anwenders, wie PIN-Eingaben, erforderlich. Der qualifizierte Zeitstempel wird einfach von einem behördlich akkreditierten Anbieter, dem ZDA bezogen. Er steht somit an jedem Ort, zu jeder Zeit und in (nahezu) jeder Menge zur Verfügung.

### Technische Rahmenbedingungen und Rechtswirksamkeit

Die technischen Rahmenbedingungen zur Erstellung einer qualifizierten personenbezogenen Signatur sind im Allgemeinen bekannt. Benötigt wird ein bestätigter Kartenleser (Smart Card Terminal) eine sichere Signaturkarte (z.B. T-TeleSec TCOS V3, D-Trust, etc.) und geeignete Signaturanwendungskomponenten (Signatursoftware). Alle drei Komponenten müssen den Anforderungen des Signaturgesetzes entsprechen. Ist nur eine der Anforderungen nicht erfüllt, kann keine qualifizierte Signatur erstellt werden.

Die vorgenannten Anforderungen an sichere Komponenten etc. gelten auch für elektronische Zeitstempel. Hervorzuheben ist jedoch, dass zur Erstellung qualifizierter Zeitstempel zwingend eine besonders gesicherte Einsatzumgebung erforderlich ist. Vielfach wird diese als (akkreditiertes) Trust Center gemäß Signaturgesetz bezeichnet. Diese Einsatzumgebung muss durch ein Sicherheitskonzept, Zugangsschutz und kontinuierliche Überwachung geschützt sein. Daher können qualifizierte Zeitstempel nur von, durch die Bundesnetzagentur, akkreditieren (bzw. angezeigten) ZDA ausgestellt werden, die ein solches Trust Center betreiben.

Im Unterschied zu den personenbezogenen Signaturen wird im Signaturgesetz nicht zwischen qualifizierten und fortgeschrittenen Zeitstempeln unterschieden. Das bedeutet, es existieren aus gesetzlicher Sicht nur „qualifizierte Zeitstempel" und „sonstige Zeitstempel". Weitere Differenzierungen und Abstufungen in der rechtlichen Relevanz existieren für elektronische Zeitstempel nicht.

Sobald nur eine der gesetzlichen Anforderungen, also beispielsweise die Einsatzumgebung, nicht erfüllt wird, ist der Zeitstempel immer „nicht qualifiziert". In diesem Fall ist auch keine Beweiskraft gemäß Signaturgesetz mit dem Zeitstempel und den zeitgestempelten Daten verbunden.

Akkreditierte ZDA unterliegen strengen Anforderungen, deren Erfüllung zu jedem Zeitpunkt des Betriebs von der Bundesnetzagentur überwacht wird. Bei Verstoß, also der Nicht-Erfüllung der Anforderungen, kann der Betrieb sofort von der Bundesnetzagentur untersagt werden.

## Hohe Anforderungen

Die hohen Anforderungen an den akkreditierten ZDA stellen auf der einen Seite für den Anbieter einen hohen Aufwand zum Betrieb des Dienstes dar, gewährleisten aber auf der anderen Seite für die Anwender und Kunden, die deren Dienste nutzen, das höchste in Deutschland und Europa verfügbare Level an Sicherheit.

Um zu verdeutlichen, in welchen Bereichen sich diese hohen Anforderungen an den ZDA vorteilig auf die Anwender bzw. Kunden auswirken, sind exemplarisch im Folgenden einige Aspekte dargestellt, welche gemäß § 4 SigG vom ZDA umzusetzen sind.

- Nachweis der Zuverlässigkeit und Fachkunde: Die Fachkunde wird insbesondere durch die Fachkunde des Personals nachgewiesen (z.B. polizeiliche Führungszeugnisse, Nachweis über deren Kenntnisse, Fähigkeiten, Erfahrungen und Zuverlässigkeit)
- Erfüllung der Sicherheitsanforderungen durch ein Sicherheitskonzept, welches über die gesamte Tätigkeitsdauer praktisch umgesetzt ist.
- Deckungsvorsorge: Ein akkreditierter Zertifizierungsdiensteanbieter hat zwingend eine Versicherung abzuschließen, welche die Nutzer seines Dienstes vor nicht absehbaren Fehlern und deren finanziellen Folgen schützt.
- Umfassende Prüfung der technischen und administrativen Sicherheit (gemäß § 15 Abs. 1 SigG)
- Prüfung und Bestätigung des Sicherheitskonzeptes und dessen Wiederholung in regelmäßigen Zeitabständen, (gemäß § 15 Abs.2 SigG)

| Einsatzbereich / Eigenschaft | Akkreditierter Zertifizierungs-diensteanbieter, Zeitstempeldienst (ZDA) gemäß SigG | Angezeigter Zertifizierungs-diensteanbieter, Zeitstempeldienst (ZDA) gemäß SigG | SigG-bestätigte Hardware (Smart Cards eines ZDAs) + SigG-bestätigte Zeitstempel-Software * außerhalb eines ZDA betrieben | sichere Hardware (HSM–Hardware Security Module) + SigG-bestätigte Zeitstempel-Software | Standard Hardware (Server) + SigG-bestätigte Zeitstempel-Software |
|---|---|---|---|---|---|
| Erzeugung qualifizierter ZS gemäß SigG | ja | ja | nein | nein | nein |
| Erzeugung sonstiger ZS | ja | ja | ja | ja | ja |
| ZS sind beweiskräftig vor Gericht gemäß SigG | ja | ja | nein | nein | nein |
| ZS Prüfbarkeit mindestens 30 Jahre gesetzlich gesichert | ja | nein | nein | nein | Nein |
| ZS Prüfbarkeit mindestens 5 Jahre gesetzlich gesichert | Ja | Ja | nein | nein | nein |
| ZS Prüfbarkeit ist auch bei „Ausfall" (z.B. Insolvenz od. Geschäftsaufgabe) des Anbieters bzw. Erstellers gewährleistet | ja | nein | nein | nein | nein |
| ZS zum Nachsignieren nach § 6 SigG und § 17 SigV geeignet | ja | bedingt | nein | nein | nein |
| BNetzA verpflichtet sich gesetzlich, die Prüfbarkeit der ZS bei „Ausfall" des ZDAs sicher zu stellen | ja | nein | nein | nein | nein |
| Deckungsvorsorge gemäß SigG (Versicherung gegen Vermögensschäden von 2,5 Mio./ZS) | ja | ja | nein | nein | nein |

Technische Möglichkeiten zur Erzeugung von Zeitstempeln: nur in besonderer Einsatzumgebung möglich.

### Merksätze Zeitstempel

1) Zeitstempel sind einfacher als elektronische Signaturen zu verwenden, da Zeitstempel vollautomatisch und personenunabhängig, bzw. anonym verwendet werden können.

2) Qualifizierte Zeitstempel akkreditierter Anbieter frieren elektronische Daten rechtssicher und vor Gericht beweiskräftig für mindestens 30 Jahre ein. Die Beweiskraft gilt unabhängig von einer branchen- oder prozessspezifischen Gesetzgebung (z.B. Sozialversicherungsrecht, Umsatzsteuergesetz).

3) „Sonstige Zeitstempel" (nicht qualifizierte Zeitstempel) unterliegen der freien Beweiswürdigung und benötigen einen besonderen Nachweis, bzw. eine spezielle rechtliche Grundlage zur Anerkennung.

4) Ausschließlich durch die Bundesnetzagentur akkreditierte oder angezeigte Zertifizierungsdiensteanbieter können qualifizierte Zeitstempel gemäß § 2 SigG erstellen.

5) Der Einsatz von SigG-bestätigter Hard- und Software allein ist nicht ausreichend, um qualifizierte elektronische Zeitstempel zu erzeugen.

6) Qualifizierte Zeitstempel eines akkreditierten Zertifizierungsdiensteanbieters sind auch im Falle einer Einstellung der Tätigkeit, Widerruf der Akkreditierung oder Insolvenz, weiterhin prüfbar.

7) Von akkreditierten Anbietern qualifiziert zeitgestempelte Daten können mindestens 30 Jahre als gesetzeskonformes Beweismittel verwendet werden.

8) Da qualifizierte Zeitstempel ausschließlich von behördlich akkreditierten (angezeigten) Diensten erstellt werden können, sind vorsätzliche oder unbeabsichtigte Zeit-Manipulationen, wie z.B. das Verstellen der Systemzeit des Clients bei der Signaturerstellung nicht möglich.

# Veranstaltungen

### Messen Kongresse

**4. IT Security Forum Regensburg**
IT Security Awareness
7.5.2009, Hochschule Regensburg,
Josef Stanglmeier Hörsaal
http://homepages.fh-regensburg.de

**IT-Sicherheits-Forum**
ComConsult Akademie
11.5. – 14.5.2009, Königswinter
www.comconsult-akademie.com

**11. Deutscher IT-Sicherheitskongress**
BSI - Bundesamt f. Sicherh. i. d. Informationstech.
12.5. – 14.5.2009, Bonn
www.bsi.de/veranst

**VoIP Day Stuttgart 09**
Tele-Consulting GmbH
15.5.2009, Stuttgart
www.tele-consulting.com

**DuD 2009 - Datenschutz und Datensicherheit**
COMPUTAS GmbH
8.6. – 9.6.2009, Berlin
www.computas.de

### Seminare

**Kommunikationssicherheit im Internet**
DFN-CERT Services GmbH
7.5. – 8.5.2009, Hamburg
www.dfn-cert.de

**IT-Notfallplanung**
Management Circle AG
12.5. – 13.5.2009, Düsseldorf
www.managementcircle.de

**IT-Security Management nach IT-Grundschutz (BSI)**
Filges IT Beratung
14.5. – 15.5.2009, Oberhausen (Ruhrgebiet)
www.filges.de

**Erfolgreiche Awareness-Kampagnen**
ITACS Training AG
15.5.2009, Zürich
www.itacs.com

**BSI IT-Grundschutz**
BSP. SECURITY
18.5. – 20.5.2009 Regensburg
www.bsp-security.de

**IT-Grundschutz nach BSI**
CBT Training & Consulting GmbH
18.5. – 20.5.2009 München
www.cbt-training.de

**BSI GSTOOL-Anwenderschulung**
PROKODA GmbH
25.5.2009 Berlin
www.prokoda.de

**Das kleine 1x1 der Verschlüsselung für Datenschutzbeauftragte**
datakontext GmbH
16.6.2009 Köln
www.datakontext.com

**Datenschutz aktuell**
FFD Forum für Datenschutz
16.6. – 17.6.2009 Wiesbaden
www.ffd-seminare.de

**Moderne Methoden der Risikoquantifizierung**
qSkills GmbH & Co. KG
16.6. – 17.6.2009, Nürnberg
www.qskills.de