Rechtliche Betrachtungen zur automatisierten Erzeugung qualifizierter elektronischer Signaturen gemäß §14 UStG und §36 SRVwV

Detlef Hühnlein[1] · Yvonne Knosowski[2] · Ragna Tern[3]

secunet Security Networks AG
[1]Sudetenstraße 16, 96247 Michelau
[2]Weidenauerstraße 223–225, 57076 Siegen
[3]Im Teelbruch 116, 45219 Essen

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

Abstract: Diese Arbeit beleuchtet einige rechtliche Aspekte der automatisierten Erzeugung qualifizierter elektronischer Signaturen – der sogenannten „Massensignatur“. Neben den generellen Rahmenbedingungen aus der Signaturgesetzgebung wird der Einsatz der „Massensignatur“ zur elektronischen Rechungsstellung gemäß §14 Abs. 4. Satz 2 UStG und zur elektronischen Archivierung schriftlicher Unterlagen gemäß §36 Abs. 1 SRVwV 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 UStG mit qualifizierten elektronischen Signaturen gemäß Signaturgesetz [SigG] versehen sein.

In ähnlicher Art und Weise verspricht die papierlose Abwicklung des Rechungswesens 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 automatisierte Erzeugung dieser qualifizierten elektronischen Signaturen – die sogenannte „Massensignatur“ – für diese Anwendungen von entscheidender Bedeutung.

Dieser Beitrag beleuchtet einige rechtliche Aspekte der „Massensignatur“ für die beiden Anwendungsfälle zur Rechnungsstellung gemäß §14 UStG und zur Archivierung gemäß §36 SRVwV. Abschnitt 2 beleuchtet die rechtlichen Rahmenbedingungen aus der Signaturgesetzgebung und Abschnitt 3 widmet sich den spezifischen Anforderungen der beiden näher betrachteten Anwendungsgesetze.

2. Signaturgesetzgebung

In diesem Abschnitt werden die rechtlichen Rahmenbedingungen der „Massensignatur“ in der Signaturgesetzgebung 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 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.

2.2 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 Eigenschaften[1] 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 [BE02] 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.“*

---

[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.“

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. Deshalb kommt der Beachtung von Sicherheitsaspekten bei der „Massensignatur“ eine besondere Bedeutung zu.

2.3 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 Hersteller des Produktes (im Folgenden mit Herstellererklärung bezeichnet) auf. Diese Herstellererklärungen 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 gestellte 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 **ITSEC**[2] **oder CC**[3] 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] „Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik“ (ITSEC – GMBl. vom 8. August 1992, S. 545)

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

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 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 Bestätigungs-Prozess in der Prüfung liegt. Die Bestätigung nach SigG ist dann meistens nur noch mit vergleichsweise geringem Aufwand verbunden.

2.4 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 RegTP[4] 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 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.“

2.5 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?

---

[4] Siehe http://www.regtp.de → Elektronische Signatur → FAQ

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 unterscheiden[5], wovon der eine semantisch aber (mit einer zusätzlichen Zeitinformation 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 Signaturprüfschlüssel 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.

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.

---

[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 Zeitinformation (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.

3. 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.

3.1 §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.

3.2 §36 SRVwV

Die Sozialversicherungsrechnungsverordnung [SVRV] und die zugehörige Verwaltungsvorschrift [SRVwV] bilden die Rechtsgrundlage für die Abläufe im Rechnungswesen der Sozialversicherungsträger[6]. Die allgemeine Verwaltungsvorschrift [SRVwV] spezifiziert, wann bei der Rechnungslegung Unterschriften[7] 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 Scanvorgang „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 Mengengerüst[8] bei vielen Sozialversicherungsträgern die „Massensignatur" unverzichtbar macht, wurde im Schriftwechsel zwischen dem Bundesversicherungsamt

---

[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. Bei der LVA-Rheinprovinz soll der komplette Aktenbestand mit bis zu 154 Mio. Belegen elektronisch erfasst werden. Das ist sicherlich eine Größenordnung, die nicht (wirtschaftlich vertretbar) ohne eine großteils automatisierte elektronische Verarbeitung bewerkstelligt werden kann.

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.

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 Sicherheitsmaßnahmen[9] für die „Massensignatur“ auch eine stichprobenartige Überprüfung der Erfassungsqualität gefordert wird.

4. Zusammenfassung

Wie in diesem Beitrag erläutert wurde, ist die automatisierte Erzeugung qualifizierter elektronischer Signaturen („Massensignatur“) kein Widerspruch in sich – und kann im Einklang mit SigG und SigV realisiert werden, wobei durch das erhöhte Angriffspotenzial besondere Sicherheitsmaßnahmen angezeigt sind und die Empfehlungen in der Begründung zu §15 Abs. 2 SigV als erste Orientierung dienen können.

Wie die Betrachtung der beiden Anwendungsfälle §14 UStG und §36 SRVwV gezeigt hat, müssen neben der Signaturgesetzgebung insbesondere auch die Anwendungsgesetze betrachtet werden, so dass bei der Frage nach der Einsetzbarkeit der „Massensignatur“ letztlich der spezifische Anwendungsfall betrachtet werden muss. Während die automatisierte Erzeugung qualifizierter Signaturen für §14 UStG sicherlich möglich ist, ist sie mit der derzeitigen Fassung des §36 SRVwV im Grunde kaum vereinbar und wird sich beispielsweise auch nicht ohne weiteres zu Zwecken einer „automatisierten Beglaubigung“ gemäß §29 SGB X bzw. §33 VerwVfG einsetzen lassen.

Literaturverzeichnis

[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 – V1 – 59012.84 – 648/2001*, Schreiben vom 31.05.2002 an das BVA

[BE02] Bovenschulte, A., Eifert, M.: Rechtsfragen der Anwendung technischer Produkte nach Signaturgesetz, (DuD 2/2002)

[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.

[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

[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 – V1 – 59012.84 – 648/2001 an das BMA

[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.; Hühnlein, D.: *Public-Key-Infrastrukturen für Sozialversicherungsträger*, in Horster P. (Hrsg.): Tagungsband Elektronische Geschäftsprozesse, IT-Verlag, 2002, ISBN 3-936052-07-7; S. 177-198

[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-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 verwaltungsverfahrensrechtlicher Vorschriften (VwVfÄndG)*, BGBl, I Nr. 60, vom 27.08.2002, via http://217.160.60.235/BGBL/bgbl1f/bgbl102s3322.pdf