

Aspekte der „Massensignatur“

Detlef Hühnlein¹ · Yvonne Knosowski²

secunet Security Networks AG

¹Sudetenstraße 16, 96247 Michelau

²Weidenauerstraße 223–225, 57076 Siegen

{detlef.huehnlein, yvonne.knosowski}@secunet.com

Zusammenfassung

Diese Arbeit beleuchtet einige Aspekte der automatisierten Erzeugung qualifizierter elektronischer Signaturen. Anhand von zwei Beispielen – der elektronischen Rechnungsstellung gemäß §14 UStG und der elektronischen Archivierung schriftlicher Unterlagen gemäß §36 SRVwV – werden neben den rechtlichen Rahmenbedingungen insbesondere auch technische und organisatorische Fragen der Realisierung hoch performanter Signatursysteme gemäß Signaturgesetz näher beleuchtet.

1 Einleitung

Die elektronische Abwicklung von Geschäftsprozessen in Wirtschaft und Verwaltung verspricht immense Einsparungspotenziale.

Beispielsweise bescheinigt eine Studie im Auftrag der EU-Kommission [EU-EBP] der elektronischen Rechnungsstellung ein Einsparungspotenzial von 70%. Da Unternehmen natürlich auch (ausschließlich) elektronisch erhaltene Rechnungen beim Vorsteuerabzug geltend machen möchten, müssen diese nach §14, Abs. 4, Satz 2 [UStG02] mit qualifizierten elektronischen Signaturen gemäß Signaturgesetz [SigG] versehen sein.

In ähnlicher Art und Weise verspricht die papierlose Abwicklung des Rechnungswesens in der Sozialversicherung immense Einsparungen. In diesem Zusammenhang ist §36 [SRVwV] (Aufbewahrung von zahlungsbegründenden Unterlagen) von besonderer Bedeutung, da papiergebundene Unterlagen eingescannt und vernichtet werden dürfen, sofern die Übereinstimmung des elektronischen Abbildes mit dem Original durch eine qualifizierte elektronische Signatur bestätigt wird.

In beiden Fällen steht ein sehr großes Einsparungspotenzial möglicherweise hohen Prozesskosten für den manuellen Einsatz qualifizierter elektronischer Signaturen gegenüber. Müsste für die Erzeugung jeder einzelnen Signatur von einem Operator eine PIN eingegeben werden, so würde dieser erhöhte Personalbedarf die möglichen Einsparungen in den Prozesskosten drastisch reduzieren oder gar zunichte machen. Deshalb ist die „Massensignatur“ – d.h. die automatisierte Erzeugung dieser qualifizierten elektronischen Signaturen - für diese Anwendungen von entscheidender Bedeutung.

Aus diesem Grund widmet sich dieser Beitrag verschiedenen rechtlichen, organisatorischen und technischen Aspekten der „Massensignatur“. So beleuchtet Abschnitt 2.1 die rechtlichen Rahmenbedingungen aus der Signaturgesetzgebung und Abschnitt 2.2 weitere relevante Ge-

setze für die oben angesprochenen Anwendungen. Abschnitt 3 widmet sich schließlich organisatorischen und technischen Aspekten, die beim Aufbau hoch performanter und gleichsam sicherer Signatursysteme Beachtung finden sollten.

2 Rechtliche Rahmenbedingungen

In diesem Abschnitt werden die rechtlichen Rahmenbedingungen für den Einsatz der Massensignatur in den oben skizzierten Anwendungsfällen zusammengetragen. Hierbei werden neben der Signaturgesetzgebung (Abschnitt 2.1) auch die entsprechenden Anwendungsgesetze (Abschnitt 2.2) betrachtet.

2.1 Signaturgesetzgebung

In diesem Abschnitt werden die rechtlichen Rahmenbedingungen der „Massensignatur“ näher beleuchtet. Insbesondere soll der Frage nachgegangen werden, welche technischen und organisatorischen Anforderungen, wie z. B. möglicherweise nötige Prüfungen und Bestätigungen, mit der automatischen Signaturerzeugung verbunden sind.

2.1.1 Die „Massensignatur“ in der Begründung zu §15 Abs. 2 SigV

Das Signaturgesetz [SigG] benennt die automatisierte Signaturerstellung nicht explizit, verbietet sie aber auch nicht. Dies liegt hauptsächlich daran, dass das Signaturgesetz nur Belange eines Zertifizierungsdiensteanbieters (ZDA) regelt, nicht aber die Art und Weise der Nutzung des Signaturschlüssels durch den Signaturschlüssel-Inhaber.

Die Begründung zur Signaturverordnung [SigVBeg] nimmt jedoch im Zusammenhang mit §15 Abs. 2 SigV Bezug auf die automatisierte Signaturerstellung:

*„Insbesondere bei der automatischen Erzeugung von Signaturen ("Massensignaturen") muss sichergestellt sein, dass Signaturen nur zu dem voreingestellten Zweck (z. B. Signaturen zu Zahlungsanweisungen bei Großanwendern) und durch eine zuvor **geprüfte und abgenommene Anwendung** vorgenommen werden können.“*

§15 Abs. 2 SigV sowie dessen Begründung gibt sicherheitstechnische Hinweise, die dazu dienen, dass eine Signatur nur durch die berechtigte Person erzeugt werden kann und nur über die Daten erzeugt wird, welche diese Person signieren will. Es handelt sich also um Maßnahmen, die den Signaturschlüssel-Inhaber vor dem Missbrauch seines Signaturschlüssels schützen sollen.

Welche Art von Prüfung und Abnahme in der Begründung gemeint ist, bleibt an dieser Stelle unklar. Einzelne Betrachtungen befinden sich im folgenden Abschnitt.

2.1.2 Bezieht sich „geprüft und abgenommen“ auf „geprüft und bestätigt“ gemäß §15 Abs. 7 SigG?

Die Formulierung „geprüfte und abgenommene Anwendung“ könnte vermuten lassen, dass hier auf §15 Abs. 7 SigG Bezug genommen wird, wonach bei der freiwilligen Akkreditierung eines Zertifizierungsdiensteanbieters Produkte für qualifizierte elektronische Signaturen und damit insbesondere Signaturanwendungskomponenten „geprüft und durch eine Stelle nach §18 bestätigt“ worden sein müssen.

Dies scheint jedoch im Widerspruch zu §17 Abs. 2 SigG zu stehen. Bzgl. der Eigenschaften¹ für die Darstellung zu signierender Daten durch eine Signaturanwendungskomponente besagt §17 Abs. 2 SigG letzter Satz:

*„Die Signaturschlüssel-Inhaber **sollen** solche Signaturanwendungskomponenten einsetzen oder andere geeignete Maßnahmen zur Sicherheit qualifizierter elektronischer Signaturen treffen.“*

Die Begründung des Regierungsentwurfs (siehe [BrTe01]) macht deutlich, dass die Nutzung *„geeigneter Signaturanwendungskomponenten in das Ermessen der Signaturschlüssel-Inhaber gestellt bleibt“* und sagt zu der Formulierung *„soll“*, dass damit klargestellt wird, dass *„die Verwendung von geeigneten Signaturanwendungskomponenten **nicht** Voraussetzung für die Erzeugung einer qualifizierten elektronischen Signatur ist“*. Einer Signatur (auch einer qualifizierten elektronischen) ist es nach deren Erzeugung ohnehin nicht mehr anzusehen, ob sie mit einer „solchen“ Anwendungen erstellt wurde, oder mit einer anderen (siehe dazu auch [BoEi02] und [BrTe01]).

Analog liegt es auch im Ermessen eines Signaturschlüssel-Inhabers eine nach dem Signaturgesetz geprüfte und bestätigte Anwendung zur Erzeugung einer qualifizierten elektronischen Signatur zu verwenden.

Weiterhin sind Akkreditierte Zertifizierungsdiensteanbieter nach §15 Abs. 7 Nr. 3 SigG verpflichtet, *„die Signaturschlüssel-Inhaber im Rahmen des § 6 Abs. 1 über nach Satz 1 geprüfte und bestätigte Signaturanwendungskomponenten zu unterrichten.“*

Es muss also der akkreditierte Zertifizierungsdiensteanbieter dem Signaturschlüssel-Inhaber eine Liste der geprüften und bestätigten Signaturanwendungskomponenten liefern. Die derzeit am Markt befindlichen Anbieter liefern mit der sicheren Signaturerstellungseinheit (Signaturkarte) meist auch eine solche aus. Aber auch das bedeutet nicht, dass der unterrichtete Anwender - als Kunde eines akkreditierten Zertifizierungsdiensteanbieters - verpflichtet wäre, diese geprüften und bestätigten Anwendungen auch tatsächlich einzusetzen.

Da also keine Verpflichtung zur Nutzung bestimmter (z. B. geprüfter und bestätigter) Anwendungen besteht, ist die Formulierung in der Begründung nach der Nutzung einer geprüften und abgenommenen Anwendung vermutlich derart zu verstehen, dass sich eine Organisation, welche Techniken zur Erzeugung von Massensignaturen einsetzt, durch eine (möglicherweise selbst definierte) Überprüfung und Abnahme davon überzeugen soll bzw. sicherstellen soll, dass die eingesetzte Anwendung nur solche Daten signiert, die sie auch signieren soll. Es sollen eben nur korrekt arbeitende Anwendungen eingesetzt werden und bei der massenhaften Erzeugung von Signaturen den höheren Gefahren Rechnung getragen werden. Diese Aspekte werden in Abschnitt 3 näher betrachtet.

2.1.3 Besteht eine Pflicht zur Prüfung auch bei Produkten mit Herstellererklärung?

Im Zusammenhang mit Anwendungen, welche zur Signaturerstellung genutzt werden, taucht in aktuellen Diskussionen auch oft die in §17 Abs. 4 SigG genannte Erklärung durch den Her-

¹ „Für die Darstellung zu signierender Daten sind Signaturanwendungskomponenten erforderlich, die die Erzeugung einer qualifizierten elektronischen Signatur vorher eindeutig anzeigen und feststellen lassen, auf welche Daten sich die Signatur bezieht.“ Und: „Signaturanwendungskomponenten müssen nach Bedarf auch den Inhalt der zu signierenden [...] Daten hinreichend erkennen lassen.“

steller des Produktes (im Folgenden mit Herstellererklärung bezeichnet) auf. Diese Herstellererklärung müssen nicht-akkreditierte Zertifizierungsdiensteanbieter, welche aber qualifizierte Zertifikate ausstellen (im Folgenden mit angezeigte Zertifizierungsdiensteanbieter bezeichnet), für bestimmte ihrer eingesetzten Produkte für qualifizierte elektronische Signaturen besitzen.

Ist ein Produkt (z. B. eine Signaturanwendungskomponente) mit einer solchen Herstellererklärung ausgestattet, dann besagt die von der Regulierungsbehörde für Telekommunikation und Post (RegTP) auf ihrer Webseite zur Verfügung gestellten Erläuterung [RegTP-HE]:

*„Die Herstellererklärung **muss** dabei auf einer Prüfung des Produktes für qualifizierte elektronische Signaturen aufsetzen, die gemäß Anlage 1 Abschnitt I Nr. 1 SigV nach den Kriterien **ITSEC² oder CC³** von einer geeigneten Prüfstelle durchgeführt wurde.“*

Nach §15 Abs. 5 SigV muss eine Herstellererklärung nach §17 Abs. 4 SigG

„1. den Aussteller und das Produkt genau bezeichnen und

2. genaue Angaben darüber enthalten, welche Anforderungen des Signaturgesetzes und dieser Verordnung im einzelnen erfüllt sind.

Bei der Prüfung und Bestätigung der Sicherheit von Produkten nach §17 Abs. 1 und 3 Nr. 1 des Signaturgesetzes sind die Vorgaben des Abschnitts II der Anlage 1 zu dieser Verordnung zu beachten.“

Evtl. wird dadurch die Herstellererklärung mit dem Abschnitt II der Anlage 1 zur SigV in Zusammenhang gebracht (obwohl der Satz mit „bei der Prüfung und Bestätigung“ anfängt). Dort wird folgendes formuliert:

„II. Zu § 15 Abs. 5 dieser Verordnung und nach § 17 Abs. 1 und 3 Nr. 1 des Signaturgesetzes (nach § 4 Abs. 3 des Signaturgesetzes angezeigte Zertifizierungsdiensteanbieter ohne freiwillige Akkreditierung)

*Für die **Prüfung** von Produkten nach § 15 Abs. 5 gelten die Anforderungen nach Abschnitt I entsprechend.*

Abweichend hiervon können

- *Produkte zum Einsatz kommen, die den Normen nach § 15 Abs. 6 entsprechen,*
- *Produkte nach den § 17 Abs. 2 und 3 Nr. 2 und 3 des Signaturgesetzes (bzw. nach Abschnitt I Nr. 1.1 Buchstabe c und d) zum Einsatz kommen, bei denen **anstelle der Bestätigung eine Herstellererklärung** nach §17 Abs. 4 des Signaturgesetzes vorliegt.“*

Der erste Satz („Für die Prüfung von Produkten nach §15 Abs. 5 gelten die Anforderungen nach Abschnitt I entsprechend.“) verweist auf Abschnitt I der Anlage 1 zu SigV, welche die Prüftiefe definiert.

Demnach ist klar, welche Anforderungen bei einer Prüfung der Signaturanwendungskomponente – sofern denn eine solche durchzuführen ist - erfüllt werden müssen. Die angesprochene

² „Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik“ (ITSEC – GMBI. vom 8. August 1992, S. 545)

³ „Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik“ (CC - Common Criteria for Information Technology Security Evaluation – Banz. 1999, S. 1945 – ISO/IEC 15408).

Interpretation, wonach auf jeden Fall geprüft werden muss, und entweder eine Bestätigung oder eine Herstellererklärung zur Erfüllung der Anforderungen aus Signaturgesetz und -verordnung benötigt wird, könnte sich auch auf die Formulierung „*anstelle der Bestätigung eine Herstellererklärung*“ stützen, die in diesem Kontext (scheinbar) bewusst auf die Erwähnung der Prüfung verzichtet.

Es stellt sich abschließend die Frage, welchen Sinn eine Herstellererklärung anstelle einer Bestätigung nach einer bereits erfolgreich durchlaufenen ITSEC- oder CC-Evaluation noch hat. Zur Zeit ist es in der Regel so, dass der meiste Aufwand im Prüf- und Bestätigungsprozess in der Prüfung liegt. Die Bestätigung nach SigG ist dann meistens nur noch mit vergleichsweise geringem Aufwand verbunden.

2.1.4 Anforderungen an Signaturanwendungskomponenten

Nachdem die eher formalen Fragen der Prüfung und Bestätigung erörtert wurden, sollen insbesondere auch inhaltliche Anforderungen an Signaturanwendungskomponenten nach SigG behandelt werden. Folgende gesetzliche Vorgaben kommen insbesondere zur Anwendung, wenn Signaturanwendungskomponenten (oder auch nur Teile solcher Komponenten, wie Funktionsbibliotheken o. ä.) nach ITSEC oder CC geprüft werden und wenn eine Bestätigung nach SigG erfolgt.

„Signaturanwendungskomponenten“ sind in §2 Nr. 11 SigG definiert als:

„Software- und Hardwareprodukte, die dazu bestimmt sind,

- a) Daten dem Prozess der Erzeugung oder Prüfung qualifizierter elektronischer Signaturen zuzuführen oder*
- b) qualifizierte elektronische Signaturen zu prüfen oder qualifizierte Zertifikate nachzuprüfen und die Ergebnisse anzuzeigen,“*

Die Anforderungen an diese Signaturanwendungskomponenten sind in §17 Abs. 2 SigG festgehalten:

„Für die Darstellung zu signierender Daten sind Signaturanwendungskomponenten erforderlich, die die Erzeugung einer qualifizierten elektronischen Signatur vorher eindeutig anzeigen und feststellen lassen, auf welche Daten sich die Signatur bezieht. Für die Überprüfung signierter Daten sind Signaturanwendungskomponenten erforderlich, die feststellen lassen,

- 1. auf welche Daten sich die Signatur bezieht,*
- 2. ob die signierten Daten unverändert sind,*
- 3. welchem Signaturschlüssel-Inhaber die Signatur zuzuordnen ist,*
- 4. welche Inhalte das qualifizierte Zertifikat, auf dem die Signatur beruht, und zugehörige qualifizierte Attribut-Zertifikate aufweisen und*
- 5. zu welchem Ergebnis die Nachprüfung von Zertifikaten nach § 5 Abs. 1 Satz 2 geführt hat.*

Signaturanwendungskomponenten müssen nach Bedarf auch den Inhalt der zu signierenden oder signierten Daten hinreichend erkennen lassen. Die Signaturschlüssel-Inhaber sollen solche Signaturanwendungskomponenten einsetzen oder andere geeignete Maßnahmen zur Sicherheit qualifizierter elektronischer Signaturen treffen.“

§15 Abs. 2 und Abs. 4 SigV machen weitere Angaben zu den Anforderungen an solche Signaturanwendungskomponenten:

„(2) Signaturanwendungskomponenten nach § 17 Abs. 2 des Signaturgesetzes müssen gewährleisten, dass

1. bei der Erzeugung einer qualifizierten elektronischen Signatur

- a) die Identifikationsdaten nicht preisgegeben und diese nur auf der jeweiligen sicheren Signaturerstellungseinheit gespeichert werden,*
- b) eine Signatur nur durch die berechtigt signierende Person erfolgt,*
- c) die Erzeugung einer Signatur vorher eindeutig angezeigt wird und*

2. bei der Prüfung einer qualifizierten elektronischen Signatur

- a) die Korrektheit der Signatur zuverlässig geprüft und zutreffend angezeigt wird und*
- b) eindeutig erkennbar wird, ob die nachgeprüften qualifizierten Zertifikate im jeweiligen Zertifikat-Verzeichnis zum angegebenen Zeitpunkt vorhanden und nicht gesperrt waren.“*

Die Begründung zu §15 Abs. 2 SigV geht nun näher darauf ein, was dies im einzelnen – insbesondere auch für „Massensignaturen“ – bedeutet:

- *„Damit die Erzeugung einer Signatur nur durch die berechtigte Person erfolgen kann, dürfen bei der Aktivierung der Signaturerstellungseinheit die Identifikationsdaten (z. B. die **PIN**) beim Vergleich mit den auf der Signaturerstellungseinheit gespeicherten Referenzdaten **nicht auslesbar oder speicherbar** sein (Nummer 1 Buchst. a)). Ihre Geheimhaltung ist zu jedem Zeitpunkt zu gewährleisten.“*
- *„Die Signaturkomponente darf nicht ohne Anwendung der Identifikationsdaten genutzt werden können, es sei denn, Signaturen sollen für ein **festes Zeitfenster** oder eine **bestimmte Anzahl** ohne jeweilige Identifizierung erzeugt werden. In diesem Falle ist sicherzustellen, dass Unberechtigte keine Signaturen veranlassen können (Nummer 1 Buchst. b)).“*
- *„Die Erzeugung einer Signatur muss durch einen Warnhinweis vorher angezeigt werden (Nummer 1 Buchst. c)). Insbesondere bei der automatischen Erzeugung von Signaturen ("Massensignaturen") muss sichergestellt sein, dass Signaturen nur zu dem **voreingestellten Zweck** (z. B. Signaturen zu Zahlungsanweisungen bei Großanwendern) und durch eine zuvor **geprüfte und abgenommene Anwendung** vorgenommen werden können.“*

Nach §15 Abs. 4 SigV müssen „sicherheitstechnische Veränderungen an technischen Komponenten“ ... „für den Nutzer erkennbar werden.“

Die Antwort zu Frage 18 der FAQ der RegTP⁴ gibt bei der „Massensignatur“ weiterhin folgendes zu bedenken:

„Trotz Verwendung dieser technischen Hilfsmittel werden die Erklärungen aus den signierten Dokumenten dem Absender zugerechnet. Daher sollte bei derartigen „automatisch“ erstellten

⁴ Siehe <http://www.regtp.de> → Elektronische Signatur → FAQ

Signaturen immer ein besonderer Schutz gegen Missbrauch implementiert werden. Dieser Schutz sollte sich an dem Aktivierungszeitraum orientieren, was von einem verschlossenen Stahlschrank für Karte und Kartenleser, bis hin zur TrustCenter Umgebung reichen kann.“

2.1.5 Zeitstempel statt Signatur?

Eine weitere Fragestellung, die im Zusammenhang mit der „Massensignatur“ oft diskutiert wird ist, ob ein qualifizierter Zeitstempel u. U. eine qualifizierte Signatur ersetzen kann.

Kann man nicht einfach die heute bereits existierenden, typischerweise hoch performant ausgelegten, Zeitstempelsysteme verwenden, um massenhaft Signaturen zu erstellen?

Diese Frage ist zunächst einmal berechtigt, wenn man bedenkt, dass sich ein erzeugter Zeitstempel bei manchen derzeit schon auf dem Markt befindlichen Produkten technisch nicht von einer Signatur unterscheidet. Es kann also zwei Datensätze geben, deren Formate sich syntaktisch nicht voneinander unterscheiden⁵, wovon der eine semantisch aber (mit einer zusätzlichen Zeitinformaton versehene) signierte Daten und der andere mit einem Zeitstempel versehene Daten darstellt.

Ein qualifizierter Zeitstempel ist gemäß §2 Nr. 14 SigG

„eine elektronische Bescheinigung eines Zertifizierungsdiensteanbieters [...] darüber, dass ihm bestimmte Daten zu einem bestimmten Zeitpunkt vorgelegen haben.“

Ein qualifizierter Zeitstempel bestätigt also lediglich, dass bestimmte Daten zu einem bestimmten Zeitpunkt existiert haben, nicht aber, dass die darin enthaltenen Daten korrekt sind oder dass eine Person dem Inhalt dieser Daten zugestimmt hat. Der Sinn und Zweck eines Zeitstempels ist eben ein anderer, als der einer Signatur.

So kann insbesondere jeder legitime Nutzer des Zeitstempeldienstes eines Zertifizierungsdiensteanbieters einen qualifizierten Zeitstempel an beliebige Daten anbringen lassen. Ist durch das Erstellen dieser Signatur eine „Unterschrift“ (im Sinne einer Willenserklärung) erfolgt? - Wohl kaum. Der Zertifizierungsdiensteanbieter - präziser gesagt die natürliche Person, für die das qualifizierte Zertifikat des Zeitstempeldienstes ausgestellt wurde - hätte in diesem Fall auch etwas „unterschrieben“, dessen Inhalt er gar nicht kennt. Ein Zertifizierungsdiensteanbieter wird deshalb jeden qualifizierten Zeitstempel, den er ausstellt, deutlich als solchen kennzeichnen, um oben erwähnten Missinterpretationen vorzubeugen. Diese Kennzeichnung ist zur Zeit bei akkreditierten Zertifizierungsdiensteanbietern deutlich zu erkennen. Ein qualifizierter Zeitstempel eines akkreditierten Zertifizierungsdiensteanbieters wurde mit einem Signaturschlüssel signiert, für dessen zugehörigen Signaturprüf Schlüssel die RegTP ein qualifiziertes Zertifikat ausgestellt hat. Dieses qualifizierte Zertifikat enthält üblicherweise ein eindeutiges Pseudonym, welches den intendierten Zweck des Zertifikates sowie den Zertifizierungsdiensteanbieter kennzeichnet. Denkbar wäre auch, im Zertifikat ein spezielles Feld „Verwendungszweck“ zu nutzen.

⁵ Beispielsweise ist dies bei der Nutzung des Signaturformates [PKCS#7] (Cryptographic Message Syntax Standard) der Fall, der für Signaturen („digitally signed data“) optional das Hinzufügen einer Zeitinformaton (Attribut „signing time“, welches im Standard [PKCS#9] detailliert spezifiziert wird) erlaubt. Solche Datenformate werden in der Praxis sowohl für (qualifizierte elektronische) Signaturen als für (qualifizierte) Zeitstempel verwendet.

Es ist also denkbar, dass die zur Erzeugung qualifizierter Zeitstempel existierenden Produkte technisch zur massenhaften Erzeugung qualifizierter elektronischer Signaturen eingesetzt werden, sofern sie technisch Signaturen erzeugen. Jedoch werden dann in der Regel in diesen Produkten Signaturkarten zum Einsatz kommen, die nicht für die Ausstellung von qualifizierten Zeitstempeln vorgesehen sind.

2.2 Anwendungsgesetze

Um maßgeschneiderte Massensignatur-Lösungen entwickeln zu können, müssen neben den rechtlichen Rahmenbedingungen aus SigG und SigV auch die jeweiligen Anwendungsgesetze berücksichtigt werden. Die folgende Diskussion wird zeigen, dass diese applikationsspezifischen Anforderungen durchaus unterschiedlich sein können.

2.2.1 §14 UStG

Für den Vorsteuerabzug bei der elektronischen Abrechnung ist §14 Abs. 4 Satz 2 [UStG02] maßgeblich:

„Als Rechnung gilt auch eine mit einer qualifizierten elektronischen Signatur oder eine mit einer qualifizierten elektronischen Signatur mit Anbieter-Akkreditierung nach dem Signaturgesetz versehene elektronische Abrechnung.“

Im Vergleich dazu müssen schriftliche Rechnungen nicht mit einer handschriftlichen Unterschrift versehen werden. Damit ist hier festzuhalten, dass die qualifizierte elektronische Signatur scheinbar nicht eine „Unterschrift“ ersetzen soll, sondern vermutlich vielmehr dem Integritätsschutz und der Verbindlichkeit dient. Durch o. g. Formulierung („mit einer Signatur [...] versehene elektronische Abrechnung“) müssen keine zusätzlichen Anforderungen bzgl. der automatisierten Signaturerstellung berücksichtigt werden.

Wir werden sehen, dass sich die Situation bei der elektronischen Archivierung schriftlicher Unterlagen gemäß §36 SRVwV etwas anders darstellt.

2.2.2 §36 SRVwV

Die Sozialversicherungsrechnungsverordnung [SVRV] und die zugehörige Verwaltungsvorschrift [SRVwV] bilden die Rechtsgrundlage für die Abläufe im Rechnungswesen der Sozialversicherungsträger⁶. Die allgemeine Verwaltungsvorschrift [SRVwV] spezifiziert, wann bei der Rechnungslegung Unterschriften⁷ zu leisten sind und dass nach §41 die benötigten Unterschriften auch durch qualifizierte elektronische Signaturen gemäß Signaturgesetz ersetzt werden können.

§36 SRVwV (Aufbewahrung) enthält folgende Regelung:

„(1) Schriftliche Unterlagen dürfen vor Ablauf der betreffenden Aufbewahrungsfrist vernichtet werden, wenn

⁶ Die SVRV und SRVwV gilt beispielsweise für Träger der gesetzlichen Kranken-, Unfall-, Renten- und Pflegeversicherung.

⁷ Wie in [HeHü02] (Abschnitt 2.1.4) erläutert, werden in den §§ 5, 7, 10, 11, 15, 16, 18, 20, 21 und 36 der SRVwV Unterschriften gefordert.

1. sie auf einen maschinell verwertbaren Datenträger so übertragen sind, dass sie in bildlicher Form wiedergegeben werden können,
2. die bildliche Wiedergabe mit den zu vernichtenden Unterlagen übereinstimmt und sie die darin enthaltenen Daten erkennbar macht,
3. durch **digitale Signatur dessen, der die bildliche Wiedergabe erzeugt hat, die Übereinstimmung der bildlichen Wiedergabe mit der Unterlage bestätigt** und dadurch die **unbemerkte Veränderung der Unterlage ausgeschlossen ist,**“

Hier wird also davon ausgegangen, dass ein Operator nicht nur eine Signatur erzeugt, sondern dass er vorher

1. ein Schriftstück eingescannt hat und
2. das elektronische Abbild mit dem schriftlichen Original vergleicht

und die Signatur schließlich nur im Erfolgsfall erstellt.

Die Signatur des Operators dient hier also insbesondere auch als Bestätigung, dass der Scanningvorgang „alle relevanten Informationen mit hinreichender Präzision“ erfasst hat, so dass die (inhaltliche) Rekonstruktion der Originalunterlage möglich ist und elektronische Belege dadurch die gleiche Verbindlichkeit erlangen wie schriftliche Unterlagen.

Während §36 SRVwV die Aufbewahrung zahlungsbegründender, also für das Rechnungswesen relevanter, Unterlagen regelt, so existieren ähnliche Bestimmungen in §110 a)-d) SGB IV für „sonstige schriftliche Unterlagen“ (vgl. Artikel 47 [VwVfÄndG]). Hier erhalten die elektronisch aufbewahrten Unterlagen (nach §110 d) SGB IV) durch die qualifizierte elektronische Signatur dessen, der die elektronische Wiedergabe erstellt hat, Beweiskraft, „*soweit nach den Umständen des Einzelfalles kein Anlass ist, ihre sachliche Richtigkeit zu beanstanden.*“

Die Erstellung einer qualifizierten elektronischen Signatur nach §36 SRVwV und §110 SGB IV - oder auch zur Beglaubigung eines Dokumentes gemäß §33 VwVfG (vgl. Artikel 1 [VwVfÄndG]) – ist also im Vergleich zur Situation bei der elektronischen Rechnungsstellung mit einem zusätzlichen (manuellen) Prüfungsvorgang verbunden, der sich grundsätzlich nur schwer vollständig automatisieren lassen wird.

So ist der Einsatz der „Massensignatur“ zur elektronischen Archivierung gemäß §36 SRVwV mit zusätzlichen Problemen behaftet und mit der heutigen Fassung dieses Paragraphen streng genommen **nicht** vereinbar.

Da aber das Mengengerüst⁸ bei vielen Krankenkassen die „Massensignatur“ unverzichtbar macht, wurde im Schriftwechsel zwischen dem Bundesversicherungsamt und dem Bundesministerium für Arbeit und Sozialordnung (siehe [BVA02] und [BMA02]) bereits angedeutet, dass dem Einsatz der „Massensignatur“ zur Archivierung gemäß §36 SRVwV unter den in der Begründung zu §15 Abs. 2 SigV enthaltenen Bedingungen zugestimmt wird und dass die Vorschrift des §36 SRVwV „*bei der nächsten Überarbeitung*“ entsprechend angepasst wird.

⁸ Beispielsweise muss die KKH für zwei Versicherte jährlich etwa drei Belege (Meldungen zur Sozialversicherung, Beitragsnachweise, Arbeitsunfähigkeitsbescheinigungen, ...) archivieren. Bei Kassen mit 8 Mio. Versicherten (wie z.B. der DAK oder der Barmer Ersatzkasse) wären das etwa eine Million Belege pro Monat. Das ist sicherlich eine Größenordnung, die nicht (wirtschaftlich vertretbar) ohne die massenhafte elektronische Verarbeitung bewerkstelligt werden kann.

Hier darf man gespannt sein, ob im Rahmen dieser Überarbeitung, die möglicherweise zusammen mit der Entwicklung der Verwaltungsvereinbarung gemäß §110 c) SGB IV realisiert wird, neben Sicherheitsmaßnahmen⁹ für die „Massensignatur“ auch eine stichprobenartige Überprüfung der Erfassungsqualität gefordert wird.

3 Technische und organisatorische Aspekte

In diesem Abschnitt werden verschiedene technische und organisatorische Aspekte der Realisierung sicherer und gleichsam performanter Systeme zur Erzeugung und Verifikation qualifizierter elektronischer Signaturen erörtert.

3.1 Sicherheit

Wie in Abschnitt 2 angedeutet wurde, existieren gewisse grundlegende Sicherheitsanforderungen für die Erzeugung von qualifizierten elektronischen Signaturen. Insbesondere die massenhafte automatisierte Erzeugung solcher Signaturen birgt immense Risiken, da bei Fehlern oder Angriffen evtl. sofort massenhaft falsche Signaturen erzeugt werden. Außerdem erfolgt das Bemerkens eines Fehlers oder Angriffs u. U. erst sehr spät oder gar nicht.

Ungeachtet dessen, ob nun eine Prüfung und Bestätigung oder eine Prüfung und Abnahme einer Anwendung zur Erzeugung von qualifizierten elektronischen Signaturen erforderlich ist, sind grundsätzliche Sicherheitsbetrachtungen unerlässlich¹⁰.

Insbesondere muss der generellen Bedrohung des „Missbrauchs des Signatursystems“ entgegengewirkt werden. Letztlich ist durch geeignete Maßnahmen zu verhindern, dass ein Angreifer unlegitimierte Signaturen erstellen kann.

Durch diese Maßnahmen ist dafür zu sorgen, dass das Signaturerstellungssystem selbst integer ist und in einer vertrauenswürdigen Einsatzumgebung angewandt wird. So ist beispielsweise durch Zutrittskontrollanlagen, Benutzerauthentisierung, Maßnahmen der Netzwerk- und Systemsicherheit (Netzsegmentierung, Firewall- und Intrusion-Detection-Systeme, Systemintegritäts- und Virenschutzmechanismen etc.) und nicht zuletzt organisatorische Maßnahmen für ein vertrauenswürdigen betriebenes Gesamtsystem zu sorgen.

Die bereits erwähnte Prüfung einer Anwendung durch eine unabhängige dritte Partei kann dem Nutzer zunächst versichern, dass die Anwendung selbst nicht korrupt ist. Jedoch muss auch sie korrekt eingesetzt werden, so dass die implementierten Sicherheitsmechanismen greifen. Deshalb ist neben einer – möglicherweise geprüften und bestätigten - Komponente selbst stets auch ihre Einsatzumgebung zu berücksichtigen.

Signaturanwendungskomponenten mit einem von der RegTP vergebenen Gütesiegel genügen einer einheitlichen Spezifikation hinsichtlich der zu beachtenden Einsatzumgebung (siehe

⁹ Beim Einsatz der automatisierten Datenverarbeitung und Signaturtechnologie für die Belange des Rechnungswesens in der Sozialversicherung wird nach §40 [SRVwV] – unabhängig davon, ob die Signaturerstellung automatisiert oder manuell erfolgt - eine Dienstanweisung benötigt, in der neben diversen Aspekten des IT-Betriebes auch Fragen der Informationssicherheit behandelt werden müssen. In diesem Fall sind neben Sicherheitsaspekten für das System zur (automatisierten) Signaturerzeugung insbesondere auch Datenschutzaspekte gemäß §78a [SGB X] zu berücksichtigen.

¹⁰ Beim Einsatz der Signaturtechnologie für das Rechnungswesen in der Sozialversicherung ist dieser generellen Empfehlung durch §40 SRVwV explizit Nachdruck verliehen.

[RegTP-SE]). Auch lediglich nach ITSEC oder CC geprüfte Komponenten müssen in den mit dem Produkt ausgelieferten Dokumentationen Hinweise auf die korrekte und sichere Nutzung des Produktes enthalten. Da es sich dabei aber ggf. nur um Teilkomponenten des Datenerzeugungs- und Signierungsprozesses handelt, müssen auch in diesem Fall, trotz der unabhängigen Prüfung, weitere Aspekte zum Schutz gegen Missbrauch betrachtet werden. Beispielsweise kann schon das System angreifbar sein, welches die Daten zu einem zu signierenden Datensatz zusammenfügt. Analog kann eine Manipulation auf dem Übertragungsweg von diesem System zur Signatur-Anwendung erfolgen. Denkbar wäre hier, dass die Signatur-Anwendung eine Plausibilitätsprüfung an den zu signierenden Daten durchführt, was jedoch auch nicht gegen alle möglichen Angriffe wirkt. Auch bei der Handhabung der eingesetzten Signaturkarten (und evtl. vorhandener Ersatzkarten) sind eine Reihe von Bedrohungen zu berücksichtigen. Diese und viele andere Überlegungen spielen insbesondere bei der „Massensignatur“ eine wichtige Rolle und bedürfen einer detaillierten individuellen Betrachtung.

Zur Befriedigung grundlegender Schutzbedürfnisse kann die Vorgehensweise des IT-Grundschutzhandbuches [BSI02], sowie anderer Standards für Sicherheitsmanagementsysteme, verwendet werden. Nach dem IT-Grundschutzhandbuch erfolgt die Erstellung des Grundschutz-Sicherheitskonzeptes in folgenden Schritten:

- IT-Strukturanalyse
- Schutzbedarfsbestimmung
- IT-Grundschutzanalyse¹¹
- Realisierungsplanung

Während durch die standardisierten Bedrohungen und Maßnahmen des IT-Grundschutzhandbuches auf ressourcenschonende Art und Weise ein grundlegendes Sicherheitsniveau erreicht werden kann, so besteht natürlich nicht die Garantie, dass die vorgeschlagenen Standardmaßnahmen auch wirklich angemessen sind. Werden durch „Massensignatur“-Systeme potenziell sehr werthaltige Dokumente verarbeitet, so dass ein Missbrauch zu beträchtlichen Schäden führen oder gar existenzbedrohende Ausmaße annehmen kann, so empfiehlt sich zusätzlich die Anwendung der im IT-Sicherheitshandbuch [BSI92] des BSI beschriebenen Methodik, wonach die IT-Grundschutzanalyse durch eine ausgefeiltere Bedrohungs- und Risikoanalyse ergänzt wird und bei der Erstellung des Sicherheitskonzeptes zusätzlich eine Abschätzung des Restrisikos durchgeführt wird.

Weiterhin kann eine Einschränkung des Wirkungsumfanges des genutzten qualifizierten Zertifikates durch geeignete Attribute und Beschränkungen im Zertifikat zum Einsatz kommen, was jedoch nicht präventiv wirkt. Zur Zeit sind solche Attribute und Beschränkungen jedoch nur unvollständig standardisiert und werden zudem nicht von jedem Zertifizierungsdiensteanbieter angeboten.

3.2 Performance

Neben den oben geschilderten Sicherheitsaspekten sind bei Systemen zur „Massensignatur“ insbesondere auch Aspekte der performanten Realisierung zu beachten. Verlangt die Prob-

¹¹ Bei erhöhtem Schutzbedarf oder falls keine geeigneten Grundschutzbausteine verfügbar sind, müssen ergänzende Sicherheitsanalysen, z.B. gemäß IT-Sicherheitshandbuch [BSI92], durchgeführt werden.

lemstellung eine Lösung, die in der Lage ist eine große Anzahl an Signaturen in kurzer Zeit zu erzeugen, so existieren hierfür grundsätzlich verschiedene Möglichkeiten:

- **Einsatz leistungsfähigerer Signaturerstellungseinheiten (HSM statt Chipkarte)**

Hier wäre es denkbar, an Stelle einer Chipkarte, wie sie heute typischer Weise zur Erstellung von Signaturen eingesetzt wird, ein leistungsfähigeres Hardware-Sicherheits-Modul (HSM) einzusetzen. Da bei qualifizierten elektronischen Signaturen gemäß §2 Nr. 3 SigG aber neben der Verwendung eines qualifizierten Zertifikates auch der Einsatz einer sicheren Signaturerstellungseinheit gemäß §2 Nr. 10 SigG gefordert ist, sind die Anforderungen aus §17 oder §23 SigG und SigV zu beachten.

Gemäß Anlage 1 SigV sind die sicheren Signaturerstellungseinheiten beispielsweise gemäß ITSEC E3 (hoch) oder EAL4 (einschließlich der Prüfung gegen hohes Angriffspotenzial und einer vollständigen Missbrauchsanalyse) zu prüfen und – nach §17 Abs. 4 *zwingend* von einer Stelle nach §18 SigG – zu bestätigen. Derzeit existieren lediglich Chipkarten, die eine solche Prüfung und Bestätigung vorweisen können.

Auf der anderen Seite wurde beispielsweise in Österreich bereits ein (Chrysalis Luna CA³) HSM für die Verwendung als sichere Signaturerstellungseinheit zugelassen¹². Nach §23 Abs. 3 SigG werden solche Produkte auch in Deutschland anerkannt, „wenn sie nachweislich gleichwertige Sicherheit aufweisen“. So lange dieser Nachweis nicht erbracht ist, scheidet diese Möglichkeit jedoch aus.

- **Parallelisierung**

Eine einfache, und in der Praxis häufig eingesetzte, Methode zur Steigerung der quantitativen Leistungsfähigkeit von Signatursystemen besteht in der naiven Parallelisierung - statt einer Chipkarte werden mehrere parallel betrieben. Die Signatur-Anwendungssoftware verteilt die zu signierenden Daten auf die parallel angeordneten Chipkarten. In diesem Szenario existieren besondere Anforderungen an die Leistungsfähigkeit und Zuverlässigkeit der Serverkomponente.

Unterstellt man, dass eine ideale Parallelisierung möglich ist und die Erstellung einer Signatur (inklusive der Kommunikation) etwa eine Sekunde dauert, dann können täglich die in Tabelle 1 aufgeführte Anzahl an Signaturen erstellt werden.

Anzahl parallel arbeitender Chipkarten	Anzahl möglicher Signaturen pro Tag
1	86.400
5	432.000
10	864.000

¹² Die entsprechende Bestätigungsurkunde findet sich unter http://www.a-sit.at/signatur/bestaetigungsstelle/bescheinigung/veroeffentlichung_andere/bestaet_chrys_its_luna.pdf.

15	1.296.000
20	1.728.000
50	4.320.000
100	8.640.000

Tabelle 1: Anzahl möglicher Signaturen pro Tag

- **Stapelsignaturen**

Ist auch die durch Parallelisierung erreichbare Leistungsfähigkeit nicht ausreichend, so kann der Versuch unternommen werden, algorithmische Optimierungen und Stapelverarbeitungsstrategien gewinnbringend einzusetzen.

Da die mathematische Signaturerzeugung (Errechnen der Signatur unter Verwendung des geheimen Schlüssels und des Hashwertes der Nachricht) auf der Chipkarte durchgeführt wird, scheiden algorithmische Optimierungen, z. B. im Stile von [Merk99], aus.

Durch die Bildung von baumartig aufgebauten Hashketten, wie beispielsweise in [PaBo99] und davon unabhängig in [BrPo02] vorgeschlagen (vgl. Abbildung 1), ist es möglich mittels einer mathematischen Signaturerzeugung (Signatur der Wurzel) einen ganzen „Stapel“ von Hashwerten (alle Blätter) zu signieren.

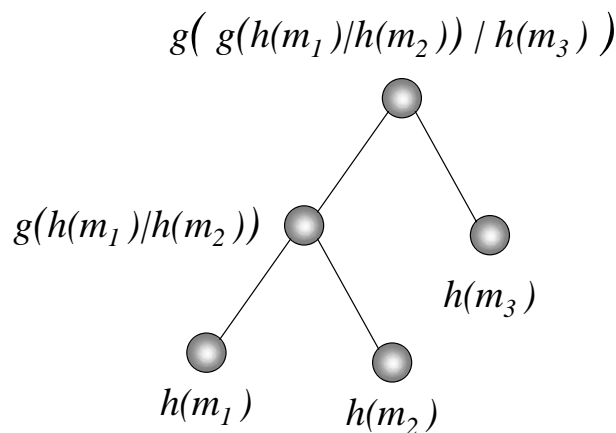


Abbildung 1: Baumartig aufgebaute Hashketten

Unterstellt man, dass die verwendeten Hashfunktionen (g und h) kollisionsresistent sind, dann kann gezeigt werden (vgl. Lemma 1 in [PaBo99]), dass die so erzeugten Signaturen genau so sicher wie gewöhnliche Signaturen sind. Während dieser Ansatz theoretisch sehr ansprechend ist, so spricht das Fehlen entsprechender Standards für derartige Stapelsignaturen (derzeit) gegen diesen Ansatz.

4 Danksagung

Die vorliegende Arbeit profitierte vom fruchtbaren Gedankenaustausch mit einer Reihe von Personen. In diesem Zusammenhang möchten wir uns besonders herzlich bei den Teilnehmern des BVA und der RegTP am Arbeitskreis „Elektronische Signatur“ bedanken.

Literatur

- [BMA02] Bundesministerium für Arbeit und Sozialordnung (Wershoven, K.): *Betreff: Einsatz elektronischer Signaturen nach dem Signaturgesetz (SigG) in der Finanzbuchhaltung der Sozialversicherungsträger ...*, *Bezug: Ihr Schreiben vom 28.03.2002 – VI – 59012.84 – 648/2001*, Schreiben vom 31.05.2002 an das BVA
- [BoEi02] Bovenschulte, A., Eifert, M.: Rechtsfragen der Anwendung technischer Produkte nach Signaturgesetz, (DuD 2/2002)
- [BrPo02] Brandner, R.; Pordesch, U.: Long-term conservation of provability of electronically signed documents, Beitrag zu ISSE, 2002
- [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
- [BSI92] Bundesamt für Sicherheit in der Informationstechnik: *IT-Sicherheitshandbuch – Handbuch für die sichere Anwendung der Informationstechnik*, 1992, Bezugsinformationen unter <http://www.bsi.bund.de/literat/kriterie.htm>
- [BSI02] Bundesamt für Sicherheit in der Informationstechnik: *IT-Grundschutzhandbuch*, Mai 2002, via <http://www.bsi.de/gshb/>
- [BVA02] Bundesversicherungsamt (Müller, R.): Einsatz elektronischer Signaturen nach dem Signaturgesetz (SigG) in der Finanzbuchhaltung der Sozialversicherungsträger; hier: elektronische Archivierung von Beitragsnachweisen nach §28 f., Abs. 3 SGB IV; Antrag der Kaufmännischen Krankenkasse (KKH) nach §19 SVRV, Schreiben vom 28.03.2002 – VI – 59012.84 – 648/2001 an das BMA
- [EGSRL] Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen, via http://europa.eu.int/comm/internal_market/en/media/sign/Dir99-93-ecDE.pdf
- [EU-EBP] Price Waterhouse Coopers: Study on the requirements imposed by the Member States, for the purpose of charging taxes, for invoices produced by electronic or other means, 1999 via http://europa.eu.int/comm/taxation_customs/publications/reports_studies/taxation/final_report_pwc.pdf
- [HeHü02] Hesse, J.; Hühlein, D.: *Public-Key-Infrastrukturen für Sozialversicherungsträger*, in Horster P. (Hrsg.): Tagungsband Elektronische Geschäftsprozesse, IT-Verlag, 2002, ISBN 3-936052-07-7, SS. 177-198
- [Merk99] Merkle, J.: *Effiziente Signaturerzeugung durch Server-Unterstützung und Vorberechnung*, Dissertation, Universität Frankfurt 1999
- [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> (siehe auch Kaliski B., RFC2315, via <http://www.ietf.org>)
- [PKCS#9] RSA Labs: *PKCS #9 – Selected Attribute types*, via <http://www.ietf.org><http://www.rsasecurity.com/rsalabs/pkcs/pkcs-9/index.html> (siehe Nyström M. und Kaliski B., RFC2985, via <http://www.ietf.org>)
- [RegTP-SE] RegTP: *Einheitliche Spezifizierung der Einsatzbedingungen für Signaturanwendungskomponenten*,
http://www.regtp.de/imperia/md/content/tech_reg_t/digisign/118.pdf
- [RegTP-HE] RegTP: *Herstellererklärung für Produkte für qualifizierte elektronische Signaturen, Version 2.0 vom Oktober 2002*, via
http://www.regtp.de/imperia/md/content/tech_reg_t/digisign/115.pdf
- [SGB X] SGB X: *Sozialgesetzbuch Zehntes Buch (SGB X) Verwaltungsverfahren, Schutz der Sozialdaten, Zusammenarbeit der Leistungsträger und ihre Beziehungen zu Dritten*, in der Fassung vom 18. Mai 2001 (Fassung vom 7. August 1996, via <http://www.sozialgesetzbuch.de>)
- [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>
- [SigVBeg] *Begründung zu [SigV]*, via
http://www.iid.de/iukdg/aktuelles/begr_verordnung.pdf
- [SRVwV] *Allgemeine Verwaltungsvorschrift über das Rechnungswesen in der Sozialversicherung, (SRVwV) vom 15. Juli 1999*, zuletzt geändert am 18. September 2000, via <http://www.hvbg.de/d/revision/gruen/kap3/kap32.pdf>
- [SVRV] *Verordnung über den Zahlungsverkehr, die Buchführung und die Rechnungslegung in der Sozialversicherung (Sozialversicherungs-Rechnungsverordnung – SVRV)*, BGBl. Teil I, S. 1627 (15. Juli 1999), via <http://www.hvbg.de/d/revision/gruen/kap3/kap31.pdf>
- [UStG02] *Umsatzsteuergesetz*, Neugefasst durch Bekanntmachung vom 09.06.1999 **BGBl. Teil I Seite** 1270 ff, zuletzt geändert durch das Steueränderungsgesetz StÄndG 2001, BGBl. Teil I Nr. 72 vom 22.12.2001
- [VwVfÄndG] *Drittes Gesetz zur Änderung verwaltungsverfahrenrechtlicher Vorschriften (VwVfÄndG)*, BGBl. I Nr. 60, vom 27.08.2002, via <http://217.160.60.235/BGBL/bgb11f/bgb1102s3322.pdf>