



White Paper

Elektronische Zeitstempel

Gesetzlich verankerte Absicherung
für elektronische Geschäftsprozesse aller Art,
auch in Ergänzung zu elektronischen Signaturen

AuthentiDate International AG
Rethelstraße 47
40237 Düsseldorf / Germany
Fon +49 (0)211 – 43 69 89 0

info@authentidate.de
www.authentidate.de



© 2009 - 2011 AuthentiDate International AG (alle Rechte vorbehalten)

Vervielfältigung nur mit ausdrücklicher Genehmigung der AuthentiDate International AG. Alle genannten Marken sind Marken ihrer jeweiligen Eigentümer. Irrtümer, Änderungen und Verfügbarkeit bzgl. genannter Produkte, Leistungen, Eigenschaften und Nutzungsmöglichkeiten vorbehalten. Produkte und Services werden durch die AuthentiDate Deutschland GmbH bereitgestellt. AuthentiDate übernimmt keine Gewähr für die Richtigkeit von Angaben Dritter über Eigenschaften, Leistungen und Verfügbarkeit. Im Zuge der Produktentwicklung behält sich AuthentiDate das Recht vor Änderungen an Produkten und Leistungen auch ohne vorherige Benachrichtigung vorzunehmen. Keine der Ausführungen und Darstellungen stellen eine Rechtsberatung dar oder dürfen in solcher Weise interpretiert werden. Im Fall von Abweichungen zu, in diesem Dokument in Zusammenhang stehenden Vertragsdokumenten und allgemeinen Geschäftsbedingungen der AuthentiDate, gehen die Vertragsdokumente bzw. allgemeinen Geschäftsbedingungen diesem Dokument stets vor.

Stand der Dokumentation: Januar 2011, Version 1.3

Fragen und Anregungen senden Sie bitte an obige Kontaktangaben.

Inhalt

1.	Einführung.....	5
2.	Executive Summary	6
3.	Rechtliche Rahmenbedingungen	8
3.1.	Beweiskraft von qualifiziert personenbezogenen signierten und qualifiziert zeitgestempelten Daten	8
3.2.	Unterscheidung von qualifizierten und sonstigen Signaturen und Zeitstempeln	9
4.	Technische und organisatorische Anforderungen.....	11
4.1.	Technische Anforderungen an qualifizierte personenbezogene Signaturen.....	11
4.2.	Technische Anforderungen an qualifizierte Zeitstempel.....	12
4.3.	SigG-Bestätigung von Zeitstempel-Software.....	12
5.	Auswahl geeigneter Zeitstempel	14
5.1.	Qualifizierte Zeitstempel von Zertifizierungsdiensten	15
5.1.1.	Qualifizierte Zeitstempel von akkreditierten Zertifizierungsdiensten	16
5.1.2.	Qualifizierte Zeitstempel von angezeigten Zertifizierungsdiensteanbietern	18
5.1.3.	Prüfung (Verifikation) von qualifizierten Zeitstempeln.....	19
5.2.	Sonstige Zeitstempel.....	20
5.2.1.	SigG-bestätigte Hardware, Smart Cards eines ZDA und SigG-bestätigte Zeitstempel- Software	20
5.2.2.	Hardware Security Module (HSM) und SigG- bestätigte Zeitstempel-Software.....	21
5.2.3.	Standard-Server und SigG-bestätigte Zeitstempel-Software.....	21
5.2.4.	Prüfung (Verifikation) von sonstigen Zeitstempeln.....	22
5.3.	Kosten-Nutzen-Betrachtungen.....	22
6.	Kombination von personenbezogenen Signaturen und Zeitstempeln	23
6.1.	Signaturen mit und ohne Zeitstempel.....	23
6.2.	Zeitstempel senken Compliance Risiken.....	25

7.	Anwendungsszenarien für qualifizierte Zeitstempel	26
7.1.	Rechtssichere Dokumentation des Erfassungszeit- punktes und der Vollständigkeit bei gescannten Dokumenten	26
7.2.	Nach- oder Übersignieren	28
8.	Internationale Aspekte	30
9.	Über AuthentiDate	31
10.	Abkürzungsverzeichnis	33
11.	Glossar	33
12.	Legal Disclaimer	39

1. Einführung

Bereits im Juli 1997 definierten das erste Deutsche Signaturgesetz (SigG) und die Signaturverordnung (SigV) die Rahmenbedingungen für elektronische Signaturen und elektronische Zeitstempel. Nach Erscheinen der Signaturrechtlinie der Europäischen Union im Dezember 1999 wurden die deutschen Rahmenbedingungen in Einklang mit der EU-Richtlinie überarbeitet und resultierten in der Neufassung des Deutschen Signaturgesetzes vom Mai 2001. Bis auf geringe Änderungen¹ bildet diese Fassung noch heute die Basis für Erstellung und Einsatz von qualifizierten Signaturen und Zeitstempeln.

Das vorliegende White Paper „Elektronische Zeitstempel“ beschreibt die rechtlichen Rahmenbedingungen und technischen Voraussetzungen zur Erstellung von elektronischen Zeitstempeln und beleuchtet dabei auch die Unterschiede zwischen qualifizierten und nicht qualifizierten Zeitstempeln, im Folgenden zur besseren Unterscheidung als „sonstige Zeitstempel“ bezeichnet.

Es wird erklärt, wie sich qualifizierte und sonstige Zeitstempel technisch umsetzen lassen. Daneben zeigt das White Paper auf, wie sich die unterschiedliche Umsetzung auf Compliance-Aspekte, rechtliche Beweiskraft und Kostenstrukturen auswirken kann. Darüber hinaus werden in diesem White Paper exemplarisch gängige Anwendungsszenarien für elektronische Zeitstempel dargestellt.

¹ Novellierung des SigG im Februar 2005

2. Executive Summary

Unternehmen, Behörden und Organisationen aller Art und weltweit bilden zur Optimierung, Kostenreduktion und Beschleunigung zunehmend Prozesse elektronisch ab. So werden existierende papierbasierte Prozesse durch elektronische Prozesse abgelöst oder neue Prozesse durch den Einsatz digitaler Informationen und Kommunikation erst möglich.

Diese neuen, verbesserten Prozesse (mittels elektronischer Information) unterliegen den gleichen gesetzlichen Bestimmungen, Compliance- und Schutzanforderungen, wie herkömmliche papierbasierte Prozesse. Um diesen Anforderungen zu genügen, ist sowohl papierbasierte, als auch elektronische Information u.a. vor Manipulation und Verlust zu schützen. Zur Beurteilung der Einhaltung von Compliance Anforderungen im professionellen Umfeld sind daher häufig der Nachweis der Integrität, Vollständigkeit und Vertraulichkeit die wesentlichen Kriterien.

Elektronische Zeitstempel können diesen Nachweis der Integrität und der Vollständigkeit einfach, rechtssicher, dauerhaft, kostengünstig und auf Wunsch anonym zur Verfügung stellen.

Ein Zeitstempel (engl.: time stamp) ist ein Wert in einem definierten Format, der einem Ereignis (beispielsweise dem Senden oder Empfangen einer Nachricht, der Modifikation von Daten u.a.) einen Zeitpunkt zuordnet. Der Zweck eines Zeitstempels ist es, für Menschen oder Computer deutlich zu machen, wann welche Ereignisse eintraten.

Als Zeitstempel bezeichnet man auch Bescheinigungen, dass ein elektronisches Dokument zu der angegebenen Zeit dem Aussteller des Zeitstempels vorgelegen hat. Sie sind für den Einsatz elektronischer Signaturen im Rechtsverkehr unverzichtbar. Das deutsche Signaturgesetz regelt die Anforderungen für die Ausstellung von **qualifizierten Zeitstempeln** als besonders hochwertige Form einer solchen Bescheinigung, bei der sichergestellt ist, dass die gültige gesetzliche Zeit aufgenommen wurde, und bei denen Fälschungen und Verfälschungen ausgeschlossen sind. Bei den heute verwendeten Verfahren enthält der qualifizierte Zeitstempel einen Hash-Wert des bescheinigten Dokumentes und die aktuelle Zeitangabe (Datum und Uhrzeit), und sind mit einer qualifizierten elektronischen Signatur des Ausstellers versehen.

Quelle: WIKIPEDIA

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“. Im Gegensatz zur elektronischen Signatur ist ein Zeitstempel nicht an Personen und deren Handlungen gebunden. Er kann daher wesentlich einfacher und auch vollautomatisch in elektronische Prozesse eingebunden werden.

So können elektronische Zeitstempel für Unternehmen, Behörden und Organisationen erhebliche Vorteile

bringen, indem kostengünstig und sicher elektronische Prozesse eingeführt werden können, ohne die notwendige Sicherheit im Bezug auf Einhaltung gesetzlicher Bestimmungen, Nachvollziehbarkeit und Compliance zu vernachlässigen.

Eine besondere Stellung nehmen so genannte qualifizierte Zeitstempel von akkreditierten Anbietern ein. Diese Art der Zeitstempel genießen den besonderen gesetzlichen Schutz (über das Signaturgesetz) und

können so auch für vergleichsweise ungeschützte elektronische Daten einen zuverlässigen, langfristigen Schutz über mindestens 30 Jahre garantieren.

Für die Erstellung dieser Art Zeitstempel gelten besondere rechtliche und technische Anforderungen. Dennoch sind sie, z.B. im Vergleich zu qualifizierten personenbezogenen Signaturen, einfacher zu verwenden, da der Anwender selbst über keine spezielle gesetzeskonforme Hard- oder Software verfügen muss und keine manuelle Interaktion des Anwenders, wie z.B. PIN-Eingaben, erforderlich sind. Der qualifizierte Zeitstempel wird einfach von einem behördlich akkreditierten Anbieter, dem „Zertifizierungsdiensteanbieter“ bezogen. Damit wird der qualifizierte Zeitstempel dieser Anbieter zu einem leicht verwendbaren „Werkzeug“, welches in jeden Prozessschritt, unabhängig von Ort und Branche, eingebracht werden kann und dessen Rechtssicherheit verbessert.

Hohe Flexibilität in Verbindung mit der Verfügbarkeit an jedem Ort, zu jeder Zeit und in (nahezu) jeder Menge macht den qualifizierten Zeitstempel zu einem wertvollen, leicht zu verwendenden Werkzeug für den rechtssicheren Schutz elektronischer Daten und Prozesse.

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

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).

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

3. Rechtliche Rahmenbedingungen

Das Deutsche Signaturgesetz beschreibt neben der qualifizierten elektronischen Signatur auch den qualifizierten Zeitstempel². Die elektronische Signatur dient gemäß § 2 (1) SigG in erster Linie zur Authentifizierung in Verbindung mit bestimmten, mit der Signatur verknüpften oder beigefügten Daten. Die elektronische Signatur dokumentiert somit das „Wer“ und „Was“. Im Gegensatz dazu stellt der Zeitstempel gemäß § 14 (14) SigG eine elektronische Bescheinigung dar, welche aussagt, wann bestimmte Daten vorlagen. Er dokumentiert somit das „Wann“ und „Was“.

Zum Thema internationale rechtliche Aspekte vgl. Kap.8.

3.1. Beweiskraft von qualifiziert personenbezogenen signierten und qualifiziert zeitgestempelten Daten

Wie auf der Website der Bundesnetzagentur in der FAQ 9 formuliert, legt das Deutsche Signaturgesetz den Grundstein dafür, dass alle Rechtsgeschäfte, die einem gesetzlichen Schriftformerfordernis unterliegen, in elektronischer Form (mit qualifizierter Signatur) durchführbar sind.³

Hervorzuheben ist, dass nur bei Verwendung qualifizierter Signaturen (bzw. Zeitstempel) eine der Schriftform gleichgestellte, gesetzeskonforme, elektronische Abbildung von vormals papierbasierten Prozessen möglich ist.

Je nachdem, in welchem Kontext die personenbezogene Signatur bzw. der Zeitstempel verwendet wird, definieren ggf. branchen- und/oder prozessspezifische Gesetzgebungen, Novellen und Rahmenbedingungen ergänzend die rechtliche Beweiskraft der Signaturen und Zeitstempel.

Signaturgesetz und Signaturverordnung definieren somit die branchen- und prozessneutralen Rahmenbedingungen.

Entscheidend für den Anwender ist, dass die Definitionen des Signaturgesetzes und der Signaturverordnung gesetzlich fest verankert und daher bindend sind. D.h. ein branchen- oder prozessspezifisches Gesetz kann nur auf eine qualifizierte Signatur bzw. einen Zeitstempel gemäß Signaturgesetz referenzieren. Es kann nicht definieren, wie diese qualifizierte Signatur bzw. der qualifizierte Zeitstempel erstellt werden und welche Sicherheitseigenschaft und Beweiseigenschaften somit zum Tragen kommen. Dies wird stets einheitlich im Signaturgesetz und in der Signaturverordnung definiert.

² s. § 2 SigG

³ vgl. FAQ 9 BNetzA www.bundesnetzagentur.de

Typisches Beispiel für eine prozessspezifische Anforderung ist das aktuelle Umsatzsteuergesetz. In § 14 Abs. 3 UStG ist definiert, dass elektronische Rechnungen nur zum Vorsteuerabzug herangezogen werden können, wenn sie mit einer qualifizierten personenbezogenen Signatur nach dem Signaturgesetz versehen sind.

Typisches Beispiel für eine branchenspezifische Anforderung ist die Bestätigung des Medienbruchs in der Massenbelegerfassung bei zahlungsrelevanten Belegen der gesetzlichen Krankenkassen. Hier definiert u.a. das Sozialversicherungsrecht, welchem alle gesetzlichen Krankenkassen unterliegen, dass zwingend eine qualifizierte personenbezogene Signatur verwendet werden muss, wenn Papierdokumente nach dem Scannen (Massenbelegerfassung) vernichtet werden. Dies wird auch von der für diese spezielle Branche zuständigen Behörde (dem Bundesversicherungsamt - BVA) überwacht. Details zum Einsatz der qualifizierten personenbezogenen Signatur gemäß Signaturgesetz sind daher in der branchenspezifischen Gesetzgebung (§ 286 Abs. 3 SGB V, § 17 SVRV und § 36, § 40, § 41 SRVwV) und den jeweiligen Dienstanweisungen des BVA zu finden.

3.2. Unterscheidung von qualifizierten und sonstigen Signaturen und Zeitstempeln

Zusätzlich zu der „Art“ (personenbezogene Signatur oder Zeitstempel) beschreibt das Signaturgesetz verschiedene „Sicherheitsstufen“. Dies kommt, zumindest im Zusammenhang mit personenbezogenen Signaturen, durch die ergänzenden Bezeichnungen „fortgeschritten“ und „qualifiziert“ zum Ausdruck.

Hierbei differenziert das Signaturgesetz wie folgt:

- „fortgeschrittene elektronische Signaturen“ (§ 2 Nr.2 SigG)
 - sind ausschließlich dem Signaturschlüssel-Inhaber zugeordnet
 - ermöglichen die Identifizierung des Signaturschlüssel-Inhabers
 - werden mit Mitteln erzeugt, die der Signaturschlüssel-Inhaber unter seiner alleinigen Kontrolle halten kann
 - und sind so mit den Daten, auf die sie sich beziehen, verknüpft. Eine nachträgliche Veränderung kann somit ausgeschlossen werden.

- „qualifizierte elektronische Signaturen“ (§2 Nr.3 SigG)
 - beruhen zusätzlich zu den Anforderungen für fortgeschrittene Signaturen auf einem zum Zeitpunkt ihrer Erstellung gültigem qualifizierten Zertifikat und
 - werden mit einer sicheren Signaturerstellungseinheit (Signaturkarte) erzeugt.

Ein typisches Beispiel für eine fortgeschrittene personenbezogene Signatur ist eine elektronische Signatur, die mit einem Softwarezertifikat erstellt wird. Mit dem Softwarezertifikat ist z.B. der Name des Zertifikatsinhabers verknüpft. Mit Hilfe einer Client-Software

kann der Anwender z.B. ein Dokument elektronisch unterschreiben. Da kein qualifiziertes Zertifikat und keine sichere Signaturerstellungseinheit verwendet wird, handelt es sich hierbei bestenfalls um eine fortgeschrittene personenbezogene Signatur. Mit dieser fortgeschrittenen personenbezogenen Signatur ist keine Beweiskraft garantiert⁴.

Auf dem Signaturgesetz aufbauende Gesetze, wie z.B. die ZPO⁵, setzen die fortgeschrittene Signatur nicht mit der handschriftlichen Unterschrift gleich. Dementsprechend ist mit der fortgeschrittenen Signatur bzw. den signierten Daten auch keine Rechtswirksamkeit verbunden.

Eine qualifizierte personenbezogene Signatur wird mit Hilfe von geprüften und bestätigten Kartenlesern (Smart Card Terminals), sicheren Signaturkarten (z.B. T-TeleSec TCOS V3, D-Trust, etc.) und geeigneten Signaturanwendungskomponenten (Signatursoftware) erstellt. Alle drei genannten 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 u.a. auch für elektronische Zeitstempel. Für diese ist gemäß Signaturgesetz eine besonders gesicherte Einsatzumgebung zwingend festgelegt. Diese Einsatzumgebung muss durch ein Sicherheitskonzept, Zugangsschutz und kontinuierliche Überwachung geschützt sein. Daher können qualifizierte Zeitstempel nur von, durch die Bundesnetzagentur, akkreditieren (bzw. angezeigten) Diensteanbietern ausgestellt werden.

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 Anforderung der gesetzlichen Anforderungen nicht erfüllt ist, ist die erstellte Signatur bzw. der Zeitstempel immer „nicht qualifiziert“.

Dies gilt auch, wenn z.B. eine bestimmte Einsatzumgebung für die Erstellung der Signaturen bzw. Zeitstempel vorgegeben ist. Hier sei das Beispiel der massenhaften Erstellung von personenbezogenen Signaturen genannt. Gemäß Bundesnetzagentur ist für Massensignaturen eine geeignete Einsatzumgebung mit Zugangsschutz und Überwachung, wie ein Stahlschrank oder ein Rechenzentrum, unabdingbare Voraussetzung⁶. Fehlt diese Voraussetzung, kann keine qualifizierte Signatur im Massensignaturverfahren erstellt werden,

⁴ vgl. Website der BNetzA www.bundesnetzagentur.de

⁵ s. § 371a ZPO

⁶ s. Website der Bundesnetzagentur FAQ 18

selbst wenn alle anderen Voraussetzungen in Bezug auf die verwendete Hard- und Software gegeben sind.

Nicht ausführlich im Signaturgesetz erwähnt ist die Form der einfachen Signatur⁷. Im Allgemeinen wird hierunter eine Signatur verstanden, die weder mit Hilfe eines qualifizierten noch fortgeschrittenen Zertifikats und auch ohne Signaturerstellungseinheit erstellt wird. Dies kann z.B. eine Fußnote unter einer Email sein. Aufgrund der geringen rechtlichen Relevanz wird in diesem White Paper auf die einfache Signatur nicht weiter eingegangen.

4. Technische und organisatorische Anforderungen

4.1. Technische Anforderungen an qualifizierte personenbezogene Signaturen

Wie dargestellt, ist gemäß § 2 SigG zur Erstellung von qualifizierten personenbezogenen Signaturen zwingend die Verwendung geeigneter Hardware (Signaturerstellungseinheit) und Software (Signaturanwendungskomponente) erforderlich. Sowohl Hardware als auch Software müssen den Anforderungen des Signaturgesetzes entsprechen. So muss beispielsweise für die Software eine Prüfung und Bestätigung nach Signaturgesetz (SigG-Bestätigung) vorliegen oder eine Herstellererklärung bei der Bundesnetzagentur eingereicht und von dieser veröffentlicht sein⁸. Verfügt der Anwender über die gesetzeskonformen Hard- und Software-Komponenten, kann er selber und an jedem Ort qualifizierte personenbezogene Signaturen erstellen⁹. Vereinfacht heißt dies, es genügen zur Erstellung einer qualifizierten Signatur eine Signaturkarte (sichere Signaturerstellungseinheit - SSEE) eines Zertifizierungsdiensteanbieters, ein bestätigter Kartenleser und eine Signaturanwendungskomponente (SAK). Die Signaturanwendungskomponente muss entweder SigG-bestätigt sein oder alternativ über eine von der Bundesnetzagentur veröffentlichte¹⁰ Herstellererklärung verfügen.

⁷ S. § 2 Abs. 1 SigG

⁸ s. §17 (4) SigG und ergänzend 1.SigÄndG vom 4.01.2005

⁹ zu berücksichtigen sind prozess- und branchenspezifische Zusatzanforderungen, wie z.B. Einsatzumgebung bei Massensignaturen (s. Website der BNetzA / FAQ 18)

¹⁰ www.bundesnetzagentur.de

4.2. Technische Anforderungen an qualifizierte Zeitstempel

Auch an die Hard- und Software zur Erstellung von qualifizierten Zeitstempeln sind strenge Anforderungen geknüpft. Wie bereits im Abschnitt 3.2 erläutert, können im Unterschied zu qualifizierten personenbezogenen Signaturen qualifizierte Zeitstempel nicht von jedermann an jedem beliebigen Ort erstellt werden. Der Einsatz gesetzeskonformer Hard- und Software ist nicht ausreichend.

Ein qualifizierter Zeitstempel ist gemäß § 2 Nr.14 SigG eine Bescheinigung eines Zertifizierungsdiensteanbieters. Somit muss ein qualifizierter Zeitstempel zwingend von einem solchen ausgestellt werden. Der Anbieter betreibt dazu einen Zertifizierungsdienst, im Allgemeinen als Trust Center bezeichnet. Dieser Zertifizierungsdienst muss eine Reihe von Anforderungen gemäß § 4 SigG erfüllen (s. Kap. 5).

Zertifizierungsdienste gibt es in zwei Ausprägungen; den akkreditierten und den angezeigten Zertifizierungsdienst. Beide sind in der Lage qualifizierte Zeitstempel auszustellen. Für den Anwender ergeben sich jedoch unterschiedliche rechtliche Möglichkeiten bei Nutzung der beiden Formen von Zertifizierungsdiensten. Sie sind in Tabelle 1 aufgezeigt und in Kap. 5 näher erläutert.

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

4.3. SigG-Bestätigung von Zeitstempel-Software

Vielfach wird der Einsatz von SigG-bestätigter Zeitstempel-Software diskutiert, um eine Möglichkeit zu schaffen, qualifizierte elektronische Zeitstempel auch außerhalb des Trust Centers eines angezeigten oder akkreditierten Zertifizierungsdiensteanbieters, z.B. im unternehmens-eigenen Rechenzentrum, zu erstellen. Dies ist aufgrund der gesetzlichen Vorschriften nicht möglich und wird im Weiteren näher erklärt.

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

Folgende einfache „Faustregeln“ helfen, die Auflagen bezüglich Bestätigungen, Einsatzgebieten und gesetzlicher Gültigkeit besser zu strukturieren:

1. Bestätigte Hardware und Software zur Erzeugung von qualifizierten Zeitstempeln muss zwingend in einem besonders geschützten Bereich, wie z.B. dem Trust Center eines Zertifizierungsdienstes, eingesetzt werden. Dies ergibt sich

bereits aus dem Signaturgesetz, welches die Erzeugung von qualifizierten Zeitstempeln explizit auf angezeigte und akkreditierte Zertifizierungsdiensteanbieter beschränkt.

2. Eine Bestätigung von Hardware und Software zur Erzeugung von Zeitstempeln nach SigG bezieht sich immer und ausschließlich auf den Betrieb und Einsatz bei einem Zertifizierungsdiensteanbieter. Bestätigungen von Komponenten zur Erzeugung von Zeitstempeln sind außerhalb des in der Bestätigungsurkunde angegebenen Einsatzgebietes nicht gültig.
3. Ist eine Hardware und Software speziell für den Betrieb außerhalb von Zertifizierungsdiensteanbietern nach SigG bestätigt, so bezieht sich diese Bestätigung nicht auf die Erstellung von Zeitstempeln, da Zeitstempel gemäß Signaturgesetz innerhalb eines Trust Centers eines angezeigten oder akkreditierten Zertifizierungsdiensteanbieters erstellt werden müssen. Eine derartige Bestätigung nach SigG bezieht sich daher in der Regel auf die Erstellung und/oder Prüfung von Signaturen (Signaturanwendungskomponente).
4. Eine Bestätigung nach SigG für Hardware und Software zur Erzeugung von qualifizierten Signaturen gilt nicht einfach auch für qualifizierte Zeitstempel, da der für Zeitstempel wichtigste Aspekt der gesetzlich gültigen Zeit bei einer Bestätigung für Signaturen nicht Bestandteil der Bestätigung ist.
5. Gilt eine Bestätigung nach SigG für bestimmte Rahmenbedingungen, wie Einsatzzweck (z.B. Signaturen) und Einsatzort (z.B. besonders geschützter Bereich) und wird nur eine dieser Bedingungen verletzt, so entfällt die Bestätigung vollständig – es „überlebt“ nicht der Rest.

5. Auswahl geeigneter Zeitstempel

Wie bereits in Kapitel 3.2 ausgeführt, sind Zeitstempel in unterschiedlichen Ausprägungen verfügbar. Je nach individueller rechtlicher, technischer und kaufmännischer Anforderung ist hier die Auswahl zu treffen und zu entscheiden, ob „qualifizierte“ oder „sonstige Zeitstempel“ zum Einsatz kommen sollen, bzw. müssen.

Im Allgemeinen sind vor Auswahl die folgenden Fragestellungen zu beantworten und anschließend mit den technischen Voraussetzungen abzugleichen (weitere branchenspezifische, individuelle Anforderungen sind ebenfalls zu prüfen):

- Wie lange sollen die Zeitstempel rechtlich verbindlich geprüft werden können?
- Wie lange soll z.B. die Integrität und damit Vollständigkeit der Daten zu einem bestimmten Zeitpunkt rechtssicher nachgewiesen werden können?
 - Mindestens 30 Jahre
 - Mindestens 5 Jahre
 - Keine rechtlich verbindliche Prüfung erforderlich; die Vollständigkeit der zeitgestempelten Daten muss nicht nachgewiesen werden
- Soll die Prüfung der Zeitstempel auch dann gewährleistet sein, wenn z.B. der Anbieter bzw. Ersteller der Zeitstempel seine Geschäftstätigkeit einstellt?
- Sollen die zeitgestempelten Daten vor Gericht als Beweismittel genutzt werden können; unabhängig davon, ob eine spezifische Gesetzgebung für die Branche oder den Geschäftsprozess, in welchem die Zeitstempel Verwendung finden, existiert?
- Sollen die Zeitstempel zum Nachsignieren (Übersignieren) gemäß § 17 SigV genutzt werden?
- Soll das eigene Haftungsrisiko gesenkt und Risiken auf Lieferanten, wie z.B. denjenigen, der den Zeitstempel erstellt, verlagert oder aufgeteilt werden?

Die nachfolgende Tabelle 1 zeigt konsolidiert die Abhängigkeiten zwischen den rechtlichen Eigenschaften und der technischen Umsetzung bei der Erstellung von Zeitstempeln auf.

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 *	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 außerhalb eines ZDA betrieben	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

Tab. 1 – Konsolidierte Darstellung Zeitstempel Eigenschaften in Abhängigkeit der technischen und organisatorischen Voraussetzungen, bzw. Einsatzbereiche

* Zeitstempelsoftware kann grundsätzlich SigG-bestätigt sein. Wird diese jedoch außerhalb eines Zertifizierungsdienstes eingesetzt, verliert die SigG-Bestätigung ihre Gültigkeit.

Die in Tabelle 1 aufgeführten Einsatzbereiche werden im Folgenden näher spezifiziert.

5.1. Qualifizierte Zeitstempel von Zertifizierungsdiensten

Es bestehen grundsätzlich nur zwei Alternativen qualifizierte Zeitstempel gemäß Signaturgesetz und damit rechtlich wirksam zu erzeugen.

- a. Im Betrieb (Trust Center) eines akkreditierten Zertifizierungsdiensteanbieters gemäß SigG oder
- b. Im Betrieb (Trust Center) eines angezeigten Zertifizierungsdiensteanbieters gemäß SigG

Im Gegensatz zu qualifizierten personenbezogenen Signaturen ist der Ort, an dem die qualifizierten Zeitstempel physisch erstellt werden, von entscheidender Bedeutung. Zwingende Voraussetzung ist der Betrieb, also die geprüfte und bestätigte sichere räumliche Umgebung eines Zertifizierungsdienstes. Dieser wird, wie schon beschrieben, im Allgemeinen als Trust Center bezeichnet.

Qualifizierte Zeitstempel können nur von, gemäß Signaturgesetz akkreditierten oder angezeigten, Zertifizierungsdiensteanbietern (ZDA) erstellt werden.

Qualifizierte Zeitstempel müssen immer in einer geprüften, bestätigten und isolierten Einsatzumgebung (z.B. Trust Center) erstellt werden.

Der Betrieb eines Zeitstempeldienstes für qualifizierte Zeitstempel nach Signaturgesetz ist bei der Bundesnetzagentur anzeige- oder akkreditierungspflichtig.

Zeitstempel, die nicht durch einen angezeigten oder akkreditierten ZDA erstellt werden, sind immer sonstige Zeitstempel. Dies ist unabhängig davon, in welcher Umgebung und mit welcher Hard- bzw. Software sie erzeugt werden.

5.1.1. Qualifizierte Zeitstempel von akkreditierten Zertifizierungsdiensten

Akkreditierte Zertifizierungsdiensteanbieter unterliegen strengen Anforderungen, deren Erfüllung kontinuierlich, d.h. zu jedem Zeitpunkt des Betriebs von der Bundesnetzagentur überwacht wird¹¹. Bei Verstoß, d.h. Nicht-Erfüllung der Anforderungen, kann der Betrieb sofort von der Bundesnetzagentur untersagt werden.

Diese hohen Anforderungen an den akkreditierten Zertifizierungsdiensteanbieter 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 Zertifizierungsdiensteanbieter vorteilhaft auf die Anwender bzw. Kunden auswirken, sind exemplarisch im Folgenden einige Aspekte dargestellt, welche gemäß § 4 SigG vom Zertifizierungsdiensteanbieter umzusetzen sind.

¹¹ s. §4 Abs.4) SigG

Wesentliche Anforderungen an akkreditierte Zertifizierungsdiensteanbieter gemäß § 4 SigG:

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

Für die Anwender ergeben sich aus der Akkreditierung zwei wesentliche Vorteile:

1. Gemäß § 15 Abs.6 SigG stellt die Bundesnetzagentur immer sicher, dass eine Abwicklung der Verträge, die der Zertifizierungsdiensteanbieter geschlossen hat, über die gesetzliche Frist ermöglicht wird. Dies bedeutet:
Qualifizierte Zeitstempel eines akkreditierten Zertifizierungsdiensteanbieters sind auch im Falle einer Einstellung der Tätigkeit, Widerruf der Akkreditierung oder Insolvenz, weiterhin prüfbar.
2. Gemäß § 4 SigV muss ein akkreditierter Zertifizierungsdiensteanbieter die Prüfbarkeit qualifizierter Zertifikate mindestens 30 Jahre nach Ablauf der Gültigkeit des jeweiligen Zertifikates sicherstellen. Qualifizierte Zeitstempel von akkreditierten Zertifizierungsdiensteanbietern sind somit mindestens 30 Jahre nach Zeitstempelung prüfbar. Dies bedeutet:
Von akkreditierten Anbietern qualifiziert zeitgestempelte Daten können mindestens 30 Jahre als gesetzeskonformes Beweismittel verwendet werden.

Insbesondere diese Sicherheit - auch im Falle der Aufgabe des Geschäftsbetriebes oder einer Insolvenz - macht den qualifizierten

Zeitstempel eines akkreditierten Anbieters zu einem wertvollen Rohstoff mit hoher Investitionssicherheit. Speziell für langfristig rechtsichere Daten bietet sich daher dessen Einsatz an.

An dieser Stelle ist anzumerken, dass der Gesetzgeber für akkreditierte Zertifizierungsdienste eine Nachprüfbarkeit von Zertifikaten und/oder Zeitstempeln von mindestens 30 Jahren „bei Bedarf“ vorschreibt. Da bei der Erstellung eines Zertifikates oder Zeitstempels in der Regel der „Bedarf“ nicht für die folgenden 30 Jahre auszuschließen ist, besteht diese Verpflichtung faktisch für alle erstellten Zertifikate und Zeitstempel.

Ergänzend ist zu bemerken, dass qualifizierte Zeitstempel, die in einem Trust Center erstellt werden, sogar Intervalle kleiner einer Sekunde differenzieren. Über eine Paginierung werden Daten, die innerhalb derselben Sekunde zeitgestempelt werden, nach Eingangszeitpunkt des Zeitstempel-Requests beim Trust Center unterschieden und paginiert.

5.1.2. Qualifizierte Zeitstempel von angezeigten Zertifizierungsdiensteanbietern

Qualifizierte Zeitstempel von angezeigten Zertifizierungsdiensteanbietern erfüllen die in 5.1.1 genannten Anforderungen nur zum Teil. Sie tragen daher auch kein Gütesiegel der Bundesnetzagentur. Im Wesentlichen erfüllen sie die Anforderungen (a) bis (c), d.h. Nachweis der Zuverlässigkeit und Fachkunde, Sicherheitskonzept und Deckungsvorsorge.

Angezeigte Zertifizierungsdiensteanbieter unterliegen keiner umfassenden Prüfung der technischen und administrativen Sicherheit und keiner Prüfung und Bestätigung des Sicherheitskonzeptes einschließlich Wiederholung.

Für Anwender bedeutet dies im Vergleich zu akkreditierten Anbietern zwei signifikante Einschränkungen:

1. Im Falle der Geschäftsaufgabe oder Insolvenz des angezeigten Zertifizierungsdiensteanbieters besteht keine gesetzliche Sicherheit, dass diese noch prüfbar sind. Die Prüfbarkeit kann somit, ohne dass der Anwender dies bemerkt von einem Tag auf den anderen erlöschen. Der Anwender hat dann keinerlei Möglichkeit mehr, seinen Datenbestand in Bezug auf die Integrität zu einem bestimmten Zeitpunkt nachzuweisen oder nachträglich zu sichern.
2. Zertifikate angezeigter Zertifizierungsdiensteanbieter müssen gemäß § 4 Abs.1 SigV nur fünf Jahre ab Ablauf des Zertifikates prüfbar sein. Unabhängig von der Geschäftstätigkeit des

Anbieters können die zeitgestempelten Daten somit ggf. maximal fünf Jahre nach Ablauf des Zertifikates als Beweismittel herangezogen werden. Da qualifizierte Zeitstempel insbesondere für Bereiche, wie langfristige Datenintegrität, Langzeitarchivierung und Nachsignieren verwendet werden, ist der Einsatz in diesen Bereichen nur sehr eingeschränkt möglich, bzw. sinnvoll.

5.1.3. Prüfung (Verifikation) von qualifizierten Zeitstempeln

Sowohl der Prüfung (Verifikation) von personenbezogenen Signaturen, als auch von Zeitstempeln kommt eine besondere Bedeutung zu. Die Erstellung einer Signatur bzw. eines Zeitstempels allein kann die Beweiskraft elektronischer Daten nicht ermöglichen. Erst wenn in einem ebenfalls rechtssicheren und den gesetzlichen Anforderungen entsprechenden Verfahren nachgewiesen werden kann, dass die Signatur bzw. der Zeitstempel korrekt sind, können die elektronischen Daten als Beweismittel verwendet werden.

Im Fall der personenbezogenen Signatur sind die Kriterien einer personenbezogenen Signatur gemäß § 2 SigG zu prüfen, d.h. Authentizität und Integrität der Daten.

Im Falle eines Zeitstempels sind gemäß § 2 SigG die Bescheinigung des Zeitpunktes in Verbindung mit der Integrität der elektronischen zeitgestempelten Daten zu prüfen.

Wie in Kap. 5.1.1. dargestellt, nehmen qualifizierte Zeitstempel von akkreditierten Anbietern bei der Nachhaltigkeit der Prüfungsmöglichkeit eine Sonderstellung ein.

Qualifizierte Zeitstempel akkreditierter Zertifizierungsdiensteanbieter sind mindestens 30 Jahre nach Ende des Jahres prüfbar in dem die Gültigkeit des Zertifikates endet. Unabhängig davon, ob der Zertifizierungsdiensteanbieter zu diesem Zeitpunkt noch akkreditiert ist oder seine Geschäftstätigkeit überhaupt noch betreibt. Dieser Zeitraum ist im Signaturgesetz festgelegt und wird durch eine Eigenerklärung/Selbstverpflichtung der Bundesnetzagentur garantiert. Dadurch wird eine sehr hohe Investitionssicherheit für jeden Anwender gewährleistet. Deren zeitgestempelte Daten können mindestens 30 Jahre lang als gesetzliches Beweismittel verwendet werden.

Im Unterschied dazu besteht für qualifizierte Zeitstempel **angezeigter Zertifizierungsdiensteanbieter gesetzlich geregelt maximal eine Prüfbarkeit von fünf Jahren** ab Ablaufzeitpunkt des Zertifikates. Jedoch ist dieser Zeitraum nicht garantiert und kann, z.B. durch Einstellung der Tätigkeit des Dienstes, auch jederzeit früher enden.

Da die Bundesnetzagentur bei angezeigten Zertifizierungsdiensteanbietern nicht verpflichtet ist, eine Möglichkeit zur Prüfung der verwendeten Zertifikate für mindestens 30 Jahre zu schaffen, wird bei Aufgabe der Geschäftstätigkeit oder Insolvenz des angezeigten Anbieters auch in der Regel keine Prüfung der Zeitstempel mehr möglich sein.

Damit eignet sich der Zeitstempel eines angezeigten Zeitstempeldienstes eher nur für den kurzfristigen Einsatz, welcher keine garantierte Prüfmöglichkeit über Monate oder Jahre benötigt.

5.2. Sonstige Zeitstempel

Sonstige Zeitstempel werden in der Praxis durch verschiedene technische Systeme und organisatorische Lösungen bereitgestellt. Die Bereitstellungsmöglichkeiten sind nahezu unbegrenzt. Es obliegt dem Anwender, nach Kosten- und Praktikabilitätsgründen zu wählen.

Alle nachfolgend dargestellten Möglichkeiten haben gemeinsam, dass mit den „produzierten“ sonstigen Zeitstempeln keine Gesetzeskonformität im Sinne des Signaturgesetzes verbunden ist. D.h. eine Anerkennung vor Gericht unterliegt der freien Beweiswürdigung des jeweiligen Gerichts bzw. Richters.

Im Folgenden werden einige am Markt diskutierte Lösungen skizziert und in Bezug auf Praktikabilität, Performanz und Administrierbarkeit kurz bewertet.

5.2.1. SigG-bestätigte Hardware, Smart Cards eines ZDA und SigG-bestätigte Zeitstempel-Software

Wie unter 4.3. erläutert, können durch den Einsatz SigG-bestätigter Hardware, Smart Cards und SigG-bestätigter Zeitstempelsoftware außerhalb eines Zertifizierungsdienstes keine qualifizierten Zeitstempel erzeugt werden. Dies gilt unabhängig davon, ob die Zeitstempelsoftware SigG-bestätigt ist oder nicht. D.h. diese Variante ermöglicht nur die Erstellung von „sonstigen Zeitstempeln“.

Als SigG-bestätigte Hardware ist z.B. die Nutzung von extern per USB anzuschließenden Kartenlesern im 19" RACK der Firma Reiner SCT möglich. Soll die Performanz solcher Systeme erhöht werden, kann dies stufenlos skalierbar durch zusätzliche Kartenleser, bzw. Einschübe, realisiert werden. Weitere zusätzliche Hardware wäre nicht erforderlich.

Verwendet man anstelle externer Systeme, eine SigG-bestätigte Hardware mit integrierten Kartensteckplätzen, so ist zu berücksichtigen, dass die Performanz des Systems nicht stufenlos und

beliebig erhöht werden kann. Hierzu ist die Installation eines weiteren Systems erforderlich, sobald die Anzahl der Kartensteckplätze nicht ausreicht.

Grundsätzlich ist bei Nutzung von Zeitstempelsystemen unter Einsatz von Signaturkarten stets die Geschwindigkeit der Signaturkarte der limitierende Faktor im Durchsatz des Gesamtsystems.

Zur Erstellung von „sonstigen Zeitstempeln“ eignen sich Zeitstempelösungen unter Einsatz von Signaturkarten aufgrund der geringen Performanz und vergleichsweise hohen Kosten nur bedingt.

5.2.2. Hardware Security Module (HSM) und SigG-bestätigte Zeitstempel-Software

Da bisher noch für kein am Markt verfügbares HSM eine gültige Bestätigung nach SigG vorliegt, können in dieser Variante ausschließlich „sonstige Zeitstempel“ erzeugt werden, diese jedoch mit einem besonders hohen Durchsatz.

Am Markt sind aktuell HSM Lösungen (nCipher, SafeNet, Utimaco, u.a.) mit einem Durchsatz von über 250 Transaktionen pro Sekunde verfügbar. Diese leistungsfähigen HSM Systeme werden in der Regel zusammen mit einer Zeitstempelsoftware betrieben und können so sonstige Zeitstempel in hoher Anzahl zur Verfügung stellen.

Da in der Regel nur die Zeitstempel-Software zentral verwaltet und keine einzelnen Smart Cards angeschafft und administriert werden müssen, zeichnen sich HSMs im Betrieb mit einer Zeitstempelsoftware durch hohen Durchsatz und einfache Administration aus.

5.2.3. Standard-Server und SigG-bestätigte Zeitstempel-Software

Anstatt alle kryptographischen Operationen von einem dedizierten HSM durchführen zu lassen, kann eine SigG-bestätigte Zeitstempel-Software auch allein auf einem beliebigen Server (IBM, Dell, HP, etc.) installiert und betrieben werden. Auch auf diese Weise werden „sonstige Zeitstempel“ erzeugt. Im Unterschied zur Verwendung eines HSM ergeben sich Einschränkungen im Durchsatz, da die Prozessoren eines Standard Serversystems nicht für kryptographische Operationen optimiert sind. Die Sicherheit dieser Variante ist vergleichsweise niedrig, da die privaten Schlüssel der verwendeten Zertifikate nur wenig geschützt sind. Daher obliegt es der freien Beweiswürdigung eines Richters, ob er einem sonstigen Zeitstempel auf Basis eines HSMs

einen höheren Beweiswert zuspricht, als einem Zeitstempel auf Basis eines Standard-Servers. In beiden Fällen ist keine Gesetzeskonformität im Sinne des Signaturgesetzes gegeben.

Vorteil der Nutzung von Zeitstempelsoftware auf einem Standard-Server sind die geringen Kosten des Standard-Servers im Vergleich zur Anschaffung eines HSM, sowie die höhere Skalierbarkeit im Vergleich zu Zeitstempellösungen unter Einsatz von Signaturkarten. Nachteil ist die vergleichsweise geringere Sicherheit.

5.2.4. Prüfung (Verifikation) von sonstigen Zeitstempeln

Für die Prüfung sonstiger Zeitstempel gelten keine spezifischen gesetzlichen Anforderungen. Dies bedeutet im Umkehrschluss, da keine gesetzliche Vorgabe einzuhalten ist, ist auch keine gesetzliche Sicherheit für den Anwender vorhanden, wie lange eine Prüfung sonstiger Zeitstempel möglich sein muss. Ggf. ist diese bereits kurz nach der Erstellung nicht mehr gegeben und der Anwender kann aus den zeitgestempelten Daten keinerlei Sicherheit ableiten.

Die Prüfbarkeit sonstiger Zeitstempel ist gesetzlich nicht geregelt und nicht garantiert. Sie kann unvorhergesehen enden.

Der Anwender hat daher selbst Sorge dafür zu tragen, dass alle sonstigen Zeitstempel über den erforderlichen Zeitraum prüfbar vorgehalten werden.

5.3. **Kosten-Nutzen-Betrachtungen**

Welche Art von Technologie genutzt werden sollte, hängt stets vom jeweiligen Geschäftsprozess und den Zielsetzungen ab, die durch den Einsatz von Signaturen und Zeitstempeln verfolgt werden sollen.

In manchen Prozessen kann es ausreichend sein, durch sonstige Zeitstempel eine verbesserte Nachvollziehbarkeit und so eine Risikominimierung zu erzielen. Aus Compliance-Sicht und zur Vermeidung von Haftungsrisiken ist jedoch bei einer Vielzahl von Prozessen der Einsatz von qualifizierten Zeitstempeln zu favorisieren.

Für qualifizierte Zeitstempel sprechen insbesondere der anonyme, vollautomatisierte Einsatz in Verbindung mit der einzigartigen Rechtsicherheit und langfristigen Prüfbarkeit (bei akkreditierten Diensten).

In der Kosten-Nutzen-Betrachtung werden Kosten für qualifizierte Zeitstempel im Allgemeinen als Transaktionskosten pro Zeitstempel

ausgewiesen. Dies ist darin begründet, dass jeder qualifizierte Zeitstempel von einem Zertifizierungsdiensteanbieter einzeln „on Demand“ produziert wird. Somit beansprucht jeder qualifizierte Zeitstempel Ressourcen, z.B. in Form von Bandbreiten und Rechenzentrumsleistung.

Jeder so produzierte qualifizierte Zeitstempel beinhaltet jedoch zugleich auch eine individuell für den Anwender erstellte Leistung. Nämlich die rechtssichere Dokumentation der elektronischen Daten des Anwenders. Dieser Vorgang ist vergleichbar mit der Leistung eines Notars, der rechtssicher eine Akte für seinen Klienten dokumentiert. Auch dieser berechnet seine Kosten „transaktionsbasiert“.

Der Zeitstempелеinsatz kann wesentlich optimiert werden. Dies ist für die Kosten-Nutzen-Betrachtung wichtig. So kann durch entsprechende organisatorische Maßnahmen und Prozessdesign die Anzahl der benötigten qualifizierten Zeitstempel in vielen Fällen erheblich reduziert werden, ohne auf die gesetzlich garantierte Beweissicherheit verzichten zu müssen.

Ein mögliches Verfahren zur Transaktions- und Kostenoptimierung ist die Bildung einer Gruppe, bzw. eines „Batch“. D.h. Dokumente bzw. Daten werden in spezieller Art in einer Gruppe („Batch“) zusammengefasst und durch einen einzigen qualifizierten Zeitstempel rechtssicher eingefroren. Die Integrität zu einem bestimmten Zeitpunkt eines jeden einzelnen Dokumentes aus der Gruppe kann so kostengünstig mit nur einem einzigen qualifizierten Zeitstempel rechtssicher nachgewiesen werden. Vgl. hierzu auch Kap. 7.2 „Nachsignieren“.

6. Kombination von personenbezogenen Signaturen und Zeitstempeln

6.1. Signaturen mit und ohne Zeitstempel

In vielen Prozessen werden personenbezogene Signaturen und Zeitstempel kombiniert, um rechtssicher nicht nur Authentizität und Integrität nachweisen zu können, sondern auch den Zeitpunkt der Signaturerstellung bzw. der Ablage der signierten Daten vor Gericht beweiskräftig zu dokumentieren.

Vielfach taucht in diesem Zusammenhang die Frage auf, ob in solchen Kombinationsfällen die Qualität (das rechtliche Niveau) der Signatur und des zugehörigen Zeitstempels identisch sein sollte. Anders

formuliert, die Frage danach, ob qualifiziert personenbezogen signierte Daten anschließend mit sonstigen Zeitstempeln kombiniert werden sollten und umgekehrt.

Grundsätzlich gilt nicht nur beim Einsatz von Signaturen und Zeitstempeln eine einfache Regel bzgl. Beweiskraft und Sicherheit:

Die rechtliche Beweiskraft des Gesamtprozesses ist stets so stark wie das schwächste Glied in der gesamten Prozesskette.

Nutzt man z.B. qualifizierte personenbezogene Signaturen, um rechtssicher nachzuweisen, welcher Mitarbeiter ein Dokument bestimmten Inhalts erstellt hat und kombiniert dies mit einem sonstigen Zeitstempel, so ist der Gesamtprozess (Wer, Was, Wann) nicht vollständig rechtsicher gemäß Signaturgesetz dokumentiert. Der Beweis „Wer und Was“ ist korrekt gemäß Signaturgesetz mit qualifizierter Signatur dokumentiert, jedoch das „Was und Wann“ nur mit einem „sonstigen Zeitstempel“. Dieser unterliegt der freien Beweiswürdigung – daher ist der Zeitpunkt der Erstellung des Dokumentes und der Signatur nicht zweifelsfrei sicher dokumentiert.

Das nachfolgende Beispiel verdeutlicht, warum qualifizierte personenbezogene Signaturen in der Regel mit einem „gleichwertigen“ qualifizierten Zeitstempel kombiniert werden sollten.

Alle personenbezogenen Signaturen allein, gleich ob fortgeschritten oder qualifiziert, beinhalten keine rechtlich verbindliche Zeitangabe. Durch die Verwendung falscher Zeitangaben in der Signatur kann Missbrauch entstehen.

So ist z.B. der folgende Fall jederzeit möglich:

Herr Jürgen Schmidt, ein enthusiastischer Automobil-Liebhaber, erwirbt über das Internet ein Fahrzeug. Nachdem er sich mit dem Verkäufer, Herrn Peter Müller, über das Fahrzeug, Lieferung und Preis geeinigt hat, sendet ihm der Verkäufer, Herr Müller, einen Kaufvertrag per E-Mail zu. Der Vertrag ist ein PDF Dokument, welches bereits von Herrn Müller qualifiziert signiert wurde – mit der Bitte um Gegenzeichnung.

Herr Schmidt ist sich jedoch unsicher, ob seine Bank das Fahrzeug auch finanziert – gleichzeitig will er sich die Gelegenheit nicht entgehen lassen. Daher stellt er die Uhr seines Computers um zwei Tage vor und unterschreibt den Vertrag auf seinem PC mit qualifizierter Signatur. Dann sendet er den Vertrag an Herrn Müller zurück.

Am nächsten Tag spricht Herr Schmidt mit seiner Bank und diese teilt ihm leider mit, dass eine Finanzierung nicht möglich ist. Herr Schmidt ist sehr betrübt – und nun gezwungen, den am Vortag verbindlich geschlossenen Vertrag wieder zu lösen.

Nun hilft ihm sein Trick mit der Uhr. Herr Schmidt ruft einfach den Herausgeber der Signaturkarte an und sagt, die Karte sei abhanden

gekommen und müsse sofort gesperrt werden. Am nächsten Tag ruft Herr Müller an und möchte die Details der Lieferung und Bezahlung klären. Herr Schmidt erklärt Herrn Müller, dass der Vertrag leider ungültig ist und er nicht gewillt ist, diesen seinerseits zu erfüllen.

Herr Müller ist sehr verärgert, pocht auf seinen Vertrag und prüft zur Sicherheit die Unterschrift von Herrn Schmidt. Die Prüfung ergibt, dass die Unterschrift zu einem Zeitpunkt geleistet wurde, als die Karte bereits gesperrt war. Daher sind die elektronische Unterschrift und der Vertrag ungültig. Herr Müller bleibt nun nur der sehr aufwändige Weg, zu beweisen, dass Herr Schmidt den Vertrag zu einem früheren Zeitpunkt – als in der Signatur ausgewiesen – elektronisch unterschrieben hat.

An dem vorgenannten Beispiel wird deutlich, dass nur eine Kombination aus qualifizierter Signatur und qualifiziertem Zeitstempel solche Vorgänge unabhängig von der eingesetzten IT-Infrastruktur rechtssicher abbilden kann. Durch den qualifizierten Zeitstempel wäre der Zeitpunkt der Signaturerstellung rechtssicher dokumentiert gewesen. Es wäre jederzeit nachweisbar, dass das Zertifikat erst nach der Signaturerstellung zurückgezogen und gesperrt wurde.

Die Signatur allein – ohne Zeitstempel – bietet ohne sofortige Prüfung keine Sicherheit in Bezug auf den Zeitpunkt der Erstellung. Der Zeitstempel ist daher eine wichtige Ergänzung der Signatur.

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.

6.2. Zeitstempel senken Compliance Risiken

Bei Einsatz von qualifizierten Zeitstempeln, auch ohne Signaturen, ergibt sich insgesamt ein anderes Bild.

Auch hier ist die gesamte Beweiskette natürlich nur so stark, wie das schwächste Glied der Kette. Jedoch ist der Einsatz von Zeitstempeln mit und ohne Signaturen für bestimmte Anwendungsbereiche sehr sinnvoll.

Der qualifizierte Zeitstempel dokumentiert gesetzeskonform die Integrität der Daten zu dem Zeitpunkt, als diese dem Zertifizierungsdiensteanbieter vorlagen. Da, wie unter 5.1 erläutert, der qualifizierte Zeitstempel von einem akkreditierten Zertifizierungsdiensteanbieter nicht durch vorsätzliches oder unbeabsichtigtes Fehlverhalten missbraucht werden kann, ist zumindest die Integrität der Daten und der Zeitpunkt, zu dem diese dem Dienst vorgelegen haben, immer rechtssicher dokumentiert.

Hier sei ergänzend angemerkt, dass akkreditierte Zertifizierungsdiensteanbieter sofort bei Erstellung eines qualifizierten Zeitstempels den Zeitstempel, einschließlich des Hash-Wertes, für mindestens 30 Jahre archivieren. Damit ist ein Nachweis auch über einen langen Zeitraum jederzeit möglich.

Die Anwendungsfälle für Zeitstempel sind zahlreich und sehr unterschiedlich. So können anonyme, systembezogene Daten, wie z.B. Log-Files eines SAP-Systems oder eines Krankenhausinformationssystems mit qualifizierten Zeitstempeln rechtsicher versiegelt werden.

In anderen Fällen kann mit Hilfe von qualifizierten Zeitstempeln die Vollständigkeit von Daten, unabhängig von einer personenbezogenen Signatur, beweiskräftig und gesetzeskonform dokumentiert werden (s. Kap. 7.1 Massenbelegerfassung).

Bei wesentlichen Compliance Aspekten, wie z.B. der Nachvollziehbarkeit von elektronischen Transaktionen zu einem bestimmten Zeitpunkt, erweist sich der Einsatz qualifizierter Zeitstempel auch in Kombination mit fortgeschrittenen personenbezogenen Signaturen als durchaus sinnvoll. In der elektronischen Langzeitarchivierung können qualifizierte Zeitstempel auch ohne personenbezogene Signatur die Integrität der Daten über einen langen Zeitraum zweifelsfrei dokumentieren.

Qualifizierte Zeitstempel sind einfach und vollautomatisch einsetzbar. Sie schützen die Integrität der Daten über einen langen Zeitraum und ermöglichen so eine langfristige, sichere, chronologische Nachvollziehbarkeit von Geschäftstransaktionen.

7. Anwendungsszenarien für qualifizierte Zeitstempel

7.1. Rechtssichere Dokumentation des Erfassungszeitpunktes und der Vollständigkeit bei gescannten Dokumenten

Immer mehr Branchen nutzen qualifizierte personenbezogene Signaturen, um den Medienbruch innerhalb eines Scan-Prozesses rechtssicher zu dokumentieren. An jedem Scan-Arbeitsplatz werden hierzu Signaturhard- und -software (Signaturerstellungseinheit und Signaturanwendungskomponente) gemäß Signaturgesetz installiert.

Der Scan-Operator signiert qualifiziert personenbezogen das elektronische Abbild, welches beim Scannen von den Papierbelegen erzeugt wird. Er bestätigt mit seiner personenbezogenen Signatur die Übereinstimmung von Papierbeleg und elektronischem Abbild.

Im Allgemeinen werden die signierten Daten aus dem Scan-Prozess langfristig elektronisch archiviert. Typische Beispiele sind Belege bei Krankenkassen und Patientenakten in Krankenhäusern. Hier bietet sich der Einsatz qualifizierter Zeitstempel als Ergänzung zur Medienbruchbestätigung durch die qualifizierte personenbezogene Signatur an. Der qualifizierte Zeitstempel sichert rechtlich belastbar ab, welche Daten aus dem Scan-Prozess zu einem dedizierten Zeitpunkt vorlagen und archiviert wurden. Ein Zufügen oder Löschen von Daten ist nicht möglich, ohne dass der Zeitstempel zerstört und damit ungültig würde. Der rechtssichere Zeitstempel übernimmt somit eine wichtige Funktion des zeitbezogenen Nachweises der Integrität und Vollständigkeit der Daten unabhängig von der qualifizierten personenbezogenen Signatur.

Von entscheidender Bedeutung ist, dass das rechtssichere „Einfrieren“ der Daten und damit die rechtliche Wirksamkeit unabhängig von vorgelagerten Prozessen, wie hier dem Scannen, erfolgt.

Dies gilt auch dann, wenn der Einsatz der qualifizierten personenbezogenen Signatur am Arbeitsplatz des Scanner-Operators nicht ausdrücklich gesetzlich geregelt ist. So werden z.B. Patientenakten in Krankenhäusern beim Scannen mit qualifizierten personenbezogenen Signaturen versehen, um den Medienbruch zu bestätigen. Dies geschieht in Anlehnung an die Vorschriften für Krankenkassen¹². Gerade hier ist der Einsatz qualifizierter Zeitstempel im Anschluss an den Scan-Prozess sinnvoll.

Durch Verwendung qualifizierter Zeitstempel nach dem Scan-Prozess kann später nicht abgestritten werden, dass diese Daten dem Archiv zugeführt wurden und somit zu einem dedizierten Zeitpunkt vollständig und mit bestimmtem Inhalt vorgelegen haben. Umgekehrt können Daten, z.B. zusätzliche Patientenakten, zu einem späteren Zeitpunkt nicht unbemerkt hinzugefügt werden, um Patientendaten zu manipulieren.

Das Beispiel illustriert den nachweisbaren Gewinn an Sicherheit durch die Kombination aus qualifizierten Zeitstempeln mit (qualifizierten) personenbezogenen Signaturen. So wird auch für elektronische Prozesse, für die keine individuelle, dedizierte gesetzliche Regelung besteht, eine lückenlose Nachvollziehbarkeit bereitgestellt.

Selbstverständlich gilt auch in diesen Fällen, dass die Anzahl der qualifizierten Zeitstempel durch geeignetes Prozessdesign, z.B. Gruppenbildung („Batch“) deutlich reduziert werden kann. Damit ist jederzeit eine wirtschaftlich attraktive Lösung gewährleistet.

¹² S. Kap. 3.1 Anforderungen Massenbelegerfassung im Sozialversicherungsbereich

7.2. Nach- oder Übersignieren

Qualifizierte Signaturen und Zeitstempel sind Instrumente zur kurz-, mittel- und langfristigen Sicherung elektronischer Daten. Aufgrund des technologischen Fortschritts müssen Technologien, mit denen qualifizierte Signaturen und Zeitstempel erzeugt werden, kontinuierlich überwacht und ggf. Sicherheitsanforderungen erhöht werden. Aus diesem Grund nimmt das BSI (Bundesamt für Sicherheit in der Informationstechnik) jährlich eine Bewertung der kryptographischen Algorithmen und Schlüssellängen vor. Hieraus resultiert eine Empfehlung für Algorithmen und Schlüssellängen mit zeitlichen Gültigkeitsprognosen. Die Bundesnetzagentur greift diese Empfehlung auf und veröffentlicht auf dieser basierend eine Übersicht zu den geeigneten Algorithmen, Schlüssellängen und deren Gültigkeitszeiträume. So waren bis zum 31. 12.2007 der Algorithmus SHA1 und die Schlüssellänge RSA1024 gültig und für qualifizierte Signaturen und Zeitstempel zugelassen. Aktuell sind u.a. der Algorithmus SHA256 und die Schlüssellänge RSA2048 als gültig und sicher eingestuft.

Diese Algorithmen und Schlüssellängen sind zu verwenden, um gesetzeskonforme qualifizierte Signaturen und Zeitstempel gemäß deutschem Signaturgesetz zu erstellen.

Soweit Algorithmen und/oder Schlüssellängen nicht mehr als ausreichend sicher eingestuft werden, ist es erforderlich, Daten, die bereits signiert wurden, nach- oder überzusignieren. Gemäß Signaturverordnung¹³ müssen hierzu qualifizierte Zeitstempel verwendet werden. Abb. 1 zeigt exemplarisch auf, welche Fälschungsmöglichkeiten durch schwachwerden des Hash-Algorithmus bzw. der Schlüssellänge bestehen. Diese Fälschungsmöglichkeiten werden durch das Nachsignieren mittels qualifizierter Zeitstempel eliminiert.

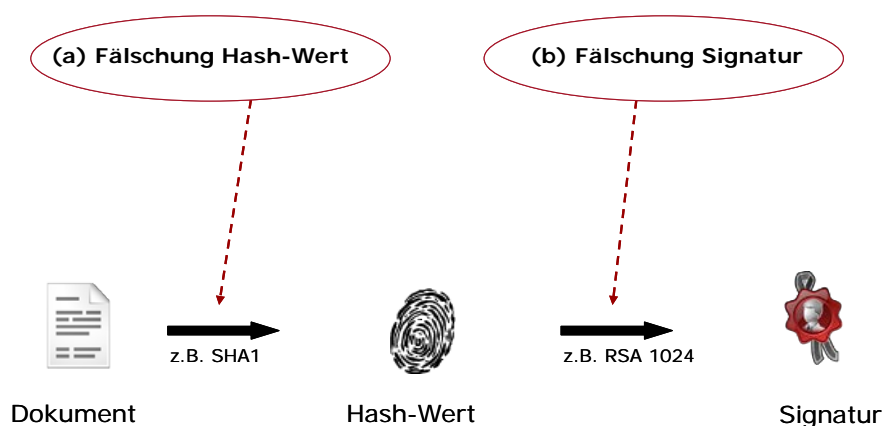


Abb. 1 – Exemplarische Darstellung: Fälschungsmöglichkeiten bei schwachwerden von Hash-Algorithmus und Schlüssellänge

¹³ s. § 17 SigV

Welche Daten nachsigniert werden müssen und welches Verfahren angewendet werden kann, richtet sich danach, ob nur die Schlüssellängen unsicher werden oder ob Schlüssellängen und Hash-Algorithmus zugleich unsicher werden.

In der Vergangenheit haben sich unterschiedliche Verfahren zum Nachsignieren entwickelt. Die Wahl des Verfahrens richtet sich, neben der gesetzlichen Anforderung, häufig nach den Vorgaben des beim Anwender genutzten Archivsystems.

Bei der Beurteilung der unterschiedlichen Verfahren ist, neben dem wirtschaftlichen Aspekt, auch im Wesentlichen die technische Implementierung zu berücksichtigen. So ist es unbedingt erforderlich, dass ein Verfahren zum Nachsignieren nicht nur die Schlüssellänge (RSA1024, RSA2048), sondern auch den Hash Algorithmus (SHA1, SHA256, SHA512) schützt. Von Verfahren, die nur einen Aspekt berücksichtigen, ist daher abzuraten. Der zukünftige Aufwand des Nachsignierens kann bei solchen Lösungen schnell unkalkulierbar werden.

Beispielhaft ist in der Abb. 2 ein Verfahren skizziert, in dem der Beweiswert von signierten Daten, sowohl bei Änderung des Hash-Algorithmus, als auch der Schlüssellänge, durch Nachsignieren mit einem qualifizierten Zeitstempel aus einem akkreditierten Trust Center gesetzeskonform erhalten wird.

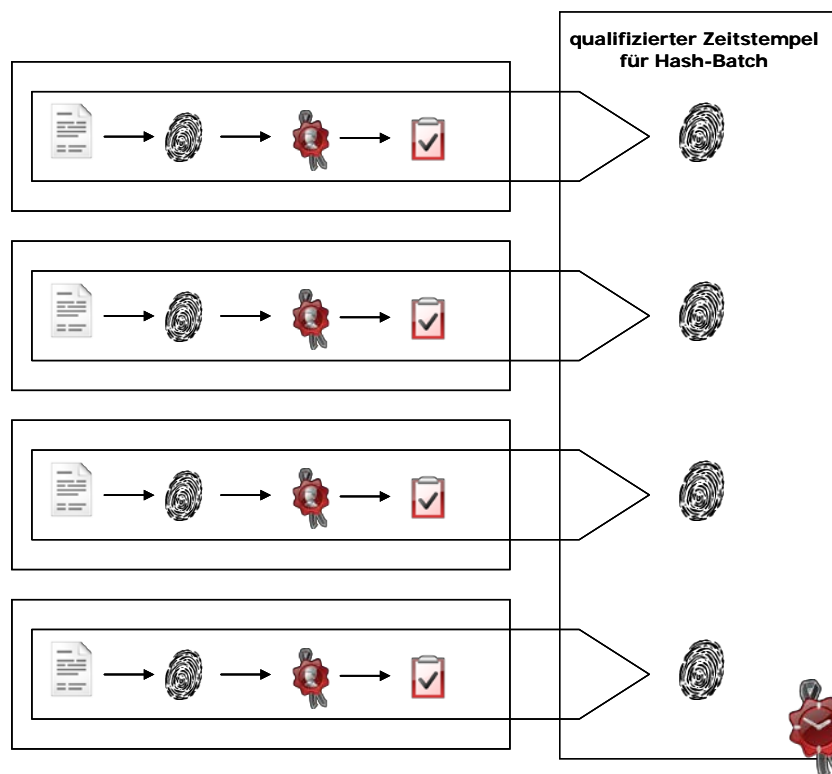


Abb. 2 - Exemplarische Darstellung des Nachsignierens im Batch-Verfahren

Durch Gruppen bzw. Batch-Bildung kann gleichzeitig die Anzahl benötigter qualifizierter Zeitstempel wesentlich minimiert werden.

Derartige Verfahren wurden bereits Ende 2007 beim Wechsel des Hash-Algorithmus¹ und der Schlüssellängenänderung erfolgreich in der Praxis angewendet. Der Beweiswert von vielen Millionen signierten Datensätzen wurde auf diese Weise mit vergleichsweise wenigen qualifizierten Zeitstempeln sehr effizient gesichert.

8. Internationale Aspekte

Kaum ein Geschäftsprozess kann in der heutigen Zeit ausschließlich national abgewickelt werden. So ist es unabdingbar, auch elektronische Geschäftsprozesse an international anerkannten Rahmenbedingungen zu orientieren.

Das deutsche Signaturgesetz in der Fassung vom Mai 2001 hat die internationalen Rahmenbedingungen der EU-Signaturrechtlinie (2001/115/EG) vom Dezember 1999 in nationales Recht umgesetzt. Qualifizierte Signaturen und Zeitstempel, die den strengen Anforderungen des deutschen Signaturgesetzes entsprechen, erfüllen somit auch die Anforderungen der EU-Signaturrechtlinie. Elektronisch signierte, bzw. zeitgestempelte Daten können daher auch im internationalen Umfeld als Beweismittel herangezogen werden.

Für das nicht-EU Ausland, z.B. Schweiz, gelten gesonderte Regelungen, die jedoch vielfach mit den in Deutschland verfügbaren Technologien umgesetzt werden können. Gleiches gilt für den US-amerikanischen Raum. Hier wurden durch den ESIGN Act und die Rahmenbedingungen der American Bar Association (ABA) die notwendigen Grundlagen für Signaturen und Zeitstempel geschaffen.

9. Über AuthentiDate

AuthentiDate International AG

(mit Sitz in Deutschland, Düsseldorf) wurde am 9. November 2001 als erstes Unternehmen mit Schwerpunkt qualifizierte Zeitstempel von der Bundesnetzagentur (früher Regulierungsbehörde für Telekommunikation und Post) als akkreditierter Zertifizierungsanbieter nach neuem deutschem Signaturgesetz und europäischen Richtlinien akkreditiert. Damit bieten die von AuthentiDate International AG gelieferten Zeitstempel für alle elektronischen Daten den gesetzlich anerkannten höchsten Schutz in Form von qualifizierten elektronischen Signaturen mit Anbieterakkreditierung.



High Security
Signaturgesetz

regtp Z 0 0 1 5

Qualifizierte Zeitstempel der AuthentiDate International AG entsprechen auch den Anforderungen der EU-Signaturrechtlinie. Sie können somit auch international für rechtssichere elektronische Prozesse verwendet werden.

Die **AuthentiDate Deutschland GmbH**, eine 100%ige Tochter der AuthentiDate International AG, liefert und entwickelt eigenständig herstellerunabhängige Softwarelösungen zur Integration von Zeitstempeln und personenbezogenen Signaturen in Geschäftsprozesse aller Art. Hierbei können sowohl qualifizierte als auch fortgeschrittene Signaturen und Zeitstempel genutzt werden.

International führend

AuthentiDate Produkte sind bei mittelständischen Unternehmen und Konzernen nahezu jeder Branche im Einsatz. Alle Technologien sind auch als Dienstleistung verfügbar. So können Signatur- und Zeitstempelleistungen auf Wunsch komplett outsourced werden.

AuthentiDate hat seine Expertise im Bereich qualifizierter Zeitstempel auch im Aufbau von Zeitstempeldiensten außerhalb der EU eingebracht; so wurde ein in der Schweiz akkreditierter Zeitstempeldienst mit AuthentiDate Produkten aufgebaut und realisiert.

Erfinder der Massensignatur

AuthentiDate ist der Erfinder der zentralen, qualifizierten Massensignatur und hat diese Lösung international, zum Beispiel im Rahmen der elektronischen Rechnungsstellung, etabliert.

Als Pionier im Signaturmarkt hat das Unternehmen den ersten weltweit verfügbaren Dienst zur Prüfung von Signaturen aufgebaut. Dieser kann mehrsprachig, anwenderfreundlich und ohne zusätzliche Software rund um die Uhr and 365 Tagen überall auf der Erde genutzt werden.

Über die Hälfte der gesetzlichen Krankenkassen in Deutschland nutzen AuthentiDate Signaturlösungen, um zahlungsrelevante Belege zu digitalisieren und zu archivieren. Fast alle marktgängigen DMS-, Archiv- und Scananbieter haben die AuthentiDate Signaturprodukte standardmäßig integriert.

Weltweit einzigartig & gesetzeskonform

Alle AuthentiDate Signaturprodukte erfüllen die strengen Anforderungen des deutschen Signaturgesetzes, der EU-Signaturrechtlinie und US-amerikanische Richtlinien.

Die AuthentiDate Signaturtechnologie ist weltweit einzigartig. Die durchgängig vom Betriebssystem unabhängige, gesetzeskonforme, zukunftsweisende SOA (Software Oriented Architecture) und SaaS (Software as a Service) Architektur ermöglicht erstmals verteilte Client-Server Signaturprozesse. Die flexible JAVA Architektur ermöglicht die Abbildung aller aktuellen und zukünftigen Karten und Standards, wie eCard API des BSI, eHealth/eGK Formate und Prozesse, ERS und Langzeitarchivierung.

AuthentiDate ist der Spezialist für:

- qualifizierte & fortgeschrittene Signaturen
- qualifizierte & sonstige Zeitstempel
- Organisationszertifikate
- Einfach-, Komfort-, Stapel- & Massensignaturen
- Signatur Client-Komponenten
- Webservices (Software as a Service)
- Zertifizierte Signaturprodukte
- Signaturprodukte für Dienstleister & Systemanbieter

Weitere Informationen unter www.authentidate.de

10. Abkürzungsverzeichnis

Abb.	-	Abbildung
AG	-	Aktiengesellschaft
BNetzA	-	Bundesnetzagentur
EU	-	Europäisch
GmbH	-	Gesellschaft mit beschränkter Haftung
SAK	-	Signaturanwendungskomponente
SSEE	-	sichere Signaturerstellungseinheit
SigG	-	Signaturgesetz
SigV	-	Signaturverordnung
Tab.	-	Tabelle
z.B.	-	zum Beispiel
ZDA	-	Zertifizierungsdiensteanbieter
ZS	-	Zeitstempel

11. Glossar

Akkreditierung

In Verbindung mit dem Signaturgesetz verwendeter Begriff zur näheren Beschreibung eines Zertifizierungsdiensteanbieters, der nach den Auflagen von Signaturgesetz, Signaturverordnung und entsprechender Prüfung durch die Bundesnetzagentur (BNetzA) seinen Dienst betreibt. (s. auch „Zertifizierungsdiensteanbieter“)

Authentizität

Unter dem Nachweis der Authentizität von elektronischen Daten versteht man den Nachweis über die Echtheit der Daten (s. auch „Integrität“) und die eindeutige Zuordnung zum Verfasser, Ersteller und/oder Absender.

Batch

Zusammenführung und zusammengefasste Verarbeitung mehrerer Datensätze.

Client

Rechner an einem Einzelarbeitsplatz, der auf Software und Daten zugreifen kann, die zentral an anderer Stelle des Unternehmens im Zugriff liegen (z.B. auf einen zentralen Server, Archivsysteme etc.).

Common PKI

Common PKI ist eine gemeinsame Spezifikation von dem Verein TeleTrust und der T7-Gruppe für elektronische Signaturen, Verschlüsselung und PKI. Wesentliches Ziel ist es, durch Common PKI die Voraussetzung für eine internationale Standardisierung und Interoperabilität für Anwendungen auf den genannten Gebieten zu schaffen. Bis vor kurzer Zeit wurde Common PKI als ISIS-MTT bezeichnet.

CRL

Abk. für den englischen Begriff: Certificate Revocation List
Liste, die durch den „Zertifizierungsdiensteanbieter“ erstellt und veröffentlicht wird und die beinhaltet, welche Zertifikate durch den Zertifikatsinhaber gesperrt („revoziert“) worden sind.

Elektronische Signatur

Im allgemeinen Sprachgebrauch häufig auch als „digitale Signatur“ bezeichnet. Bezeichnung aus dem Deutschen Signaturgesetz und der EU-Signaturrichtlinie. Eine elektronische Signatur ist vergleichbar mit einer elektronischen Unterschrift. Sie wird durch die Verwendung von „privaten Schlüsseln“ erzeugt. Der Vorgang zur Erzeugung einer elektronischen Signatur kann vereinfacht wie folgt dargestellt werden: Mittels eines bestimmten mathematischen Algorithmus wird aus den Daten, die signiert werden sollen, ein „HASH-Wert“ ermittelt. Dieser „HASH-Wert“ wird mit dem „privaten Schlüssel“ verschlüsselt. Der korrespondierende „öffentliche Schlüssel“ wird in Form eines „Zertifikats“ ausgegeben, welches zudem Informationen über den Urheber der Signatur enthält. Die „Verschlüsselung“ des „HASH-Wertes“ in Verbindung mit dem entsprechenden Zertifikat wird als elektronische Signatur bezeichnet. Alle diese Vorgänge laufen automatisch durch entsprechende Softwareprogramme ab.
s. auch „fortgeschrittene Signatur“ und „qualifizierte Signatur“

Entschlüsselung

Vorgang, bei dem unter Verwendung mathematischer Algorithmen und „privater Schlüssel“ elektronische Daten wieder les- bzw. verarbeitbar gemacht werden. In verschlüsselter Form sind die Daten weder von unbefugten Dritten einsehbar noch veränderbar, die Daten können nur vom Besitzer des entsprechenden „privaten Schlüssels“ wieder in die Originalform überführt werden.

Fingerabdruck

Häufig verwendet als Synonym für „Hash-Wert“.

Fortgeschrittene Signatur

Eine „fortgeschrittene Signatur“ ist eine Signatur, die mit Hilfe von „fortgeschrittenen Zertifikaten“ erstellt wird. Daten, die fortgeschritten signiert wurden, haben - im Gegensatz zu Daten die qualifiziert signiert wurden - keine Rechtssicherheit.

Geheimer Schlüssel

s. „Privater Schlüssel“

Hash-Wert

Mathematischer Wert (Prüfsumme), der durch Anwendung einer Rechenoperation (mathematischer Algorithmus) von einer elektronischen Datei erzeugt wird. Ein Hash-Wert bildet eine eindeutige Verknüpfung zum ursprünglichen elektronischen Original ab. Zudem kann von einem Hash-Wert die zugrunde liegende Datei nicht wieder rekonstruiert werden. Im Allgemeinen werden hierfür die von der Bundesnetzagentur (BNetzA) zugelassenen und als sicher eingestuft Hash-Algorithmen verwendet (z.B. SHA-512, RSA 2048)

HSM

Abk. für den englischen Begriff: Hardware-Security-Module

Ein HSM ist eine Hardware, die es ermöglicht, kryptographische Schlüssel in besonders sicherer Form aufzubewahren. Daneben ermöglicht die Hardware auch die Verwendung in komplexeren Anwendungen, z.B. als Server. Ein HSM ist vergleichbar mit einer überdimensionalen Smart Card, die neben der Aufbewahrung der privaten und öffentlichen Schlüssel auch andere Funktionen übernehmen kann.

Integrität

Unter dem Nachweis der Integrität elektronischer Daten versteht man den Nachweis, dass diese vollständig und unverändert sind.

ISIS-MTT

Frühere Bezeichnung für Common PKI. s. Common PKI.

JAVA

Programmiersprache, die hohe Flexibilität und Interoperabilität ermöglicht. Mit Hilfe von JAVA können z.B. Anwendungen entwickelt werden, die durch die Verwendung einer virtuellen Maschine unabhängig vom Betriebssystem und Internetbrowser lauffähig sind.

Öffentlicher Schlüssel

Teil eines kryptographischen Schlüsselpaares, der öffentlich bekannt und frei zugänglich ist. Der öffentliche Schlüssel wird auch verwendet, um Daten zu verschlüsseln und an eine bestimmte Person in verschlüsselter Form weiterzuleiten. Nur diese Person kann im Anschluss mit dem zugehörigen nur ihr bekannten „privaten Schlüssel“ die Daten wieder entschlüsseln.

s. auch „privater Schlüssel“

OCSP-Abfrage

OCSP ist die Abk. für den englischen Begriff: Online Certificate Status Protocol

Möglichkeit zur Abfrage des Status von Zertifikaten. Mittels dieser Online Abfrage kann z.B. geprüft werden, ob ein Zertifikat durch den Benutzer gesperrt worden oder abgelaufen ist.

PGP

Abk. für den englischen Begriff: Pretty Good Privacy

Programm zur Verschlüsselung/Signatur von Daten mittels „öffentlicher“ und „privater Schlüssel“ auf Basis eines „Web of Trust“, d.h. gegenseitiger Empfehlung der Vertrauenswürdigkeit eines Teilnehmers. PGP Zertifikate werden daher nicht durch akkreditierte Zertifizierungsdiensteanbieter ausgegeben und beinhalten folglich keine Möglichkeit, rechtssichere Signaturen gemäß Deutschem Signaturgesetz zu erzeugen.

PKCS

Abk. für den englischen Begriff: Public Key Cryptography Standards

Bezeichnung für verschiedene Industriestandards (wie z.B. PKCS#6, PKCS#7 etc.), die sich am allgemeinen Markt stark etabliert haben.

PKI

Abk. für den englischen Begriff: Public Key Infrastructure

Technische Infrastruktur, die es ermöglicht asymmetrische kryptographische Technologien im Unternehmen auszurollen und zu betreiben. Hierbei kommen die entsprechenden kryptographischen Schlüssel (s. auch „privater Schlüssel“ und „öffentlicher Schlüssel“) zum Einsatz. PKI Lösungen umfassen typischerweise Komponenten zur Beantragung, Erzeugung, Verwaltung und zum Ausrollen resp. Betrieb von zertifikatsbasierten Infrastrukturen auf Basis asymmetrischer Schlüssel. Anwendungsfelder für PKI basierte Lösungen sind die „elektronische Signatur“ und „Ver-/Entschlüsselung“ von elektronischen Dokumenten.

Privater Schlüssel

Teil eines kryptographischen Schlüsselpaares, der nur demjenigen bekannt ist bzw. in dessen Zugriff ist, der eine Signatur erzeugt und somit elektronische Daten elektronisch unterschreibt. Der private Schlüssel wird auch verwendet, um verschlüsselte Daten, die nur einer bestimmten Person zugänglich gemacht werden sollen, von dieser Person zu entschlüsseln.

s. auch „öffentlicher Schlüssel“

Qualifizierte Signatur

Eine qualifizierte Signatur ist eine „elektronische Signatur“, die auf Basis eines qualifizierten „Zertifikats“ erstellt wird. Stammt das qualifizierte „Zertifikat“ von einem akkreditierten „Zertifizierungsdiensteanbieter“ und wird für die Erstellung einer sicheren „Signaturerstellungseinheit“ verwendet, so können mittels der qualifizierten Signatur elektronische Daten rechtssicher unterschrieben werden.

s. auch „fortgeschrittene Signatur“

Signatur

s. „elektronische Signatur“

Signaturanwendungskomponente

Zur Erstellung einer qualifizierten Signatur ist eine geeignete Signatursoftware erforderlich. Diese wird als Signaturanwendungskomponente (SAK) bezeichnet. Damit die qualifizierte Signatur rechtssicher und damit der handschriftlichen Unterschrift gleichgestellt ist, muss die SAK den Anforderungen des Signaturgesetzes bzw. der Signaturverordnung genügen. Ein solcher Nachweis über die Qualität der SAK kann z.B. erbracht werden, indem die SAK nach Signaturgesetz bestätigt wird (SigG-Bestätigung).

Signaturerstellungseinheit

Ebenso wie eine Signatursoftware, ist auch geeignete Hardware zur Erstellung gesetzekonformer, qualifizierter Signaturen erforderlich. D.h. sowohl die Signaturkarte (Smart Card), als auch der eingesetzte Kartenleser muss den Anforderungen des Signaturgesetzes und der Signaturverordnung entsprechen. Auch dies kann durch eine entsprechende Bestätigung nach Signaturgesetz (SigG-Bestätigung) nachgewiesen werden.

Signaturprüfung

Die Signaturprüfung umfasst zwei verschiedene Prüfverfahren bzw. Prüfungsarten. Die sind die mathematische Prüfung („Integrität“) und die Prüfung des Zertifikats („Authentizität“ und Gültigkeit). Bei der mathematischen Prüfung wird durch entsprechende Software geprüft,

ob der Hash-Wert, des signierten Dokumentes mit dem Hash-Wert der zugehörigen Signatur zum Dokument übereinstimmt und somit das signierte Dokument nach Erzeugung der Signatur nicht modifiziert worden ist. Bei der Prüfung des Zertifikats wird ebenfalls durch entsprechende Software ermittelt, ob das Zertifikat zum Zeitpunkt der Signaturerstellung gültig war und zudem die Güte der Signatur („fortgeschritten“, „qualifiziert“) bestimmt.

Smart Card

„Signaturerstellungseinheit“, die dazu dient, Zertifikate sicher in Form einer Chipkarte aufzubewahren.

SSL

Abk. für den englischen Begriff: Secure Sockets Layer

Möglichkeit, über ein bestimmtes Übertragungsprotokoll durch Austausch von Zertifikaten sicher, verschlüsselt über das Internet zu kommunizieren. Häufig genutzt in der Kommunikation eines Einzelplatzrechners über das Internet mit einem Server, z.B. bei Bankgeschäften.

Trust Center

In Verbindung mit dem Signaturgesetz bezeichnet der Begriff Trust Center eine vertrauenswürdige Instanz, die in der Regel gemäß den strengen Auflagen des Signaturgesetzes und der Signaturverordnung Dienste anbietet, wie z.B. Ausgabe von Zertifikaten, Ausstellung von qualifizierten Zeitstempeln, Auskünfte über den Status von Zertifikaten.

Verschlüsselung

Technisches Verfahren unter Verwendung von „öffentlichen“ und „privaten Schlüsseln“ zum Schutz von elektronischen Daten. Die Daten werden durch die Verschlüsselung vor unbefugter Einsicht und Zugriff Dritter geschützt.

(s. auch „PKI“)

X.509

Standardformat für Zertifikate auf Basis asymmetrischer kryptographischer Verfahren.

Zeitstempel

„Sonderform“ der elektronischen Signatur. Elektronische Bescheinigung darüber, dass die mit dem Zeitstempel signierten Daten zum Zeitpunkt der Signatur in der signierten Form vorgelegen haben. Der Zeitstempel gemäß Signaturgesetz friert die Daten rechtssicher ein.

Zertifikat

Man unterscheidet zwischen Software basierenden Zertifikaten und Hardware basierenden Zertifikaten.

Wird ein Zertifikat als Software Zertifikat ausgegeben, so werden die privaten und öffentlichen Schlüssel direkt als Software auf einem Rechner installiert. Signaturen, die mit Software basierenden Zertifikaten ausgestellt werden, können keine rechtssicheren elektronischen Daten erzeugen.

Wird ein Zertifikat als Hardware basierendes Zertifikat ausgegeben, so werden die benötigten Schlüssel auf einer Hardware, z.B. in Form einer Smart Card, bereitgestellt. Werden die Zertifikate bzw. die Smart Card von einem akkreditierten „Zertifizierungsdienst“ ausgegeben, so können mit Hilfe der auf ihr enthaltenen qualifizierten Zertifikate auch „qualifizierte Signaturen“ erstellt werden. Somit können durch diese Zertifikate auch rechtssichere elektronische Daten erzeugt werden.

Zertifizierungsdiensteanbieter

Anbieter, der einen Dienst gemäß Deutschem Signaturgesetz (und Signaturverordnung) und EU-Signaturrichtlinie betreibt. Es werden Dienste, wie z.B. Ausgabe von Zertifikaten, Ausstellung qualifizierter Zeitstempel, Auskünfte über den Status von Zertifikaten angeboten.

12. Legal Disclaimer

Das vorliegende White Paper enthält ausschließlich unverbindliche technische und rechtliche Informationen. Irrtümer bleiben vorbehalten. Verbindliche technische Aussagen zu den einzelnen Produkten, die in diesem Dokument genannt werden, sind ausschließlich den jeweiligen Produktspezifikationen zu entnehmen.

AuthentiDate haftet nicht für die Aktualität, Korrektheit, Vollständigkeit oder Qualität, der in diesem Dokument enthaltenen Informationen. Haftungsansprüche, welche sich auf Schäden materieller oder ideeller Art beziehen, die durch die Nutzung oder Nichtnutzung der hier dargebotenen Informationen bzw. durch die Nutzung fehlerhafter und unvollständiger Informationen verursacht werden, sind grundsätzlich ausgeschlossen.

Rechtliche Aussagen sind in keinem Fall verbindlich. Im Fall von Abweichungen zu, mit diesem Dokument in Zusammenhang stehenden Vertragsdokumenten oder allgemeinen Geschäftsbedingungen der AuthentiDate, gehen die Vertragsdokumente bzw. allgemeinen Geschäftsbedingungen der AuthentiDate diesem Dokument stets vor.