Forum Elektronische Steuerprüfung

Ausgabe 7/2007

Umgang mit 2D- Barcode- „Signaturen“ für Versender und Empfänger elektronischer Rechnungen

Darstellung der rechtlichen Anforderungen an die Verarbeitung von 2D-Barcode- „Signaturen“ im Hinblick auf Vorsteuerabzugsfähigkeit und steuerliche wie handelsrechtliche Aufbewahrungspflichten. Stellungnahme zum Sinn oder Unsinn einer technischen Lösung zum Transport qualifizierter Signaturen.

Raoul Kirmes

Über den Autor

Raoul Kirmes ist Produktmanager bei der Mentana-Claimsoft AG, einem auf PKI- und Signaturlösungen spezialisierten Software-unternehmen. Er ist Mitautor des Buches „Digitale Signaturen in der Praxis“ und Verfasser von zahlreichen Fachbeiträgen zum Thema Signaturen und Beweiskraft elektronischer Dokumente.

Einleitung

Anlass dieses Beitrages ist das zunehmende Auftreten von sog. "Barcodesignaturen“ für den Versand elektronischer Rechnungen und die auftretenden Probleme bei der Verifikation dieser Rechnungen für die Empfänger.

Leider bestehen in der Praxis erhebliche Fehlvorstellungen sowohl bei Empfängern solcher Rechnungen als auch bei Fachleuten[1] über die dem Verfahren zugrundeliegende Technik und die daraus folgenden Notwendigkeiten für einen wirksamen Vorsteuerabzug gemäß § 15 UStG und die gesetzlichen Aufbewahrungsanforderungen.

Diese Fehlvorstellungen werden nicht selten auch von den Versendern selbst und vermutlich auch von den dahinter stehenden Herstellern dieser Lösungen verbreitet.

Beispielhaft für solche fehlerhaften „Werbeaussagen“ soll nachfolgend der Hinweis eines Versenders aus dem Bereich Telekommunikation vorgestellt und untersucht werden.

Die ***Fa. Sipgate*** schreibt auf ihrer Website[2]:

> ***„Was ist die elektronische Signatur?***
> ***Wie funktioniert die Überprüfung der elektronischen Signatur? (…) Damit Sie als Gewerbetreibender diese Rechnungen in gewohnter Form beim Finanzamt einreichen können, signiert sipgate alle Rechnungen ab sofort elektronisch. Sie erkennen Ihre elektronisch signierte Rechnung an einem schwarz / weißen Balken im unteren Abschnitt der Rechnung, der an ein Bildrauschen im Fernsehen erinnert. Innerhalb dieses Bereichs werden alle Rechnungsdaten ein zweites mal verschlüsselt wiedergegeben - so können Sie und die Finanzbehörden mittels einer Entschlüsselungssoftware (www.secrypt.de) stets feststellen, ob das Dokument dem Originalzustand entspricht oder manipuliert wurde.***
>
> ***Praktisch:***
> ***Im Gegensatz zu vielen anderen Verschlüsselungsverfahren reicht beim sipgate-System der einfach Ausdruck per Tintenstrahl oder Laserdrucker aus. Eine zusätzliche Übermittlung der elektronischen Datei an das Finanzamt ist nicht nötig. „***

Der nachfolgende Beitrag wird im Einzelnen der Frage nachgehen, ob diese Aussagen zutreffend sind.

Zur Beurteilung der rechtlichen Anforderungen an eine 2D-Barcodesignatur ist es zunächst notwendig zu erläutern, wie dieses Verfahren überhaupt technisch funktioniert und was es rechtlich bewirkt. Denn der verheißungsvolle Name lässt ein völlig neues und innovatives Verfahren vermuten, das geeignet ist, die Schwierigkeiten (Verifikation/ Archivierung) der ***„vielen anderen Systeme“*** zu vermeiden.
Allerdings wird sich das Gegenteil erweisen.

1 Beitrag in diesem Forum von Walter Steigauf "Einfache Lösung für PDF- und Fax-Rechnungen in Sicht."

2 http://www.sipgate.de ; Hilfebereich; Stand 20.06.2007.

Forum Elektronische Steuerprüfung

Ausgabe 7/2007

I. Formanforderungen an elektronische Rechnungen

Die grundsätzlichen Regelungen zu den Formanforderungen bei elektronischen Rechnungen sind inzwischen sicher keine Neuigkeit mehr. Die Regelungen für den **Aussteller** elektronischer Rechnungen ergeben sich aus **§ 14 Abs. 3 UStG.** Die Regelungen für den **Empfänger** ergeben sich aus **§ 15 Abs.1 Nr.1 Satz 2 UStG**. Zu den notwendigen Tätigkeiten beim Erhalt elektronischer Rechnungen, also zum Ablauf der sogenannten „Verifikation" einer elektronischen Rechnung, darf ich auf ein Dokument in diesem Forum verweisen:

http://www.elektronische-steuerpruefung.de/loesung/kirmes_erech.htm

Ebenfalls darf ich hinsichtlich der Folgen der Nichtbeachtung dieser Vorschriften auf einen Beitrag in diesem Forum verweisen:

http://www.elektronische-steuerpruefung.de/e_rechnungen/kirmes_1.htm

II. Was sind Barcode und 2D- Data Matrix Codes?

Ein Barcode oder auch Strichcode genannt, ist eine optoelektronisch lesbare Zeichenfolge, die entweder aus verschieden breiten parallelen Strichen und Lücken besteht (1D-Codes) oder als rechteckige Matrix dargestellt wird (2D- Codes). Die Daten in einem Strichcode werden mit optischen Lesegeräten, wie z. B. Barcodelesegeräten (Scanner) oder Kameras, maschinell eingelesen, redigitalisiert und elektronisch weiterverarbeitet. Mit dem zweidimensionalen „Data Matrix" Code kann eine beachtliche Datenmenge pro Fläche gespeichert werden. Das verbreitetste, weil sicherste, Darstellungs- bzw. Codierungsverfahren[3] ist der ECC 200. Beim ECC 200 ist der digitale Code redundant in der Matrix enthalten, sodass eine Fehlerkorrektur möglich ist. Durch das sog. "Reed-Solomon-Fehlerkorrektur-Verfahren"[4] können beim ECC 200 bis zu 25 % der Fehler, die entstehen können, wenn beispielsweise Teile des Codes überdeckt oder zerstört sind, korrigiert werden.

Zusammengefasst ist ein 2D- Barcode also ein **grafischer Datenspeicher** der in der internationalen Norm ISO/IEC 16022 definiert wurde. Zum Auswerten eines 2D-Barcodes benötigt man eine flächige Lichtquelle. Das vom 2D-Code reflektierte Licht wird dann zum Beispiel von einem CMOS[5]-Sensor scharf abgebildet und kann so als Grundlage für eine Redigitalisierung genutzt werden. In der Praxis sind also entsprechende Scanner oder Kameras von Nöten. Alternativ kann auch spezielle OCR[6]-Software eingesetzt werden, die in der Lage ist, ohne Scanner den Barcode korrekt aus dem Bild (2D-Barcode) der Datei zu extrahieren und zu interpretieren.

III. Ist ein 2D- Barcode ein neues Signaturformat?

Signaturen beruhen auf der Anwendung einer PKI,[7] deren Grundlage wiederum die Verwendung von sicheren Algorithmen[8] ist. Die gültigen Algorithmen und Verfahren werden im jährlichen sog. Algorithmenkatalog[9] der Bundesnetzagentur, der Aufsichtsbehörde nach dem Signaturgesetz, veröffentlicht. In der Praxis wird für Signaturverfahren zu fast 100% der RSA- Algorithmus in verschiedenen Schlüssellängen verwendet. Die Formatierungsverfahren für die Algorithmen sind sicherheitskritisch und deshalb „sorgfältig zu wählen"[10]. Für den RSA- Algorithmus wird durch die Bundesnetzagentur der PKCS- Standard[11] als Grundlage einer Formatierung empfohlen. Deshalb wundert nicht, dass der PKCS- Standard derzeit der einzige in der Praxis vorzufindende Standard bei Zertifizierungsdiensteanbietern[12] für den Einsatzzweck „qualifizierte elektronische Signatur" im Sinne des SigG ist. Der PKCS- Standard enthält 13 gültige Varianten, wobei die PKCS# 2 und 4 mit PKCS#1 vereinigt wurden. In der Praxis und für die Signatur relevant sind die Typen PKCS# 7[13] und PKCS# 11[14]. Die für den Anwender sichtbaren Format- bzw. Dateiendungen sind:

P7s; P7m; P7b; .p12.

---

[3] Es gibt verschiedene "Symbologien": „ECC n"; n = 0 bis 200; ECC = „Error Checking and Correction Algorithm".

[4] Es handelt sich um einen Algorithmus der 1960 von Irving S. Reed und Gustave Solomon entwickelt wurde und sehr gute Fehlerkorrektur-eigenschaften bei relativ einfachen Decodierungsgabläufen besitzt.

[5] **„C**omplementary **M**etal **O**xide **S**emiconductor" - komplementärer Metall-Oxid-Halbleiter- also ein Elektronikbaustein aus einer bestimmten Logikfamilie.

[6] **O**ptical **C**haracter **R**ecognition: optische Texterkennung.

[7] **P**ublic **K**ey **I**nfrastructure, Verfahren zur Verwendung von kryptografischen Schlüsselpaaren für Signatur und Verschlüsselung.

[8] Ebenfalls als sicher werden sog. „DAS"- Algorithmen incl. Varianten, das „EC_DSA" Verfahren und die „Nyberg-Rueppel-" Signaturen durch die BNetzA postuliert. In der Praxis ist allerdings neben dem RSA noch keine Anwendung im Bereich der qualifizierten Signatur im praktischen Einsatz.

[9] http://www.bundesnetzagentur.de/enid/9b661ea194340435f7305f99a00e171f,0/Veroeffentlichungen/Algorithmen_sw.html .

[10] Zitat: Algorithmenkatalog 2007, Pkt. 3.1. .

[11] **P**ublic **K**ey **C**ryptography **S**tandards, enthält alle gültigen interoperablen kryptografischen Spezifikationen.

[12] Sowohl im angezeigten wie im akkreditierten Bereich.

[13] Genormt in RFC 2315. Beschreibt die Verwendung für „S/MIME" und für das Signieren und/oder Verschlüsseln von Nachrichten mit einer PKI. Wird insbesondere von allen Microsoft-Systemen unterstützt.

[14] Wird insbesondere von Mozzila, Thunderbird und Netscape für die S/MIME Anwendung genutzt.

Ebenfalls zum PKCS#7 gehören Signaturen, die gemäß PDF- Referenz 1.4 bis 1.6 in das PDF Dokument integriert wurden. Die Dateiendung des PDF- Dokuments ändert sich durch die Signatur nicht, sondern verbleibt bei „.pdf“. Zur Ansicht der Unterschrift (Signatur) ist der Kartenreiter "Unterschriften" am linken Rand des Adobe Acrobat Readers zu öffnen. Diese Variante ist zweifelsohne die anwenderfreundlichste Signaturverarbeitung die derzeit am Markt zu haben ist. Ebenfalls eine Variante des PKCS# 7 ist das CMS- Format[15].

Eine ***„Verschlüsselung“*** von Daten via 2D- Barcode ist als Signaturformat somit weder strukturell geeignet noch ausreichend sicher und für eine solche Anwendung auch nicht behördlich zugelassen. Auch könnte ein neues Signaturformat ohnehin nur von einem Zertifizierungs-diensteanbieter in dem Markt gebracht werden und nicht von einem Hersteller für Software zur Nutzung von Signaturen. Denn die Entscheidung über das verwendete Signaturformat fällt bereits bei der Zertifikatsausgabe durch den Zertifizierungsdiensteanbieter.

Der 2D- Barcode ist also kein Signaturformat!

Allerdings wird dies auch von keinem mir bekannten Hersteller[16] offiziell behauptet. Ganz im Gegenteil, auch in den veröffentlichten Zulassungsdokumenten dieser Hersteller wird **nicht behauptet,** dass es sich bei dem **2D-Barcode um die Signatur handeln würde**.

Zur Anbringung einer gültigen qualifizierten Signatur im Sinne von § 2 Nr. 3 SigG und damit auch im Sinne von § 14 Abs. 3 UStG muss eine sog. „Signaturanwendungs-komponente“, also spezielle Software, genutzt werden.
Alle zugelassenen Signaturanwendungskomponenten müssen gemäß § 17 Abs. 4 Satz 2 SigG[17] in Verbindung mit § 15 Abs. 5 SigV[18] vor Inverkehrbringen durch Veröffentlichung einer sog. Herstellererklärung im Amtsblatt der zuständigen Aufsichtsbehörde nach § 3 SigG veröffentlicht werden.
Der Hersteller der Signaturanwendungskomponente des hier aufgegriffenen Beispiels (Fa. Sipgate) ist die Fa. Secrypt aus Berlin.
Aus der Herstellererklärung der Fa. Secrypt für das Produkt:

„D-SIGN matrix Version 3.2“[19] geht auf Seite 5 der Herstellererklärung folgendes hervor:

(…“**zulässige Signaturausgabeformate**:..“

- „signedData“ gemäß RFC 2630 (Dateiendungen *.pk7 und *.p7s)

- „signedData“ mit „multipart-signed“-Content gemäß RFC 2633 („…” *.p7m)

- "Portable Document Format“ PDF
(PKCS#7-konforme Signatur entsprechend Adobe-Reference 1.6)")

Nur diese Signaturformate werden also nach richtiger Ansicht des Herstellers, für die Erstellung von qualifizierten Signaturen verwendet. Es handelt sich bei allen genannten Formaten um Varianten des PKCS#7 bzw. CMS.

Was hat es nun aber mit dem 2D- Barcode auf sich?

Aus signaturtechnischer Sicht so gut wie nichts. Denn der Barcode ist lediglich ein grafischer Speicher für beliebige Daten. Selbstverständlich ist es auch möglich, Signaturinformationen oder eine Rechnungsdatei in einen 2D- Barcode zu speichern, wobei der mögliche Speicherplatz durch die verfügbare Fläche des Transportdokuments begrenzt[20] wird.
So auch die Idee bei der sog. „2D- Barcodesignatur“.
Man gibt einem Papierdokument über den 2D-Barcode elektronische Daten mit, welche zur Prüfung (Verifikation) dieses Papierbelegs benötigt werden, weil man gerade dem Papierbeleg nicht traut. Die im 2D-Barcode enthaltenen Daten werden zur Prüfung redigitalisiert und verifiziert. Eine sinnvolle Anwendung ist z.B. der Einsatz im Bereich der Flugzeugwartung zur Identifizierung von Ersatzteilen. So

[15] **C**rypto **M**essage **S**yntax, ist PKCS #7 als externe Datei oder als Envelope wie bei P7m hier aber Namens (Encapsulated Content). Hauptvorteil ist, dass man nicht mehr die Dokumente an den Signaturserver sendet, sondern den Hash und der Server die Signaturantwort als ASN.1 Struktur zurück gibt. Das macht bei Volumen von > 1 Mio. Dokumente am Tag, die nicht präsentiert werden müssen durchaus Sinn (also insbesondere in Archivlösungen).

[16] Mir sind überhaupt nur 2 Hersteller bekannt die diese Systeme auch für elektronische Rechnungen anbieten: Fa. secrypt aus Berlin und xyzmo Software GmbH ehemals Trosoft aus Östereich. Ferrari Labelt nur secrypt.

[17] Gesetz über Rahmenbedingungen für elektronische Signaturen (SigG) vom 16. Mai 2001 (BGBl. S. 876, Jahrgang 2001 Teil I Nr. 22) in der Fassung des 1. SigÄndG vom 04. Januar 2005

[18] Verordnung zur elektronischen Signatur (Signaturverordnung – SigV) vom 16. November 2001 (BGBl. Jahrgang 2001 Teil I Nr. 59) in der Fassung des 1. SigÄndG vom 04. Januar 2005

[19] vgl.http://www.bundesnetzagentur.de/enid/2b51f0258611195cf09cac7dd352562a,0/Herstellererklaerungen/SignAnwKomp_2__7_39u.html

[20] Insofern kommt auch eine nur teilweise Speicherung von Rechnungsdaten in den Barcode in Betracht. Allerdings reicht bei Weitem nicht, lediglich eine Rechnungsnummer in den Barcode zu übergeben. Es müssen alle Pflichtangaben des § 14 Abs. 4 UStG im Barcode enthalten und signiert sein.

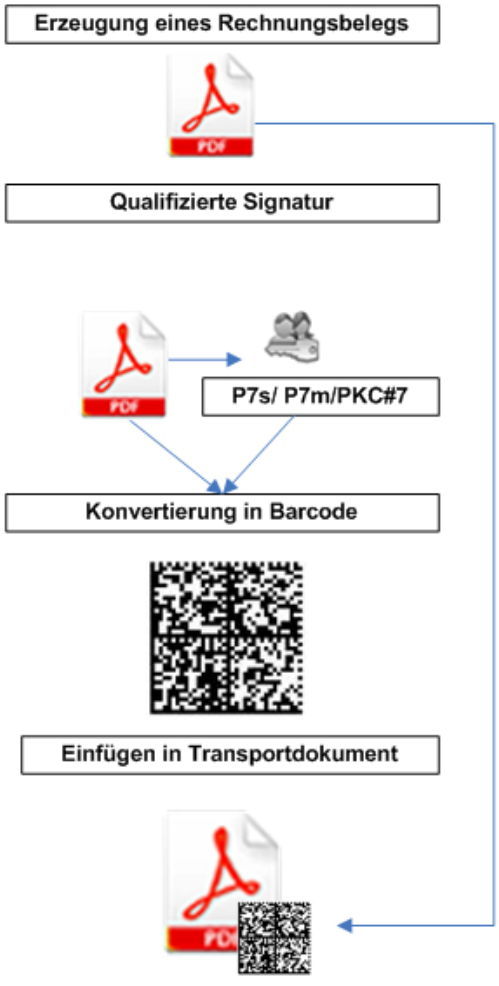
können die Ersatzteile selbst oder die Begleitscheine mit einem 2D-Barcode ausgestattet werden. Der Empfänger des Ersatzteils redigitalisiert die Daten, welche sich im Barcode befinden, verifiziert diese Daten gegen eine Prüfinstanz des Herstellers und kann dann sicher sein, dass es sich um ein Original- Ersatzteil handelt. Solche Projekte hat Fa. secrypt bei Airbus und Mentana- Claimsoft AG für Lufthansa Technik umgesetzt. Diese Technik ist also keineswegs sinnlos, sondern hat in sehr speziellen Anwendungsbereichen durchaus ihre Berechtigung.

IV. Sinn oder Unsinn eines 2D- Barcode auf Rechnungen

Fraglich ist nur, ob sich dieses Verfahren im Umfeld der elektronischen Rechnungen sinnvoll einsetzen lässt.

Technisch möglich ist folgender Ablauf.

A. Ablauf der Erzeugung einer Rechnung mit Matrixsignatur



Erstellung und Versand

Eine Rechnung wird also erstellt und konventionell qualifiziert signiert[21]. Diese signierte Datei und die Signaturdatei können nun als 2D-Barcode umgerechnet werden und auf ein „Transportdokument“ grafisch aufgebracht werden. Dies erfolgt entweder per Druck (so z.B. bei der Faxrechnung) oder wenn die Transportdatei elektronisch ausgeliefert werden soll, als Bild-Datei des Barcodes, der in die Datei eingefügt wird. Als Transportdokument wird regelmäßig eine Kopie der Ursprungsrechnung benutzt.

Allerdings muss nun Folgendes beachtet werden. Das hier als „Transportdokument“ bezeichnete Dokument wird in der Praxis häufig mit der Rechnung verwechselt. **Das Transportdokument ist aber gerade nicht die Rechnung im Sinne des Umsatzsteuergesetzes!** Dies hat folgende einfache Ursachen:

1. Dieses Dokument ist gerade nicht qualifiziert signiert und
2. durch das Aufbringen des 2D- Barcodes auf das Dokument hat sich der Hashwert[22] des Transportdokuments im Vergleich zum Originaldokument, welches der qualifizierten Signatur zugrunde lag, **nach** Signatur zwangsläufig verändert. Dieses Dokument ist also nicht mehr gültig signiert! Es ist lediglich der Torso, um den Barcode zu transportieren.

Daraus folgt, dass der Übermittlungsvorgang der elektronischen Rechnung im Sinne des § 14 Abs. 3 UStG erst abgeschlossen ist, wenn die Redigitalisierung der Rechnungs- und Signaturdaten aus dem Barcode abgeschlossen ist. Erst dann kann der Empfänger sicher sein, dass er im Besitz (§ 15 UstG) einer signierten Rechnung ist. Hat er den Besitz, muss er die Integrität von Signatur und Rechnung überprüfen, denn es wäre ohne weites möglich, dass die Signatur mit einer gesperrten Karte aufgebracht wurde. Das ist Sinn und Zweck der Verifikation.

Im Übrigen ist ohne Redigitalisierung überhaupt nicht klar, was in dem Barcode enthalten ist. Es könnte auch einfach Unsinn in den Barcode gespeichert werden, ohne dass dies für den Empfänger optisch erkennbar wäre.

[21] Dabei ist das gewählte Signaturformat letztlich frei wählbar. Die in der Grafik aufgezählten Formate sind nur beispielhaft.

[22] Hashwert, eindeutiges Ergebnis eines mathematischen Algorithmus (z.B. SHA1), der die Datei repräsentiert, die signiert wird. Die geringste Veränderung an der Datei ändert den Hash und führt zur Ungültigkeit dieser Signatur.

Erhalt und Verifikation

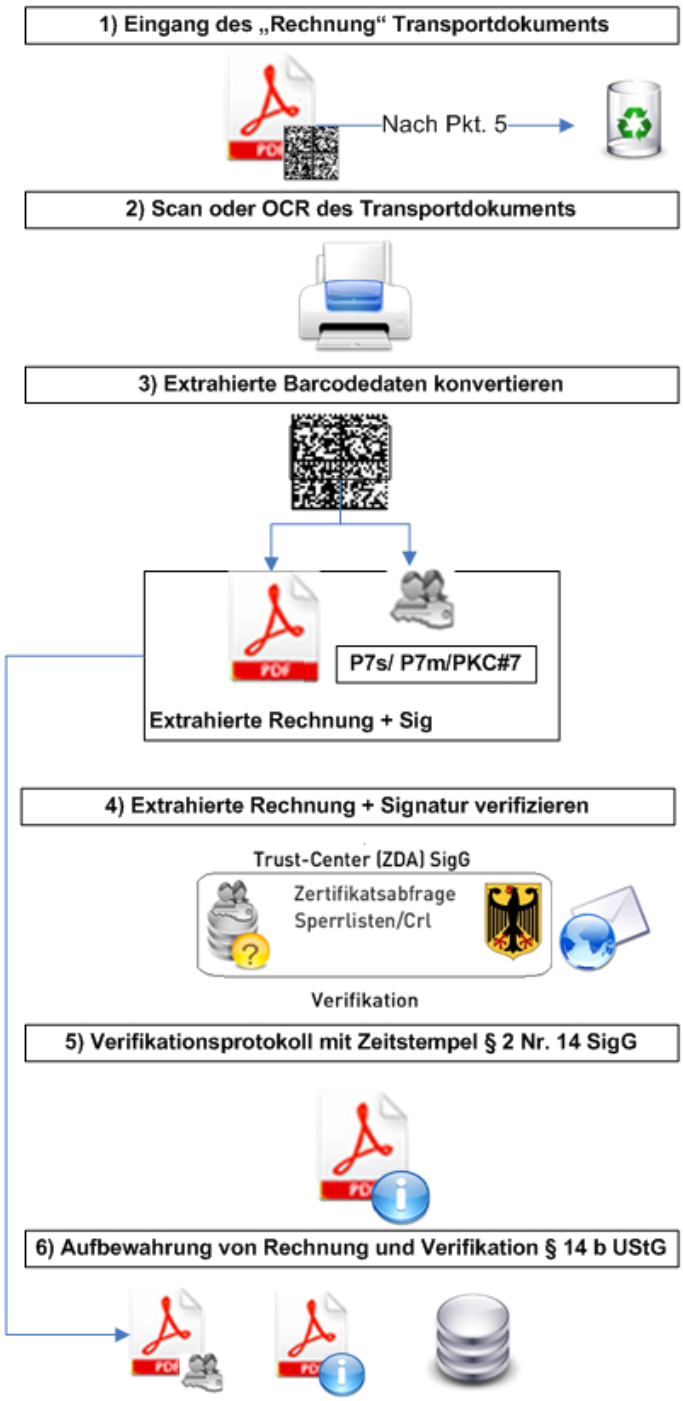
Deshalb soll nachfolgend auch der Verifikationsvorgang einer Barcoderechnung im Einzelnen dargestellt werden.

Als technische Voraussetzungen für den Erhalt der Rechnung im Rechtssinne ist zunächst einiges an Hard- und/oder Software beim Empfänger von Nöten. Denn die Auswertung eines 2D- Barcodes setzt regelmäßig einen Scanner oder eine Kamera mit entsprechender Auswertungssoftware voraus, die in der Lage ist, den verwendeten 2D- Barcode- Algorithmus auszuwerten. Erhält man die Rechnung mit dem Barcode elektronisch (z.B. per Mail oder Upload), kann man inzwischen den Scanner durch eine spez. OCR-Software ersetzen. Da allerdings die Hersteller den Codierungsalgorithmus für den 2D-Barcode bislang nicht offen legen, muss derzeit zwingend die Software des Versenders (Herstellers) beim Empfänger installiert werden, um überhaupt den Empfang der elektronischen Rechnung zu ermöglichen!

Aus Sicht des Rechnungsversenders ist dies eigentlich ein KO- Kriterium hinsichtlich des Einsatzes von Barcodesignaturen, denn ein **Zugang der Rechnung** wird **nicht bewirkt**, solange der Empfänger Hard- und Software nicht besitzt, diese nicht einsatzbereit hat oder auch einfach nicht installieren kann[23] oder will. Denn der Empfänger muss für den Zugang vom Inhalt der Nachricht (hier die Rechnung) Kenntnis nehmen können (§ 130 BGB). Fehlen ihm dazu die technischen Mittel, erfolgt kein Zugang. Es tritt im Zweifel keine Fälligkeit für den Rechnungsbetrag ein, soweit dieser von einer Rechnung abhängig war.

Unterstellen wir nachfolgend, dass der Empfänger bereit war, sich Scanner und Software zu beschaffen und zu installieren. Nun muss er die Rechnungsdaten redigitalisieren, das Ergebnis der Redigitalisierung, also die Rechnungsdatei und die Signaturdatei, verifizieren, das Ergebnis der Verifikation protokollieren und vor Veränderung (Zeitstempel § 2 Nr. 14 SigG) schützen sowie die redigitalisierten Dateien und das Verifikationsprotokoll nach § 14b UStG aufbewahren. Das Transportdokument kann er hingegen als rechtliches Nullum vernichten.

B. Ablauf der Verifikation einer Matrixsignatur

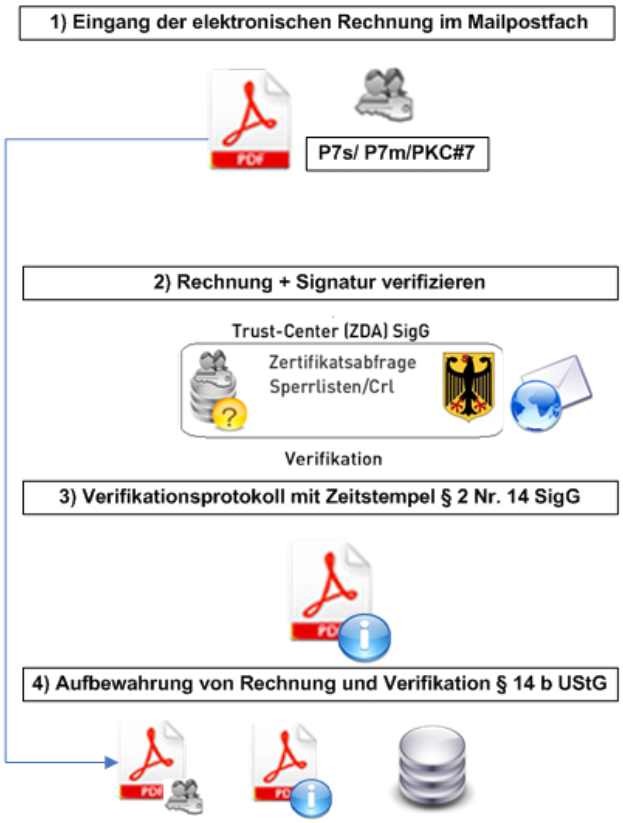


[23] z.B. wegen abweichenden Sicherheitskonzepten, die eine Installation nicht zulassen. Oder weil z.B. die Plattform des Empfängers vom Versender nicht unterstützt wird. Wenn also der Empfänger Linux oder Mac einsetzt, kann er z.B. keine Prüfsoftware installieren, die nur unter Windows verfügbar ist.

C. Ablauf der konventionellen Verifikation

Im Vergleich dazu noch einmal der „konventionelle“ Ablauf. Man sieht auf den ersten Blick, dass die Verifikation im Gegensatz zum Ablauf beim 2D- Barcode nur aus 4 statt 6 Schritten besteht. Daneben ist für den Empfang und die Ansicht der Rechnung keine spezielle Hardware oder Software notwendig, wenn man unterstellt, dass der Adobe Acrobat Reader allgemein verfügbar ist.

C. Ablauf Verifikation einer Rechnung ohne Barcode



Unterhält der Rechnungsempfänger ein E-Mail-Rechnungspostfach, welches über eine Verifikationsfunktion verfügt, läuft dieser gesamte Vorgang vollautomatisch ab. Der Empfänger erhält beim Abruf der E-Mail (POP3 oder IMAP) einfach neben der Rechnung ein qualifiziert signiertes und mit Zeitstempel versehenes Verifikationsprotokoll als weitere Datei im Anhang der Mail. Er hat im Ergebnis mit dem elektronischen Rechnungseingang keine einzige zusätzliche Aufgabe und das sollte doch das Ziel aller technischen Lösungen sein.

Der größte Nachteil der 2D-Barcodesignatur ist in diesem Zusammenhang jedoch die mangelhafte Interoperabilität. Dieses Manko ist einfach dem Umstand geschuldet, dass es nur 2 Hersteller am Markt gibt, die diese Systeme aktiv vermarkten wollen und deshalb bislang keine Standardisierung stattgefunden hat. Im Gegenteil behauptet Fa. trosoft bzw. xyzmo auf ihrer Website, im Übrigen wettbewerbswidrig, das Verfahren wäre „patentiert“, was nicht zutrifft. Auch Fa. Secrypt macht ein Geheimnis um die Entschlüsselung ihres Matrixcodes. Die Verifikation elektronischer Rechnungen lässt sich für die Empfänger jedoch nur sinnvoll gestalten, wenn er diese **versenderunabhängig** automatisieren kann. Denn nur so kann sichergestellt werden, dass ein Empfänger von diversen Versendern elektronische Rechnungen empfangen und verifizieren kann.[24] Es ist völlig inakzeptabel, dass ein Versender dem Empfänger die Verwendung einer bestimmten, nur von einem Hersteller angebotenen, Software oder die Anschaffung/ Installation von spez. Hardware aufzwingt, damit er seine Rechnungen möglichst günstig elektronisch versenden kann. Hier wird der Empfänger über kurz oder lang wieder eine Papierrechnung verlangen, denn es ist kaum vorstellbar, dass eine größere Gruppe von Empfängern solche Bedingungen akzeptiert. Die Empfänger werden den elektronischen Zugang für diese Versender verbieten, was ihr gutes Recht ist.

V. Rechtliche Bewertung des Hinweises Fa. Sipgate

Aus den vorausgehenden Darstellungen wird ersichtlich, dass der Hinweis der Fa. Sipgate leider völlig neben der Sache liegt.

1. Falschdarstellung:

> ***„Sie erkennen Ihre elektronisch signierte Rechnung an einem schwarz / weißen Balken im unteren Abschnitt der Rechnung. „***

Diese Aussage trifft in zweierlei Hinsicht nicht zu. Zum einem handelt es sich bei diesem Dokument nur um das Transportdokument, eben nicht um die Rechnung (s. o.), und der 2D- Barcode ist gerade nicht die qualifizierte Signatur, sondern nur ein Datenspeicher (s.o.).

[24] Wozu der jahrelange Kampf um die Standardisierung „ISIMTT“, wenn man die Interoperabilität von eigentlich inzwischen standardisierten Verfahren über diesen Umweg wieder zunichte macht?

2. Falschdarstellung:

„So können Sie und die Finanzbehörden.....feststellen, ob das Dokument dem Originalzustand entspricht oder manipuliert wurde."

Wie oben dargestellt ist dieses Transportdokument auf jeden Fall durch das Einfügen des 2D-Barcode nach Signatur verändert worden. Eine Signaturprüfung über das Transportdokument würde stets fehlschlagen. Auch genügt nicht die Möglichkeit (***…„So können"***.) der Verifikation, sondern diese muss erfolgen, bevor der in der Rechnung enthaltene Vorsteuerbetrag zum Abzug gebracht wird. Also regelmäßig bereits bei Erhalt, jedenfalls **vor** der zumeist monatlichen **Umsatzsteuervoranmeldung**.

3. Falschdarstellung:

„…Im Gegensatz zu vielen anderen Verschlüsselungsverfahren reicht beim sipgate-System der einfache Ausdruck per Tintenstrahl oder Laserdrucker aus."

Dieser Hinweis ist ebenfalls falsch, denn ein Ausdruck des Dokuments, welches den Barcode enthält, genügt nicht weil:

a) der Ausdruck nicht die Originalrechnung, sondern das Transportdokument betrifft. Dieses Dokument ist aber gerade nicht die Rechnung.

b) in jedem Fall redigitalisiert werden muss, um überhaupt in „Besitz" der signierten Rechnung zu gelangen, denn in dem Barcode könnte auch nur „Datenschrott" enthalten sein.

c) der Ausdruck nicht die Verpflichtung ersetzt, die redigitalisierten Daten, wie jede andere elektronische Rechnung, zu verifizieren, ein Prüfprotokoll zu erzeugen und diese Daten gemäß § 14b UStG elektronisch aufzubewahren. Selbst ein Ausdruck der redigitalisierten Daten würde nicht genügen. Dazu gleich mehr beim nächsten Punkt.

4. Falschdarstellung:

„Eine zusätzliche Übermittlung der elektronischen Datei an das Finanzamt ist nicht nötig.."

Auch dieser Hinweis ist grob falsch. Eingangsrechnungen sind „empfangene Handelsbriefe" im Sinne des § 147 Abs. 2 Nr. 1 AO, die nach § 147 Abs. 5 AO dem Datenzugriff der Finanzverwaltung bereit zu stellen sind (GDPdU). Dabei ist zu betonen, dass es sich um originär elektronisch erzeugte[25] und übermittelte Belege handelt. Dies hat zur Folge, dass diese Daten in jedem Fall auch elektronisch aufzubewahren und auf Anforderung des Betriebsprüfers auch elektronisch zu übermitteln sind (Z1 bis Z3). Der Ausdruck und **die** Aufbewahrung auf **Papier** ist gerade **ein unzulässiger Medienbruch**[26]" und wird einhellig von Literatur[27], Finanzverwaltung[28] und Rechtsprechung[29] abgelehnt.

Aus § 147 Abs. 2 AO ist auch zu entnehmen, dass der Steuerpflichtige eine Form der digitalen Aufbewahrung zu wählen hat, die nach dem Stand der Technik dem Finanzamt die gesetzlich geforderte Auswertbarkeit ermöglicht ohne zusätzliche Erschwerungen oder Hindernisse für den Betriebsprüfer zu errichten. Gemessen an diesem Maßstab ist eine „Aufbewahrung" von steuerrelevanten Buchungsdaten in einem Barcode eine unzulässige Erschwerung mit der Folge, dass nicht nur die umsatzsteuerrechtlichen Anforderungen betroffen sind, sondern auch die Aufbewahrungspflichten der AO verletzt sein dürften. Im Ergebnis heißt das: nur die aus dem Barcode redigitalisierten Daten sind Buchungsbelege im Sinne von § 147 Abs.1 Nr. 4 AO. Der Barcode kann nur als „Zwischenformat" (sog. „Inhouse-Format") verwendet werden. Eine Überführung der Daten aus dem Barcode ist somit auch aus diesem Gesichtspunkt zwingend erforderlich.

---

[25] Der Streit um die Frage, ob der Zugriff des BP sich nur auf auswertbare Daten oder auch auf elektronische Belege erstreckt, kann hier dahinstehen, da originär elektronisch Belege jedenfalls immer bereit zu stellen sind. Es zeichnet sich sogar ab, dass die Rsp. das Zugriffsrecht auf nachträglich digitalisierte und nicht auswertbare Dateien erstrecken will. Insofern ist man gut beraten, auf jeden Fall alle elektronischen Belege auch elektronisch aufzubewahren.

[26] FG- Düsseldorf, 05.02.2007, 16V 3454/06; m. w. N. in Strunk/Zöllkau, BB 2001, 703 und Kersbrock/ Riedel/Strunk, Der Betrieb 2002, Beilage Nr. 9 zu Heft Nr. 49, 2.

[27] vgl. für viele nur Bunjes/Geist UStG, 8. Auflage, Seite 601, § 14b.

[28] FAQ zum Datenzugriffsrecht der Finanzverwaltung (Stand 01.02. 2005), www.bundesfinanzministerium.de.

[29] FG-RLP, 4 K 2167/04.

Zum Schluss und als Zusammenfassung ein Blick in die **GOBS Abschnitt VIII Buchstabe b) Nr. 2:**
Dort heißt es: *(Klammern durch den Autor eingefügt)*

„- vor einer weiteren Verarbeitung der elektronischen Abrechnung ist die qualifizierte elektronische Signatur im Hinblick auf die Integrität der Daten und die Signaturberechtigung geprüft worden und das Ergebnis dokumentiert worden;“
(Also ein Verifikationsprotokoll der redigitalisierten Rechnung)

„- die Speicherung der elektronischen Abrechnung auf einem Datenträger erfolgt, der Änderungen nicht mehr zulässt. Bei einer temporären Speicherung auf einem änderbaren Datenträger muss das DV-System sicherstellen, dass Änderungen nicht möglich sind;“

(Hinsichtlich Rechnung genügt die Signaturdatei (nicht der Barcode), hinsichtlich Verifikationsprotokoll ist ein Zeitstempel nach § 2 Nr. 14 SigG oder ein spez. Archiv notwendig)

„- der Signaturprüfschlüssel aufbewahrt wird; bei Einsatz von Kryptographietechniken die verschlüsselte und die entschlüsselte Abrechnung sowie der Schlüssel zur Entschlüsselung der elektronischen Abrechnung aufbewahrt wird;“
(Dies betrifft nochmals die Anforderung, dass der redigitalisierte öffentliche Schlüssel des Versenders, der Bestandteil des Zertifikats ist, elektronisch aufzubewahren ist. Ohne spez. Archiv ist eine rechtskonforme Aufbewahrung derzeit nur als Inline- Signatur in einem PDF-Dokument nach DIN ISO 19005 praktikabel.)

„- der Eingang der elektronischen Abrechnung, ihre Archivierung und ggf. Konvertierung sowie die weitere Verarbeitung protokolliert werden;“
(Für den Nachweis, der Verifikation vor Vorsteuerabzug ist ein Zeitstempel nach § 2 Nr. 14 SigG stets verpflichtend, da nur aus diesem eine amtliche Zeit im Sinne des ZeitG gewonnen werden kann.)

VI. Schlussbemerkung

Im Mittelpunkt des Interesses für den Empfänger elektronischer Rechnungen steht naturgemäß zunächst der Anspruch auf Vorsteuerabzug aus dem Rechnungsbeleg. Wie der Wortlaut des § 15 UStG eindeutig ergibt, setzt das Recht auf Vorsteuerabzug den **Besitz (!)** einer formgerechten Rechnung gemäß § 14 Abs. 3 UStG voraus[30]. Hierüber kann man sich nur durch Verifikation Klarheit verschaffen. Daneben wird durch GOBS[31] und GDPdU[32] ein strenges Prüf- und Aufbewahrungsregime auferlegt. Allein dies macht den Umgang mit elektronischen Rechnungen schon nicht besonders einfach.

Werden dann durch den Einsatz von 2D-Barcodes noch weitere Konvertierungs- und Erkennungsaufgaben vorgeschaltet, wird die elektronische Rechnung **unnötig** weiter verkompliziert und verteuert.

Kurzum: Wenn man weiß, wie eine „Barcodesignatur“ funktioniert und bereit ist, die zusätzlichen Aufgaben dieses Verfahrens auch noch zu erbringen, ist dieses Verfahren theoretisch grundsätzlich anwendbar.

Man muss sich allerdings schon fragen, worin der Sinn liegen mag, ein bereits digital vorliegendes Objekt „aufs Papier“ zu bringen, um es anschließend wieder in die digitale Form zurück zu überführen und als solche aufzubewahren? Mir fallen wenig sinnvolle Erwägungen ein die für dieses Verfahren sprechen.

Für die elektronische Rechnung kann dieses Verfahren also nur in ganz exotischen Ausnahmefällen Sinn machen.

Ist der Empfänger nicht in der Lage oder Willens, die zusätzlichen Aufgaben im Zusammenhang mit dem 2D-Barcode zu erbringen, muss er dem elektronischen Rechnungsversand insgesamt für diesen Versender widersprechen.

Der Versender ist übrigens nicht befugt, für den dann notwendig werdenden Papierversand zusätzliche Gebühren oder sonstige Strafaktionen zu veranlassen, da der gewerbliche Empfänger einen Rechtsanspruch auf Abrechnung aus § 14 Abs. 2 UStG i. v. m. § 241 Abs. 2 BGB hat.

---

30 vgl. für viele nur Bunjes/Geist UStG, 8. Auflage, Seite 601, § 14Rd.20ff

31 Schreiben des Bundesministeriums der Finanzen an die obersten Finanzbehörden der Länder vom 7. November 1995 - IV A 8 - S 0316 - 52/95- BStBl 1995 I S. 738 Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS)

32 Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU) (BMF-Schreiben vom 16. Juli 2001 - IV D 2 - S 0316 - 136/01 -)

Eine zusätzliche Vergütung für die gesetzliche Verpflichtung des Versenders ist jedenfalls über AGB-Klauseln nach §§ 305ff BGB nicht wirksam zu vereinbaren und verstößt auch sonst gegen Treu und Glauben (§ 242 BGB). [33]

Newsletter abonnieren:

Monatlich aktuelle Informationen zum den Themen GDPdU, GoBS, elektronische Rechnungen.

http://www.elektronische-steuerpruefung.de/newsletter/a_newsletter.php4

[33] Entscheidung des AG- Brühl, vom 12.04.2006, 21C 612/05.