ZENTRALER KREDITAUSSCHUSS

MITGLIEDER: BUNDESVERBAND DER DEUTSCHEN VOLKSBANKEN UND RAIFFEISENBANKEN E.V. BERLIN · BUNDESVERBAND DEUTSCHER BANKEN E.V. BERLIN
BUNDESVERBAND ÖFFENTLICHER BANKEN DEUTSCHLANDS E.V. BERLIN · DEUTSCHER SPARKASSEN- UND GIROVERBAND E.V. BERLIN-BONN
VERBAND DEUTSCHER PFANDBRIEFBANKEN E.V. BERLIN

An den
Vorsitzenden des Finanzausschusses
des Deutschen Bundestages
Herrn Eduard Oswald, MdB
Platz der Republik 1
11011 Berlin

10178 Berlin, den 2. Oktober 2008
Burgstraße 28
AZ ZKA: STEUREG
AZ BdB: N 1.3 - Hm/Nf

Regierungsentwurf für ein Gesetz zur Modernisierung und Entbürokratisierung des Steuerverfahrens (Steuerbürokratieabbaugesetz)

Sehr geehrter Herr Oswald,

wir danken für die Gelegenheit, zum Regierungsentwurf eines Steuerbürokratieabbaugesetzes Stellung nehmen zu können.

Die im Zentralen Kreditausschuss (ZKA) vertretenen Verbände der Kreditwirtschaft befürworten ausdrücklich die Zielsetzung des Gesetzgebungsvorhabens, das Besteuerungsverfahren zu vereinfachen und zu entbürokratisieren. Dabei sollte sich der Gesetzentwurf nicht nur vorrangig auf die Ersetzung papierbasierter Verfahrensabläufe durch elektronische Kommunikation beschränken, sondern auch weitergehende Möglichkeiten der Entbürokratisierung und Vereinfachung im Rahmen des Besteuerungsverfahrens einbeziehen.

Von Seiten der Kreditinstitute besteht ein besonderes Interesse am Bürokratieabbau insbesondere auch auf dem Gebiet des Steuerrechts, da die Kreditwirtschaft zu den mit am höchsten regulierten Wirtschaftsbereichen zählt. Ein vom Zentralen Kreditausschuss beim unabhängigen Institut der Deutschen Wirtschaft in Auftrag gegebenes Gutachten hat Ende 2006 ergeben, dass die Bürokratiekosten durch allein der Kreditwirtschaft auferlegte Informationspflichten rund 3,1 Mrd € jährlich bzw. 4700 € je Mitarbeiter ausmachen. In diesen Kosten sind noch nicht die

aktuell für die Kreditwirtschaft aus der Umsetzung der Abgeltungsteuer resultierenden massiven Kosten enthalten. Diese machen deutlich, dass die Einführung der Abgeltungsteuer zum 1. Januar 2009 zwar zu einer wesentlichen Entlastung der Kapitalanleger und des Fiskus führt. Demgegenüber ist die Umsetzung und Administrierung der Abgeltungsteuer für die Kreditinstitute, die zukünftig die Hauptlast des Besteuerungsverfahrens in diesem Bereich zu tragen haben, mit weit reichenden bürokratischen Belastungen verbunden. Vor diesem Hintergrund besteht hier noch erhebliches Vereinfachungspotential und umfangreicher Nachbesserungsbedarf sowohl auf Gesetzgebungs- als auch auf Verwaltungsebene, um den Bemühungen der Kreditwirtschaft hinsichtlich einer möglichst praxisgerechten, einfachen und für alle Beteiligten nachvollziehbaren Umsetzung der Abgeltungsteuer zum Erfolg zu verhelfen.

Potential für Entbürokratisierung besteht nach Auffassung des ZKA auch beim Kontenabrufverfahren. Dieses ist über seine eigentliche Zielsetzung der Erfüllung aufsichtsrechtlicher Zwecke gemäß § 24 c KWG hinaus in ausufernder Weise sowohl zur Nutzung für steuerliche als auch für außersteuerliche Zwecke ausgeweitet worden. Hier sollte – wie von uns bereits in der Vergangenheit immer wieder vorgetragen – eine sachgerechte Eingrenzung des Verfahrens erfolgen. Soweit das Kontenabrufverfahren für aufsichtsfremde Zwecke weiterhin aufrechterhalten wird, muss den hiervon in Anspruch genommenen Kreditinstituten ein angemessener Kostenerstattungsanspruch eingeräumt werden.

Wir begrüßen ausdrücklich, dass die Verpflichtung zur Erstellung von Rechnungen, die die besonderen Anforderungen des Umsatzsteuerrechts erfüllen, bei Vorliegen steuerfreier Umsätze entfallen soll. Dies entspricht einer bereits während des Gesetzgebungsverfahrens zum Steueränderungsgesetz 2003 und auch danach immer wieder von der Kreditwirtschaft erhobenen Forderung.

Erfreulich ist hinsichtlich des Sonderausgabenabzugs nach § 10a EStG die Einfügung eines neuen Satz 4 in § 10a Abs. 2a EStG-E, wonach eine Einwilligung zur Datenübermittlung als erteilt angesehen wird, wenn der Zulageberechtigte den Anbieter nach § 89 Abs. 1a EStG bevollmächtigt hat. Somit wird unserem Petitum zum Referentenentwurf des Gesetzes entsprochen, dass neben der Bevollmächtigung nach § 89 Abs. 1a EStG keine zusätzliche Einwilligung nötig ist.

Unsere Anmerkungen zu den einzelnen Gesetzesvorschlägen haben wir in dem anliegenden Vermerk zusammengefasst verbunden mit der Bitte, diese im weiteren Gesetzgebungs-

verfahren zu berücksichtigen. Wir haben uns erlaubt, ein Exemplar unserer Stellungnahme dem Nationalen Normenkontrollrat zuzuleiten.

Mit freundlichen Grüßen
Für den Zentralen Kreditausschuss
Bundesverband deutscher Banken

Heinz-Udo Schaap

Wolfgang Skorpel

Anlage

- Anlage -

zur Stellungnahme des Zentralen Kreditausschusses vom 2. Oktober 2008 zum Regierungsentwurf eines Steuerbürokratieabbaugesetzes

I. Anmerkungen zu den Gesetzesvorschlägen

I.1 Zu Artikel 1, Nr. 2 - § 5 b Abs. 1 EStG-E

Petitum:

Auf die obligatorische Verpflichtung zur elektronischen Übermittlung von Bilanzen, Gewinn- und Verlustrechungen und Steuererklärungen sollte verzichtet werden. Es sollte allenfalls eine fakultative Möglichkeit der elektronischen Übermittlung eingeführt werden.

Begründung:

In § 5b Abs. 1 EStG-E wird vorgeschlagen, obligatorisch den Inhalt der Bilanz sowie der Gewinn- und Verlustrechnung durch Datenfernübertragung nach amtlich vorgeschriebenem Datensatz zu übermitteln. Steuerlich notwendige Anpassungen sind durch Zusätze bzw. Anmerkungen kenntlich zu machen und auf dem gleichen Weg zu übertragen. Alternativ kann auch eine Steuerbilanz elektronisch übermittelt werden.

Auch wenn im Gegensatz zum Referentenentwurf die obligatorische Übermittlung einer Steuerbilanz nicht mehr erforderlich ist, indem die in § 60 Abs. 2 EStDV enthaltenen Regelungen in § 5 b Abs. 1 EStG-E übernommen wurden, bestehen gegen den Vorschlag in der vorliegenden Form grundsätzliche Bedenken.

Die bloße elektronische Übermittlung der ergänzten Handelsbilanz oder Steuerbilanz macht keinen Sinn. Sie ist für die Finanzverwaltung bei großen Unternehmen ohne das Hinzufügen weiterer Unterlagen, insbesondere von Wirtschaftprüfungsberichten oder weiteren Erläuterungsteilen in der Praxis nicht nutzbar. Sowohl für die Handelsbilanz als auch für die Steuerbilanz ist festzustellen, dass die geforderte elektronische Übermittlung für die Unternehmen zu unangemessenen Zusatzkosten führen würde, wenn diese nach Vorgaben, die erst noch in einer Durchführungsverordnung vorgeschrieben werden sollen, zu erstellen und übermitteln sind.

Auch für Steuererklärungen größerer Unternehmen wird die in § 31 Abs.1a KStG-E, § 14a GewStG-E, 3 181 Abs.2a AO-E, § 25 Abs. 4 EStG-E vorgesehene standardmäßige elektronische Übermittlung keine (Kosten-)Vorteile bringen. Die Komplexität der Steuervorschriften lässt eine Standardisierung praktisch nicht zu, denn die Steuerformulare sind in der Praxis regelmäßig um manuelle Anlagen zu ergänzen. Wegen der Besonderheiten einzelner Wirtschaftszweige erscheint eine Universalvorlage nicht möglich, sondern es dürften eine Reihe verschiedener Vorlagen erforderlich sein, was das Verfahren sicher nicht vereinfacht. Die Standardisierung der Angaben würde bei den Unternehmen eine kostenintensive Systemanpassung (Umstellung, Prüfung, Tests) voraussetzen, die auch Sicherheitsanforderungen beinhaltet, denn ein Missbrauch der elektronischen Daten oder eine Beeinträchtigung des unternehmenseigenen EDV-Systems durch die elektronische Übermittlung müsste ausgeschlossen werden. So erscheint entgegen der Intention des Entwurfs aus unserer Sicht in den allermeisten Fällen allein die Finanzverwaltung als Nutznießer der vorgesehenen Änderungen. Aus diesem Grunde sollte die elektronische Übermittlung lediglich fakultativ vorgesehen werden. Der im Gesetzentwurf enthaltene Verzicht auf die elektronische Übermittlung zur Vermeidung unbilliger Härten reicht nicht aus, weil er im Ermessen der Finanzverwaltung steht und für größere Unternehmen regelmäßig nicht erfolgen dürfte. Die Tatsache, dass 20 % der privaten Einkommensteuererklärungen nach dem ELSTER-Verfahren bereits in elektronischer Form abgegeben werden, ist unseres Erachtens kein ausreichender Grund

für eine obligatorische elektronische Übermittlung sämtlicher Steuererklärungen, da sich die Situation im Unternehmensbereich hiervon unterscheidet.

I.2 Zu Artikel 8, Nr. 1a - § 14 Abs. 2 Satz 1 Nr. 2 UStG-E

Wir begrüßen, dass die Verpflichtung zur Erstellung von Rechnungen, die die besonderen Anforderungen des Umsatzsteuerrechts erfüllen, bei steuerfreien Umsätzen entfallen soll.

Begründung:

Mit § 14 Abs. 2 Satz 1 Nr. 2 UStG-E wird vorgeschlagen, dass die Verpflichtung zur Erstellung von Rechnungen, die die besonderen Anforderungen des Umsatzsteuerrechts erfüllen, bei steuerfreien Umsätzen entfallen soll. Hiermit wird von dem Mitgliedstaatenwahlrecht des Artikels 221 MwStSystRL Gebrauch gemacht, wie dies bereits von vornherein in fast allen anderen EU-Mitgliedstaaten geschehen ist. Wir begrüßen diese Maßnahme, da sie einer bereits seit langem regelmäßig von der Kreditwirtschaft erhobenen Forderung entspricht.

I.3 Zu Artikel 8, Nr. 1b - § 14 Abs. 3 Nr. 2 UStG-E

Wir begrüßen, dass die Verpflichtung zur Übermittlung einer zusammenfassenden Rechnung (Sammelrechnung) bei Übermittlung der Rechnungen über elektronischen Datenaustausch (EDI) entfallen soll.

Begründung:

Mit § 14 Abs. 3 Nr. 2 UStG-E wird vorgeschlagen, bei Rechnungen, die mittels EDI-Verfahren übermittelt werden, auf eine zusätzliche zusammenfassende Rechnung, die auf

Papier oder elektronisch mit qualifizierter elektronischer Signatur übermittelt werden muss, zu verzichten. Dies wird zwar dem Ziel der Entbürokratisierung gerecht und stellt auch eine Vereinfachung für die Praxis dar. Generell aber hat der deutsche Gesetzgeber die Möglicheiten des Artikels 233 MwStSystRL nicht zu Zwecken der Vereinfachung und Modernisierung der Anforderungen an die elektronische Rechnungsstellung ausgeübt.

Die strengen Voraussetzungen für die elektronische Rechnungsstellung in Deutschland, insbesondere das Erfordernis einer qualifizierten elektronischen Signatur, stellen ein enormes Hindernis für die breitere Nutzung in der Praxis dar. Nicht zuletzt auch um dem zunehmenden grenzüberschreitenden Handel in unserem elektronischen Zeitalter gerecht zu werden, muss auch der deutsche Gesetzgeber von der Möglichkeit der MwStSystRL Gebrauch machen, dass Rechnungen auch auf andere Weise elektronisch übermittelt werden können. Der ZKA hat hierzu bereits vor einiger Zeit das Verfahren des so genannten „Elektronischen Siegels“ entwickelt, dass die Authentizität und Integrität von elektronisch übermittelten Dokumenten sicherstellt. Wir verweisen in diesem Zusammenhang auf unsere Ausführungen unter Ziffer I.4. Es ist daher dringend erforderlich, dass im Hinblick auf die elektronische Rechnungsstellung weitere Maßnahmen folgen, die sowohl den Sicherheitsanforderungen gerecht werden als auch für die Unternehmen praktikabel und ohne großen Verwaltungsaufwand umsetzbar sind.

I.4 Zu Artikel 9, Nr. 2 - § 150 Abs. 2 Nr. 7 AO-E (Verwendung anderer sicherer Verfahren anstelle der qualifizierten elektronischen Signatur)

Petitum:

Die Verwendung anderer sicherer Verfahren anstelle der qualifizierten elektronischen Signatur nach dem Signaturgesetz sollte nicht nur auf die Übermittlung von Steuererklärungen beschränkt werden, sondern auch auf die Übermittlung sonstiger steuerrelevanter Dokumente, wie beispielsweise Kontoauszüge für Zwecke der DV-gestützten Buchführung des Empfängers und Rechnungen für Zwecke der Umsatzsteuer, ausgedehnt werden. In diesem Zusammenhang sollte insbesondere das so genannte „Elektronische Siegel" als ein solches sicheres Verfahren anerkannt werden.

Begründung:

Der Entwurf sieht vor, dass bei Übermittlung von Steuererklärungen nach amtlich vorgeschriebenem Datensatz durch Datenfernübertragung anstelle der Sicherung des Datensatzes mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz von der Finanzverwaltung ein anderes sicheres Verfahren zugelassen werden kann, das die Authentizität und Integrität des elektronisch übermittelten Dokuments sicherstellt. Darüber hinaus wäre eine zeitnahe Spezifizierung des Begriffs „anderes sicheres Verfahren" wünschenswert. Die hiermit eingeräumte Möglichkeit sollte sich nicht nur auf die Übermittlung von Steuererklärungen erstrecken, sondern auch auf die Übermittlung weiterer steuerrelevanter Dokumente, wie etwa der elektronischen Übermittlung von Kontoauszügen für Zwecke der DV-gestützten Buchführung des Empfängers sowie auch der elektronischen Übermittlung von umsatzsteuerrelevanten Rechnungen, ausgedehnt werden.

Qualifizierte elektronische Signaturen nach dem Signaturgesetz sind definitionsgemäß an eine bestimmte natürliche Person gebunden und damit in der Praxis, gerade im wirtschaft-

lichen Massenverkehr, nur eingeschränkt verwendbar. Eine wesentliche Erleichterung würde ein Verfahren bewirken, bei dem eine elektronische Signatur – bei gleichen Sicherheitsanforderungen – lediglich auf eine Organisation, beispielsweise eine juristische Person, die in einem geeigneten Register eingetragen ist, ausgestellt werden könnte.

Der ZKA hat hierzu bereits vor einiger Zeit ein entsprechendes Verfahren in Gestalt eines sogenannten „Elektronischen Siegels" entwickelt, das die vorgenannten Sicherheitsanforderungen erfüllt. Die Einzelheiten dieses Verfahrens sind in dem als Anhang beigefügten Konzept vom 02.08.2007 zusammengefasst, auf das wir zur Vermeidung von Wiederholungen verweisen. Der ZKA hatte sich hierzu bereits in der Vergangenheit gegenüber dem BMF – vorrangig zunächst bezogen auf elektronische Kontoauszüge im Bereich der DV-gestützten Buchführung – um Ankerkennung des Verfahrens bemüht. Diese Bemühungen sind allerdings bisher ohne Ergebnis geblieben, so dass der Druck aus der Praxis stetig wächst, hier eine Lösung zu finden.

II. Weiterer Regelungsbedarf

II.1 Kontenabrufverfahren für steuerliche und außersteuerliche Zwecke (§§ 93 Abs. 7, 93 a AO)

Petitum:

Es sollte – wie von uns bereits in der Vergangenheit immer wieder vorgetragen – eine sachgerechte Eingrenzung des Anwendungsbereichs des Verfahrens erfolgen. Soweit das Kontenabrufverfahren für die vorgenannten Zwecke teilweise aufrecht erhalten werden sollte, muss den hiervon in Anspruch genommenen Kreditinstituten zumindest ein angemessener Kostenerstattungsanspruch eingeräumt werden.

Begründung:

Potential für Entbürokratisierung besteht nach Auffassung des ZKA beim Kontenabrufverfahren. Dieses ist über seine eigentliche Zielsetzung, die Erfüllung aufsichtsrechtlicher Zwecke gemäß § 24 c KWG, in ausufernder Weise sowohl zur Nutzung für steuerliche als auch für außersteuerliche Zwecke ausgeweitet worden.

Ungeachtet der Tatsache, dass das Verfahren ursprünglich allein für die Bekämpfung schwerster Kriminalität, des Terrorismus und der Geldwäsche konzipiert war, hat es sich inzwischen zu einem routinemäßig eingesetzten Ermittlungsinstrument der Strafverfolgungs-, Steuer- und Sozialbehörden entwickelt. Dies belegen die zur Nutzung des Kontenabrufverfahrens veröffentlichten Angaben. Danach hat sich die Zahl der Abrufe durch die abrufberechtigten Stellen seit Einrichtung des Verfahrens kontinuierlich gesteigert und lag zuletzt im Jahr 2007 bei insgesamt 121.309 Abfragen. Der ganz überwiegende Anteil der Abfragen hat dabei keinen bankaufsichtlichen Hintergrund. Insgesamt 92.341 (rund 76%) wurden von Strafverfolgungsbehörden (einschließlich Zoll und Finanzbehörden in Strafsachen) und 27.749 Anfragen (rund 23%) von Sozialbehörden bzw. Finanzbehörden in Steuersachen veranlasst. Weniger als 500 Abfragen,

also unter 0,4%, wurden durch die BaFin im Rahmen ihrer Aufsichtstätigkeit initiiert.[1] Obwohl das Verfahren ganz überwiegend nicht bankaufsichtlichen Zwecken dient, wird der Betrieb des Verfahrens vollständig von der Kreditwirtschaft finanziert. Auch die Einrichtung der technischen Infrastruktur, die Kosten von über 100 Mio € verursacht hat, wurde allein von der Kreditwirtschaft getragen. Eine solche entschädigungslose Inpflichtnahme der Kreditwirtschaft für öffentliche Zwecke stößt auf grundsätzliche rechtliche Bedenken.

II.2. Ergänzung von § 118 Abs. 3 und 4 SGB VI: Modifikation der Rücküberweisungs- und Auskunftspflichten

Petitum:

In § 118 Abs. 3 S. 3 SGB VI müssten nach den Worten „anderweitig verfügt wurde" die Worte „unabhängig davon, ob das Konto zum Zeitpunkt der Verfügung im Debet oder im Haben geführt wurde" eingefügt werden. In § 118 Abs. 4 S. 4 SGB VI sollten die Worte „Empfängers oder" gestrichen werden. § 96 Abs. 3 und 4 SGB VII, § 12 Abs. 3 Bundesbesoldungsgesetz sowie § 52 Abs. 4 Beamtenversorgungsgesetz sind entsprechend zu ergänzen.

Mindestens muss § 118 Absatz 3 SGB VI um folgenden Satz 5 erweitert werden: „§ 21 Absatz 3 Satz 4 des Zehnten Buches gilt entsprechend" Der gleiche Satz sollte in § 118 Absatz 4 als neuer Satz 5 eingefügt werden.

Begründung:

Die genannten Vorschriften normieren für Kreditinstitute eine Rückzahlungs- und Auskunftsverpflichtung hinsichtlich überzahlter Rentenleistungen. Hiernach haben die Institute die für die Zeit nach dem Tod des Rentenberechtigten überwiesenen Geldleistungen der überweisenden Stelle oder den Trägern der Rentenversicherung zurück zu überweisen, wenn diese sie als zu Unrecht erbracht zurückfordern. Soweit über den entsprechenden Betrag bei Eingang der Rückforderung bereits anderweitig verfügt wurde,

[1] Die Zahlen beruhen auf in der Presse veröffentlichten Angaben der BaFin und des Bundesministeriums der Finanzen: siehe Börsenzeitung vom 30. Januar 2008, S.4, sowie dem Jahresbericht der BaFin für 2007.

besteht die Verpflichtung zur Rücküberweisung nicht. In diesem Fall hat jedoch das Kreditinstitut der überweisenden Stelle oder dem Träger der Rentenversicherung auf Verlangen Namen und Anschrift des Empfängers oder Verfügenden oder etwaiger neuer Kontoinhaber zu benennen.

Die zeitaufwändige Bearbeitung der Rückzahlungs- und Auskunftsersuchen durch die Institute verursacht erhebliche Kosten (ca. 25 Mio € p. a. für die gesamte Kreditwirtschaft), die – obwohl die Maßnahmen ausschließlich auf Anforderung und im Interesse staatlicher Stellen erfolgen – den Instituten nicht erstattet werden.

Die durch diese Vorschrift den Kreditinstituten entstehenden bürokratischen Belastungen könnten durch zwei Änderungen entscheidend reduziert werden: Zum einen sollte klargestellt werden, dass eine Rücküberweisungspflicht gemäß § 118 Abs. 3 S. 3 SGB VI in dem Fall, dass über den betreffenden Betrag bereits anderweitig verfügt wurde, unabhängig davon entfällt, ob das Konto zum Zeitpunkt dieser Verfügung im Debet oder im Haben geführt wurde. Hierdurch könnte die ansonsten erforderliche – und außerordentlich aufwendige – nachträgliche Ermittlung aller Kontobewegungen zwischen dem Zeitpunkt der Gutschrift der Rentenzahlung und des Rückforderungsverlangen entfallen. Ferner sollte die Auskunftspflicht in § 118 Abs. 4 S 4 SGB VI, die sich derzeit nicht nur auf Name und Anschrift des Verfügenden, sondern auch des Empfängers erstreckt, auf Ersteren beschränkt werden. Denn dem nach dieser Regelung verpflichteten Kreditinstitut sind Name und insbesondere Anschrift des Überweisungsempfängers in der Regel nicht bekannt. Aus rechtlichen Gründen können diese Informationen zumindest regelmäßig auch nicht vom Kreditinstitut, welches das Konto führt, auf dem die Zahlung eingegangen ist, angefordert werden. Zur Vermeidung von Wertungswidersprüchen müssten zudem auch die – vom Wortlaut her entsprechend ausgestalteten – Normen in den spezialgesetzlichen Parallelvorschriften (z. B. § 12 Bundesbesoldungsgesetz) angepasst werden.

Sofern die Änderungsvorschläge nicht umgesetzt werden, müsste – ebenso wie beispielsweise in § 60 Absatz 2 Satz 2 SGB II sowie in § 117 Absatz 3 Satz 2 SGB XII – zumindest eine Entschädigung der Kreditinstitute in entsprechender Anwendung des Justizvergütungs- und -entschädigungsgesetzes (JVEG) vorgesehen werden.

II.3 Anzeigepflicht der Vermögensverwahrer und Vermögensverwalter nach § 1 ErbStDV

Petitum:
Die in § 1 Abs. 4 Nr. 2 ErbStDV normierte Ausnahme von der Anzeigepflicht sollte auf einen Betrag von 10.000 € erhöht werden.

Begründung:

Gemäß § 33 Abs. 1 ErbStG sind Kreditinstitute in ihrer Eigenschaft als Vermögensverwahrer und –verwalter dazu verpflichtet, sämtliche bei ihnen in Gewahrsam befindlichen Vermögensgegenstände des Erblassers sowie die gegen sie gerichteten Forderungen dem zuständigen Finanzamt anzuzeigen. Eine Anzeige darf nur unterbleiben, wenn der Wert der anzuzeigenden Wirtschaftsgüter 2.500 € nicht übersteigt. Anzugeben ist der Vermögensstand vom Todestag inklusive der bis zu diesem Zeitpunkt entstandenen „Stückzinsen". Die Verpflichtung zur Abgabe der sog. Todesfallanzeige stellt nach wie vor für die Kreditinstitute einen erheblichen Verwaltungsaufwand dar, der insbesondere deshalb unverhältnismäßig erscheint, weil in der überwiegenden Anzahl der Fälle wegen der Höhe der erbschaftsteuerlichen Freibeträge tatsächlich keine Erbschaftsteuer anfällt. Auf die Kosten von 89 Mio € jährlich hatten wir mittels des vom ZKA in Auftrag gegebenen Gutachtens vom 12.12.2006 bereits hingewiesen. Eine deutliche Erleichterung würde eine weitere Anhebung der Freigrenze bringen. So hatten wir bereits Anfang des Jahres 2007 eine Anhebung der Freigrenze auf mind. 5.000 € gefordert, die nach unserem Dafürhalten auch den Interessen des Fiskus an einer vollständigen Erfassung des der Erbschaftsteuer unterliegenden Vermögens nicht zuwiderliefe, da bereits der kleinste persönliche Freibetrag 5.200 € beträgt. Zudem bewegen sich nach Erhebungen aus der Praxis mehr als ein Drittel der zu meldenden Guthaben im Bereich bis 10.000 €.

Schon in unserer Eingabe vom 23.01.2007 hatten wir auf die europarechtliche Brisanz hingewiesen, die darin besteht, dass sich die Verpflichtung für inländische Vermögensverwahrer und –verwalter in § 33 Abs. 1 ErbStG, das verwahrte oder verwaltete Vermögen nach dem Tod des Kunden dem zuständigen Finanzamt anzuzeigen, nach Rechtsprechung und Verwaltungsauffassung[2] auch auf ausländische Zweigniederlassungen (Betriebsstätten) inländischer Kreditinstitute erstreckt. Dabei wird formalrechtlich allein auf das nationale deutsche Steuerrecht abgestellt und zwar auch und gerade für

[2] Vgl. BFH-Urteil vom 31. Mai 2006, II R 66/04 sowie BMF-Schreiben v. 21. März 2001, IV C 7 – S 3844 – 6/01.

den Fall einer Kollision mit dem ausländischen Recht. In anderen Ländern wie z. B. Luxemburg, Österreich und der Schweiz ist es Mitarbeitern von Kreditinstituten jedoch grundsätzlich untersagt, Angaben über Kundenkonten und -depots zu machen. Nur ausnahmsweise sind Auskünfte auf nationaler gesetzlicher Grundlage zu erteilen (z. B. in Fällen der EU-Zinsrichtlinie für die Einkommensbesteuerung von Kapitalerträgen ausländischer Anleger und beim Steuerbetrug). Soweit der BFH im oben genannten Urteil zudem anführt, dass „lediglich hausinterne Informationen angefordert werden", geht dies fehl, denn es handelt sich um verwahrtes und verwaltetes Vermögen des Erblassers, also um Kundendaten und nicht um solche, die die ausländische Zweigniederlassung des Kreditinstituts selbst betreffen.

Die dargestellte Rechtslage ist höchst unbefriedigend und kann mittelbar zu Wettbewerbsnachteilen deutscher Institute im Verhältnis zu ausländischen Instituten führen, weil deutsche Kunden das Urteil zum Anlass nehmen könnten, das verwahrte und verwaltete Vermögen von der ausländischen Zweigniederlassung des deutschen Instituts auf ein im Ausland ansässiges Institut zu übertragen.

Der Europäische Gerichtshof konnte die Entscheidung des BFH damals nicht auf der Grundlage der Grundfreiheiten des EG-Vertrages auf ihre europarechtliche Vereinbarkeit überprüfen, weil das vor dem BFH unterlegene deutsche Kreditinstitut keine Rechtsmittel gegen das Urteil eingelegt hatte. Mit Blick auf die Fortentwicklung des EG-Binnenmarktes bleibt aber weiterhin perspektivisch die Frage zu stellen, ob es nicht einer EU-Regelung betreffend einer Anzeigepflicht auf dem Gebiet der Erbschaftsteuer bedarf, die das Problem möglicher bestehender Kollisionen der nationalen Rechte der EU-Mitgliedstaaten bzw. im Verhältnis zu bestimmten Drittstaaten beseitigt. Solange eine solche Regelung nicht besteht, sollte die Anzeigepflicht der Kreditinstitute auf Länder beschränkt werden, in denen kein rechtlicher Konflikt besteht.

II.4 Geplante Änderung der R 5.5 EStR

Petitum:
Die geplante Änderung der R 5.5 EStR sollte unterbleiben.

Begründung:

Nach dem Entwurf einer Allgemeinen Verwaltungsvorschrift zur Änderung der Einkommensteuer-Richtlinien 2005 soll R 5.5 Abs. 1 Satz 3 EStR dahingehend geändert werden, dass die Angabe "410 Euro" durch die Angabe "150 Euro" ersetzt wird.

Die Einkommensteuerrichtlinien sehen bisher vor, dass Computerprogramme, deren Anschaffungskosten nicht mehr als 410 € betragen, wie Trivialprogramme zu behandeln sind. Die Änderung würde dazu führen, dass Computerprogramme ab 2008 nur noch bei Anschaffungskosten bis 150 € als Trivialprogramme und somit als bewegliche WG gelten würden, R 5.5 Abs. 1 Satz 2 EStR.

Die Unternehmen hatten im Rahmen des Gesetzgebungsprozesses zum Unternehmensteuergesetztes 2008 bereits mehrfach auf die mit der Reduzierung des Betrages der geringwertigen Wirtschaftsgüter einhergehenden Bürokratiekosten hingewiesen, sich aber dem vermeintlichen „Gegenfinanzierungsdruck der Reform" beugen müssen. Mit der beabsichtigten Änderung der Einkommensteuer-Richtlinien soll jedoch über dies ohne Not in die bewährte Fiktion für Computerprogramme eingegriffen werden, was zu einer signifikanten Steigerung des Bürokratieaufwands führen würde. Die geplante Änderung hätte zur Folge, dass jedes Computerprogramm mit Anschaffungskosten über 150 €, einzeln zu aktivieren und abzuschreiben wäre.

Wegen der erheblichen bürokratischen Mehraufwendungen wäre es daher zu begrüßen, wenn die bisherige Grenze von 410 € nicht auf 150 € herab- sondern auf 1.000 € heraufgesetzt würde. Dies würde es ermöglichen, Computerprogramme mit Anschaffungskosten, die zwischen 150 € und 1.000 € liegen, in den Sammelposten einzubeziehen und über fünf Jahre abzuschreiben. Für den Fiskus wären mit der Anhebung des Betrages nach unserer Einschätzung keine Steuermindereinnahmen verbunden, denn Computerprogramme mit Anschaffungskosten zwischen 150 € und 1.000 € werden in der Praxis regelmäßig über einen Zeitraum von drei Jahren, nicht aber über einen Zeitraum von mehr als fünf Jahren abgeschrieben.

Wenigstens aber sollte die bisherige Grenze von 410 € beibehalten werden, denn allein die Tatsache, dass ab 2008 gemäß § 6 Abs. 2 EStG eine neue Regelung für geringwertige Wirtschaftsgüter gilt, ist keine ausreichende Begründung dafür, die Fiktion für Computerprogramme zu beschränken.

Anhang

Der elektronische Kontoauszug im Bereich der DV-gestützten Buchführung

Zentraler Kreditausschuss

2. August 2007

Inhalt

1. Zielsetzung

Der Zentrale Kreditausschuss hat mit dem DFÜ-Verfahren und dem FinTS-Standard zwei multibankfähige Electronic-Banking-Standards geschaffen, über die in Zukunft den Kunden der Kreditinstitute elektronische Kontoauszüge zur Verfügung gestellt werden sollen. Diese Multibankfähigkeit kann nur erhalten werden, wenn der Zentrale Kreditausschuss das Datenaustauschformat für den elektronischen Kontoauszug und Mindestanforderungen an die Absicherung des elektronischen Kontoauszugs einheitlich festlegt.

Es ist erklärtes Ziel des Zentralen Kreditausschusses, dass diese Anforderungen im Vorfeld der Veröffentlichung der entsprechenden Standards mit der Finanzverwaltung abgestimmt werden.

Mit diesem Dokument sollen die Grundlagen für die Akzeptanz eines „Elektronischen Kontoauszugs" durch die Finanzbehörden – insbesondere bei Betriebsprüfungen - geschaffen werden (Nichtbeanstandungsregelung).

2. Ausgangssituation

Die Vertrauenswürdigkeit, Qualität und Akzeptanz des elektronischen Geschäftsverkehrs wird zukünftig ein entscheidendes Kriterium für den Erfolg aller im Wettbewerb stehenden Unternehmen und Organisationen, d.h. auch von staatlichen Institutionen, sein. Dies belegt das in der öffentlichen Verwaltung vorhandene Bestreben, Verwaltungsabläufe in weitem Umfang für die elektronische Abwicklung zu öffnen (im Bereich der Finanzverwaltung z.B. durch das ELSTER-Projekt). Für den Bereich des Versandes von Kontoauszügen durch Kreditinstitute an ihre Kunden bedeutet dies, dass elektronische Kontoauszüge, deren Authentizität sichergestellt ist, einen wesentlichen Beitrag zur Verfahrensvereinfachung für alle Beteiligten leisten könnten, weil die enthaltenen Informationen direkt in die Datenverarbeitung der Kunden eingespeist würden und die digitalen Unterlagen für die Betriebsprüfung zur Verfügung stünden. Ein Medienbruch, der immer mit zusätzlichem Aufwand verbunden ist, würde so vermieden.

Eine wesentliche Voraussetzung für den verlässlichen Einsatz des elektronischen Geschäftsverkehrs ist die praktikable und interoperable Nutzung von zertifikatsbasierten Verschlüsselungs-, Authentifizierungs- und Signaturanwendungen. Die eingesetzten elektronischen Zertifikate sind von vertrauenswürdigen Instanzen (Trustcenter) signierte Informationen zur Kennzeichnung der Identität der Kommunikationspartner (natürliche Personen oder Organisationen) und ermöglichen somit die verlässliche Kommunikation in offenen Netzen.

Die bisher vorhandenen rechtlichen Lösungen erfassen nur Teilbereiche des elektronischen Geschäftsverkehrs oder erfüllen noch nicht die Anforderungen, die an elektronische Dokumente gestellt werden:

- Die durch das Signaturgesetz geregelten „qualifizierten Zertifikate" für natürliche Personen sichern dem darauf vertrauenden Kommunikationspartner einen hohen Beweiswert, für juristische Personen werden dort keine Festlegungen getroffen. Die bisherigen Ansätze zur Abbildung eines vergleichbaren Beweiswerts für den Bereich der Repräsentation der Identität eines Unternehmens, der Öffentlichen Verwaltung oder anderer juristischer Personen durch pseudonymisierte qualifizierte Zertifikate natürlicher Personen haben den Nachteil, dass bei der Verweigerung, dem Ableben oder Ausscheiden der Person aus der Organisation keine Signaturen mehr geleistet werden können.

- Serverzertifikate sind Stand der Technik und werden millionenfach eingesetzt, sie dienen der Verschlüsselung bei der Datenübermittlung und lassen die Identität der Internet-Adresse einer Organisation erkennen. In der jüngeren Vergangenheit wurden hierfür von den internationalen – vorwiegend US-amerikanischen Trustcentern – sogenannte „Extended Validation Certificates" definiert, die verschärfte Anforderungen an die Prüfung der Identität einer Organisation in einem elektronischen SSL-Zertifikat stellen. Jedoch gibt es bis dato keine allgemein anerkannte Rechtsgrundlage, die eine Zurechenbarkeit entsprechender Zertifikate im Sinne der Authentisierung des Inhalts regeln würde.

- Der ausschließliche Schutz vor Veränderungen des Dokuments und zur Authentizität desselben über entsprechende Dateiformate (z.B. pdf-Format) wird von Seiten der Verwaltung bisher als nicht ausreichend angesehen (vgl. zu elektronischen Kontoauszügen das BMF-Schreiben vom 27.10.2004, Az.: IV A 7 – S 0317 – 7/04).

3. Handlungsbedarf

Nach den Grundsätzen ordnungsmäßiger Buchführung werden erhöhte Anforderungen an die Art und Weise der Aufzeichnung von Geschäftsvorfällen und Aufbewahrungspflichten von Unterlagen gestellt. Diese Anforderungen gelten für buchführungspflichtige Unternehmen.

Insbesondere müssen buchungspflichtige Geschäftsvorfälle nach den Grundsätzen ordnungsmäßiger Buchführung richtig, vollständig und zeitgerecht erfasst sein sowie sich in ihrer Entstehung und Abwicklung verfolgen lassen (Beleg- und Journalfunktion). Die Grundsätze ordnungsmäßiger Buchführung (GoB) werden für den Bereich der Computer-gestützten Buchführung durch die sogenannten „Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme"[1] (GoBS) präzisiert. Ergänzend gelten für die Archivierung und Aufbewahrung steuerrelevanter digitaler Unterlagen die Anforderungen der „Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen"[2] (GDPdU).

Insbesondere fordern die GDPdU, dass die Echtheit der Herkunft (Authentizität) und die Unveränderbarkeit des Inhalts (Integrität) der digitalen Daten gewährleistet werden müssen. Weitere Vorgaben werden von der Finanzverwaltung nicht formuliert.

[1] BMF-Schreiben vom 7. November 1995, IV A 8 – S 0316 – 52/95; BStBl. I S. 738
[2] BMF-Schreiben vom 16. Juli 2001, IV D 2 – S 0316 – 136/01; BStBl. I S. 415

Bei elektronischer Übermittlung von Kontoauszügen für Zwecke der DV-gestützten Buchführung ist daher sicherzustellen, dass die Echtheit der Herkunft sowie die Unveränderbarkeit des Inhalts der Daten gewährleistet sind.

Aus Sicht des Zentralen Kreditausschusses können diese Anforderungen durch den Einsatz eines so genannten „elektronischen Siegels" (siehe Abschnitt 5) erfüllt werden. Dieses ermöglicht es, dass der Empfänger eines elektronischen Kontoauszugs auf die Integrität und die Urheberschaft durch die im Zertifikat bezeichnete Organisation (das Kreditinstitut) vertrauen kann. Da das elektronische Siegel für die Organisation und nicht für eine natürliche Person ausgestellt wird, stellt die Organisation durch entsprechende ablauforganisatorische Regelungen und Maßnahmen sicher, dass die Verwendung des Siegels im Namen der Organisation nur dazu berechtigten Personen oder Organisationseinheiten möglich ist. Eine personengebundene, qualifizierte elektronische Signatur wird nicht als erforderlich angesehen.

5. Definition des elektronischen Siegels

5.1. Technische Beschreibung

Elektronische Siegel sind Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder mit ihnen logisch verknüpft sind und zur Authentisierung dienen.

Elektronische Siegel

a) werden für Organisationen ausgestellt. Dies sind beispielsweise juristische Personen, die in einem geeigneten Register[4] eingetragen sind[5] sowie juristische Personen des öffentlichen Rechts, z. B. Behörden

b) ermöglichen eine Identifizierung der Organisation und

c) sind so mit den beigefügten oder verknüpften Daten verbunden, dass nachträgliche Veränderungen erkannt werden können.

Im technischen Sinne wird ein Elektronisches Siegel durch eine elektronische Signatur geleistet, bei der über den öffentlichen Signaturprüfschlüssel ein Organisationszertifikat ausgestellt wird.

Neben den technischen Festlegungen hinsichtlich der unterstützten Standards müssen insbesondere auch die Sicherheitsanforderungen an die geeigneten Algorithmen sowie die von dem Zertifikatsherausgeber zu berücksichtigenden Sicherheitsanforderungen festgelegt werden. Diese Anforderungen wurden im Signaturbündnis der Bundesregierung abgestimmt und in dem Dokument „Spezifikation der Vorgaben und Empfehlungen zum Einsatz von Organisationszertifikaten, Version 1.0.a vom 24. Mai 2006" zusammengefasst (siehe **Anlage**).

---

4 Unternehmensregister, Handelsregister, Vereinsregister, Handwerksrolle, IHK-Firmenspiegel etc.

5 Im folgenden Text wird der Einfachheit halber nur der Begriff der Organisation für den hier definierten Kreis juristischer Personen genutzt.

Daher muss derzeit jeweils im Einzelfall im Rahmen der Betriebsprüfung entschieden werden, unter welchen technischen Voraussetzungen elektronische Kontoauszüge, die keine Rechnungen im Sinne des Umsatzsteuerrechts sind, als originär digitale Daten GoBS-/GDPdU-konform übertragen, gespeichert und aufbewahrt werden können. Die Einzelbeurteilungen der Finanzverwaltungen vor Ort können derzeit durchaus Unterschiede aufweisen. Dies widerspricht der Anforderung der Kreditwirtschaft, multibankfähige Standards zu schaffen, die von den Kunden der Kreditinstitute bundesweit einheitlich genutzt werden können.

4. Schutzbedarf des elektronischen Kontoauszugs

Im Folgenden wird der Schutzbedarf für den elektronischen Kontoauszug als Beleg im Hinblick auf die Schutzziele „Vertraulichkeit", „Integrität", „Authentizität" und „Verbindlichkeit" ermittelt. Dem BSI Grundschutzhandbuch[3] folgend wird eine Einstufung in die Klassen „niedrig bis mittel", „hoch" und „sehr hoch" vorgenommen.

Elektronische Kontoauszüge unterliegen als „originär digitale Daten" – sofern sie steuerrelevant sind – den Anforderungen nach den §§ 145 ff. AO, den GoBS und den GDPdU. Spezialgesetzliche Vorschriften wie das Umsatzsteuergesetz bleiben hiervon unberührt.

Das Verfahren zur Speicherung und Archivierung von originär digitalen Dokumenten muss nach den GoBS (vgl. Abschnitt VIII Buchst. b Satz 4 Nr. 2 der GoBS a.a.O.) insbesondere sicherstellen, dass während des Übertragungsvorgangs auf das Speichermedium eine Bearbeitung nicht möglich ist (vgl. auch Abschnitt II.2 und III Nr. 1 der GDPdU a.a.O.).

Neben dem Schutzziel „Authentizität" steht bei Belegen für Zwecke der manuellen und DV-gestützten Buchführung somit das Schutzziel „Integrität" im Vordergrund. Insoweit ist der Schutzbedarf als „hoch" anzusehen und eine detaillierte Risikoanalyse vorzunehmen.

Demgegenüber kommt dem elektronischen Kontoauszug als Beleg für die Buchführung eine „Verbindlichkeit" im Sinne einer persönlichen Willenserklärung („Unterzeichnen") nicht zu. Zum Schutzziel „Vertraulichkeit" werden in den o.g. Vorgaben der Finanzverwaltung keine gesonderten Anforderungen gestellt. Demgemäß kann für die beiden letztgenannten Schutzziele eine detaillierte Risikoanalyse entfallen.

Soweit die auf Bankkonten gebuchten Umsätze in der Finanzbuchhaltung abgebildet werden, kommen Kontoauszüge eines Kreditinstitutes zum einen als Belege für Bankkonten betreffende Buchungsvorgänge und zum anderen als Belege für Geschäftsvorfälle im Verhältnis Bank – Kunde (Abrechnung über Bankleistungen, z.B. Kontenabschluss) in Betracht. Ein fiskalisches Risiko entstünde dann, wenn die Daten in der Absicht der Steuerhinterziehung durch den Empfänger manipuliert werden könnten. Dieses Risiko ist sowohl bei papierhaften Belegen, als auch bei originär digitalen Dokumenten denkbar.

[3] Das BSI Grundschutzhandbuch ist eine Sammlung von Maßnahmenkatalogen, die beschreiben, was man tun kann, um seine IT-Systeme zu schützen. Siehe auch http://www.bsi.de/gshb/

Dieses Dokument wurde von der Mitgliederversammlung des Signaturbündnisses im Juni 2006 verabschiedet. Das Deutsche Signatur- und Kartenforum wurde im April 2007 als Nachfolger des Signaturbündnisses eingerichtet mit dem Ziel, durch einen engen Austausch der am Aufbau einer Signatur- und Karteninfrastruktur in Deutschland beteiligten Kreise die mit dem Signaturbündnis erreichten Standards und Ergebnisse zu sichern und die Fortentwicklung dieser Ergebnisse zu begleiten. Das Deutsche Signatur- und Kartenforum hat sich dafür ausgesprochen, die weiteren Schritte zum Einsatz von Organisationszertifikaten zu konkretisieren.

5.2. Rechtliche Einordnung des elektronischen Siegels

Für die Abgabe von Willenserklärungen in elektronischer Form (§ 126a BGB) wird nach den allgemeinen zivilrechtlichen Grundsätzen wie bei einer händischen Unterschrift auch bei der elektronischen Signatur zur Erfüllung der Formvoraussetzungen ein Handeln einer natürlichen Person (z. B. Verbraucher, Kaufmann, Vertretungsberechtigter einer juristischen Person) vorausgesetzt. Dem entsprechend stellt die EU-Kommission in ihrem Bericht an das Europäische Parlament und den Rat über die Anwendung der Richtlinie 1999/93/EG über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen vom 15. März 2006[6] fest, dass der Unterzeichner einer qualifizierten elektronischen Signatur im Sinne des Artikels 5.1 der EU-Signaturrichtlinie nur eine natürliche Person sein könne, da diese Form der Unterschrift als einer handschriftlichen Unterschrift gleichwertig gilt.

Das „elektronische Siegel" soll zwar mit den Techniken einer elektronischen Signatur erstellt werden, aber nur die Urheberschaft des Unternehmens und nicht einer bestimmten für das Unternehmen handelnden natürlichen Person beweissicher dokumentieren. Der Abgabe von Willenserklärungen soll es nicht dienen und ist damit für alle Dokumente geeignet, bei denen eine Unterschrift nicht zwingend vorgeschrieben ist.

Bei Kontoauszügen, auf die ein elektronisches Siegel aufgebracht werden soll, handelt es sich um Dokumente in Textform im Sinne von § 126b BGB. Eine (personenbezogene) qualifizierte elektronische Signatur wird insofern vom Gesetzgeber nicht vorausgesetzt. Die Grundlagen zur Akzeptanz des elektronischen Siegels und insbesondere zu deren Beweiswert können daher auch außerhalb des Signaturgesetzes definiert werden, so dass eine Änderung oder Ergänzung des Signaturgesetzes nicht zwingend erforderlich ist. Artikel 5.2 der „Richtlinie 1999/93/EG über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen"[7] (EU-Signaturrichtlinie) sieht diese Möglichkeit ausdrücklich vor.

---

[6] Siehe Kommission der Europäischen Gemeinschaften, Brüssel, den 15.3.2006, KOM(2006)120 endgültig, Bericht der Kommission an das Europäische Parlament und den Rat, Bericht über die Anwendung der Richtlinie 1999/93/EG über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen,
http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:52006DC0120:DE:NOT

[7] Siehe Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen
http://europa.eu.int/eur-lex/lex/Result.do?RechType=RECH_celex&lang=de&code=31999L0093

6. Vorschlag zum weiteren Vorgehen

Der Zentrale Kreditausschuss regt an, mit den Oberfinanzdirektionen der Länder abzustimmen, ob die im Signaturbündnis der Bundesregierung formulierten Anforderungen an elektronische Siegel beziehungsweise an Organisationszertifikate für die Absicherung elektronischer Kontoauszüge grundsätzlich geeignet sind (Nichtbeanstandungsregelung).

Hierbei sollten ebenfalls die für die elektronische Steuererklärung (ELSTER) vereinbarten Anforderungen an Organisationszertifikate berücksichtigt werden.

Anlage

Deutsches Signaturbündnis

Technische Arbeitsgruppe

„Spezifikation der Vorgaben und Empfehlungen zum Einsatz von Organisationszertifikaten“

Version 1.0.a

24. Mai 2006

Inhaltsverzeichnis

1 Präambel

Die Vertrauenswürdigkeit, Qualität und Akzeptanz des elektronischen Geschäftsverkehrs wird zukünftig ein entscheidendes Kriterium für den Erfolg aller im Wettbewerb stehenden Unternehmen und Organisationen sein. Eine wesentliche Voraussetzung hierfür ist die praktikable und interoperable Nutzung von zertifikatsbasierenden Verschlüsselungs-, Authentisierungs- und Signaturanwendungen. Die eingesetzten elektronischen Zertifikate sind von vertrauenswürdigen Instanzen (Trustcenter) signierte Informationen zur Kennzeichnung der Identität von Subjekten oder Objekten und ermöglichen somit die verlässliche Kommunikation in offenen Netzen.

Die durch das Signaturgesetz geregelten „qualifizierten Zertifikate" sichern dem darauf vertrauenden Kommunikationspartner einen hohen Beweiswert. Signaturschlüssel-Inhaber können jedoch sowohl bei qualifizierten als auch bei fortgeschrittenen Signaturen stets nur natürliche Personen sein (§ 2 Nr. 9 SigG). Eine juristische Person kann daher nur von natürlichen Personen vertreten werden. Sie kann nicht selbst Inhaber eines Zertifikats sein.

Die bisherigen Ansätze zur Abbildung eines vergleichbaren Beweiswerts für den Bereich der Repräsentation der Identität eines Unternehmens, der Öffentlichen Verwaltung oder anderer juristischer Personen durch pseudonymisierte qualifizierte Zertifikate natürlicher Personen haben den Nachteil, dass für mehrere Mitarbeiter ein Zertifikat zu beantragen ist, da bei nur einem Signaturschlüssel-Inhaber in der Organisation bei Verweigerung, Ableben oder Ausscheiden dieser Person aus der Organisation die Gefahr besteht, dass – zumindest zeitweise - keine Signaturen mehr geleistet werden können.

Serverzertifikate sind Stand der Technik und werden millionenfach eingesetzt, sie dienen der Verschlüsselung bei der Datenübermittlung und lassen die Identität der Internet-Adresse einer Organisation erkennen. Hierbei sind aber bisher die Vorgaben zur Abbildung der Identität einer Organisation in einem elektronischen Zertifikat und dessen Nutzung im Sinne einer Zurechenbarkeit nicht hinreichend erfasst.

Die EU-Kommission weist in ihren aktuellen Bericht über die Anwendung der Richtlinie 1999/93/EG über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen darauf hin, dass "digitale Signaturen meist ausschließlich zur Verstärkung der Authentizität und Integrität einer Nachricht [...], ohne das Ziel oder die Absicht, im herkömmlichen Sinne zu unterschreiben" genutzt werden [1].

Zielsetzung ist es, die Grundlagen für die Akzeptanz eines „Elektronischen Siegels" auf Basis eines Organisationszertifikates zu schaffen, welches es ermöglicht, dass der Empfänger eines elektronisch gesiegelten Dokuments auf die Integrität und die Urheberschaft durch die im Zertifikat bezeichnete Organisation vertrauen kann.
Die Rückverfolgbarkeit der mit dem elektronischen Siegel geleisteten Signatur zu einer Person erfolgt hierbei organisationsintern. Durch die Verankerung des elektronischen Siegels in entsprechenden anwendungsbezogenen Vereinbarungen wird es möglich sein, das gesiegelte Dokument auch gegenüber Dritten, z.B. gegenüber Finanzbehörden oder in Gerichtsverfahren als Beweismittel einzubringen, wenn der Dritte (z.B. die Finanzbehörde) der Akzeptanz der jeweiligen Erklärung in Form eines gesiegelten Dokuments zugestimmt hat .

2 Anwendungsbeispiele für Organisationszertifikate

Die im Folgenden beispielhaft beschriebenen Anwendungsfelder zeigen den dringlichen Bedarf nach Organisationszertifikaten auf. Dabei stehen Prozesse im Vordergrund, bei denen der Austausch von Informationen und Dokumenten keinen besonderen Formerfordernissen unterliegt.

2.1 ELSTER

Das ElsterOnline-Portal www.elsteronline.de stellt seit Januar 2006 umfangreiche Dienste und neue Services zur Verfügung . Bisher kann sich ein Anwender am Portal mit seiner persönlichen Steuernummer registrieren und damit eine elektronische Identität erlangen. Durch diese elektronische Identität kann sich der Anwender bei der Abgabe von Umsatzsteuer-Voranmeldung, Lohnsteuer-Anmeldung, Dauerfristverlängerung und Zusammenfassende Meldung sowie Jahressteuern authentifizieren.

Ab Mitte 2006 wird es im Portal die Möglichkeit geben, eine Firma mit ihrer Firmensteuernummer zu registrieren und so ein Organisationszertifikat zu erlangen. Mit diesem Organisationszertifikat können alle bisherigen Steuerdaten authentisiert übermittelt werden. Weitere Einsatzmöglichkeiten des Organisationszertifikats in ELSTER werden gegenwärtig zwischen der Projektleitung ELSTER und der Kreditwirtschaft abgestimmt.

2.2 Jobcard-Verfahren (ELENA)

Im Jobcard-Verfahren ist von der elektronischen Signatur bislang vor allem insofern die Rede, als die Arbeitnehmer mit einer qualifizierten elektronischen Signatur Leistungen auf elektronischem Wege beantragen. Der Großteil der elektronischen Kommunikation wird im Jobcard-Verfahren zwischen den Arbeitgebern und den zuständigen Stellen (Arbeitsverwaltung, Krankenkassen, Kommunen, Justiz) anfallen. Hierfür übermitteln die Arbeitgeber die Sozialversicherungsdaten nur noch auf elektronischem Wege an die Sozialversicherungsträger. Diese Datenübertragung erfordert eine Absicherung; die Authentizität und Integrität der Daten, die später zur Inanspruchnahme von Leistungen berechtigen, muss sichergestellt sein. Auf der Arbeitgeberseite ergibt sich hiermit ein Einsatzgebiet für Organisationszertifikate.[1]

2.3 Zu Steuerzwecken ausgestellte Bescheinigungen

Derzeit werden Steuerbescheinigungen nach § 45a EStG (von Kreditinstituten im Zusammenhang mit Kapitalanlagen zu Steuerzwecken ausgestellte Bescheinigungen) lediglich in Papierform anerkannt, da der Schuldner der Kapitalerträge auf Verlangen des Gläubigers diesem eine Steuerbescheinigung nach amtlich vorgeschriebenen Muster aushändigen müsse (§ 45a Abs. 2 Satz 1 EStG).

Der Zentrale Kreditausschuss spricht sich dafür aus, dass im Rahmen des Online Banking bereitgestellte elektronische Dokumente wie etwa Kontoauszüge oder elektronische

[1] Zuständiger Ansprechpartner ist die ITSG, mit der die Anforderung an Organisationszertifikate und deren technische Einbindung geklärt werden müssten. Die ITSG gibt eigene Firmenzertifikate durch ihr Trustcenter heraus (siehe www.datenaustausch.de).

Steuerbescheinigungen als Beleg für steuerliche Zwecke verwendet werden können. Für die Authentifizierung der elektronisch übermittelten Daten soll das Organisationszertifikat zum Einsatz kommen.

2.4 E-Mail-Kommunikation

Wenn eine E-Mail-Adresse für eine Organisation oder eine Organisationseinheit (z. B. kundenbetreuung@firma.de) stehen soll, ist dies auch ein Anwendungsfall für Organisationszertifikate. Dies kann Phishing-Attacken erschweren.

2.5 IHK-Signaturanwendung „Elektronisches Ursprungszeugnis"

Das Berechtigungssystem der IHK-Signaturanwendung „Elektronisches Ursprungszeugnis" beruht auf der Abfrage der IHK-Firmenidentnummer, die in den Zertifikaten der (qualifizierten) IHK-Signaturkarten enthalten ist.

Die Anwendung soll mittelfristig nicht mehr verpflichtend an die IHK-Signaturkarte gebunden, sondern auch für andere Zertifizierungsdiensteanbieter geöffnet werden. Da bei den anderen Anbietern aber die IHK-Firmenidentnummer im Zertifikat fehlt, muss diese auf anderem Weg zur Verfügung gestellt werden. Die Anmeldung könnte also per Organisationszertifikat erfolgen, in dem die IHK-Firmenidentnummer enthalten sein wird und so den Zertifikatsinhaber auf den ihm vorbehaltenen Daten- und Bearbeitungsbereich zugreifen lässt.

2.6 Projekt Comparo „Bestands- und Beschaffungsmanagement"

Im Rahmen der Multimediaaktivitäten des Landes Niedersachsen wurde der Beschaffungsprozess (G2B und B2G) zwischen einem öffentlichen Auftraggeber und der Wirtschaft explizit untersucht. Die Teilprozesse Bestellung, Lieferung und Rechnung sind Bestandteil einer Pilotierung, die insbesondere die Aspekte der abzubildenden und anzupassenden Prozesse aus technischer und rechtlicher Sicht betrachtet.

Aus dieser Anforderung ergibt sich unter anderem das Erfordernis, Organisationszertifikate einzusetzen, welche für die verschiedenen Organisationseinheiten entlang der Prozesskette Bestellung, Lieferung oder Rechnung des öffentlichen Auftraggebers stehen. Hier sollen insbesondere elektronische Siegel zum Einsatz kommen.

2.7 Versendung von Rehabilitations- und Rentenbescheiden

Die Deutsche Rentenversicherung Bund bietet einen Großteil ihrer Dienstleistungen online an. So können z. B. Anträge auf Rente, Anträge auf Rehabilitationsmaßnahmen, Anträge auf Kontenklärung und Anträge auf bargeldlose Beitragsentrichtung online gestellt werden. Die Deutsche Rentenversicherung Bund bietet ihren Kunden die elektronische Versendung von Bescheiden und Versicherungsverläufen an. Positive Bescheide sowie Versicherungsverläufe werden in diesem Fall über die Virtuelle Poststelle (E-Mail oder OSCI) signiert, verschlüsselt und verschickt. Dabei wird derzeit ein auf die Deutsche Rentenversicherung Bund ausgestelltes Zertifikat aus der PKI der Verwaltung (PKI-1-Verwaltung über CA IVBB Deutsche Telekom AG) genutzt. Es ist sinnvoll, für die Versendung von Bescheiden und Versicherungsverläufen ein Organisationszertifikat zu nutzen.

2.8 Archivierung elektronischer Akten

Der Umfang der Führung elektronischer Akten nimmt in Wirtschaft und Verwaltung auch durch die Möglichkeiten des Einsatzes von Signaturkarten stetig zu. Eine besondere Herausforderung ist in diesem Zusammenhang die revisionssichere Archivierung der verakteten Dokumente. In den Projekten *ArchiSig* und *ArchiSafe* wird dieses Problem aus Verwaltungssicht bearbeitet. Dabei wurde die rechtzeitige und beweiskräftige Signaturerneuerung durch Anbringen qualifizierter Zeitstempel über Hashwertbäumen der signierten und archivierten Dokumente als Weg zur revisionssicheren Langzeitarchivierung definiert. Es ist denkbar, für diese Übersignierung auch ein Organisationszertifikat einzusetzen.

2.9 Weitere Anwendungsbeispiele

Darüber hinaus sind Anwendungsmöglichkeiten in vielen anderen Bereichen vorstellbar. Dies betrifft zum Beispiel die elektronische Kommunikation zwischen Geschäftspartnern oder Behörden (G2B und G2G) über zentrale Kommunikationskomponenten wie z. B. Virtuellen Poststellen. Ein möglicher Anwendungsfall ist die Bestätigung von Schreiben beratender Berufe wie z. B. Wirtschaftsprüfer oder Steuerberater.

Ferner ist denkbar, dass bei Kommunikationsprozessen, an deren Abwicklung besondere Anforderungen (z.B. die Verwendung qualifizierter Signaturen nach dem SigG) gestellt werden, Organisationszertifikate ergänzend zur Identifikation der absendenden Stelle eingesetzt werden.

3 Begriffsdefinition

Organisationen im Sinne dieses Dokuments sind juristische Personen, die in einem geeigneten Register[2] eingetragen sind[3] sowie juristische Personen des öffentlichen Rechts, z. B. Behörden. Für diese Organisationen können Organisationszertifikate ausgestellt werden.

Elektronische Siegel sind Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder mit ihnen logisch verknüpft sind und zur Authentisierung dienen. Damit sind elektronische Siegel wie folgt definiert:

a) Sie beruhen auf Organisationszertifikaten.

b) Sie ermöglichen eine verlässliche Identifizierung der Organisation.

c) Sie sind so mit den beigefügten oder verknüpften Daten verbunden, dass nachträgliche Veränderungen erkannt werden können.

2 Unternehmensregister, Handelsregister, Vereinsregister, Handwerksrolle, IHK-Firmenspiegel etc.

3 Im folgenden Text wird der Einfachheit halber nur der Begriff der Organisation für den hier definierten Kreis juristischer Personen genutzt.

4 Grundsätzlicher Regelungsbedarf

Für den Einsatz von Organisationszertifikaten sind die folgenden Punkte zu regeln:

1. Welchen Vertrauensstatus bietet ein elektronisches Siegel dem Empfänger?
   - Zurechenbarkeit der Inhalte zur siegelnden Organisation
   - Integrität und Authentizität der Dokumente
   - Anforderungen an die Trustcenter
2. Wie erfolgt die Prüfung eines elektronisch gesiegelten Dokuments?
3. Wie wird die Zuordnung zwischen Organisationszertifikat und der das Zertifikat führenden Organisation sichergestellt?
4. Welchen technischen Anforderungen muss das Organisationszertifikat genügen?
5. Wie wird die Gültigkeit von Organisationszertifikaten geprüft?

4.1 Vertrauensstatus eines elektronischen Siegels

Zur Gewährleistung eines geeigneten Sicherheitsniveaus sind Regelungen in Form einer Certificate Policy zu treffen. Entscheidend für eine geeignete Policy ist, dass die Organisation eine Erklärung der Zurechenbarkeit aller mit dem Elektronischen Siegel versehenen Dokumente abgibt (z. B. in Form eines Relying Party Statements).[4]

Die grundlegende Akzeptanz von Organisationszertifikaten erfordert, die Qualität durch eine freiwillige Selbstregulierung sicherzustellen. Die Entscheidungsprozesse der European Bridge-CA werden hierfür als geeignetes Modell angesehen.

Die Policy der European Bridge-CA [5] und ETSI TS 102 042 [3] dienen als Grundlage für die Erstellung eines geeigneten Regelwerkes für B2B-, B2G- und G2G-Geschäftsprozesse.

Ein Herausgeber von Organisationszertifikaten sollte mindestens folgende Anforderungen erfüllen:

- Es gibt verbindliche Regelungen über die Haftung des Herausgebers von elektronischen Siegeln.
- Der Herausgeber hat sicherzustellen, dass Informationen über den Status des Organisationszertifikats jederzeit für jeden zugänglich sind.
- Es müssen ein Certificate Practice Statement und Certificate Policies veröffentlicht werden.

Ergänzend dazu sind Regelungen zur Registrierung der Organisationen gemäß den Vorgaben in 4.3 zu treffen.[4]

[4] Im Sinne der Reduktion der eigenen Haftung und der operationellen Risiken wird es im Interesse der Organisation liegen, eine effektive Kontrolle der Siegelerstellungseinheit sicherzustellen.

4.2 Prüfung eines elektronischen Siegels

Die Prüfung eines elektronischen Siegels erfolgt nach den internationalen Standards (X.509, RFC 3280 [6]) über einen Zertifizierungspfad bis zu einem Vertrauensanker, der von der für den jeweiligen Anwendungskontext zuständigen Stelle veröffentlicht wird.

4.3 Zuordnung eines Organisationszertifikats

Die Zuordnung zwischen Organisationszertifikat und der das Zertifikat führenden Organisation wird durch den Herausgeber sichergestellt. Dazu hat sich die Organisation vorab gegenüber dem Herausgeber oder seinen Erfüllungsgehilfen in geeigneter Weise zu legitimieren.

Für die erstmalige Ausstellung eines Zertifikats gelten folgende Regelungen:

Juristische Personen, die ein Zertifikat beantragen, werden durch persönliches Erscheinen einer sie zu diesem Zweck vertretenden Person identifiziert. Diese Person muss

- sich mit einem amtlichen Ausweisdokument authentisieren,
- ihre Vertretungsvollmacht zur Beantragung eines Zertifikates für die juristische Person nachweisen,
- den Existenznachweis der Organisation durch einen Auszug aus einem geeigneten Register beibringen. Diesem Auszug müssen die Pflichteinträge des Zertifikats (Name der Organisation, Adresse, eindeutige Zuordnung per Registernummer) zu entnehmen sein.

Die Person, die das Zertifikat beantragt, dient dem Herausgeber auch über die Antragstellung hinaus als verantwortlicher Ansprechpartner. An sie übermittelt der Herausgeber das Zertifikat, zugehörige Daten und Hinweise zur sicheren Nutzung des Zertifikates. Der Wechsel des Ansprechpartners ist dem Herausgeber mitzuteilen. Die Änderungsmittlung erfolgt in schriftlicher Form oder mittels elektronischer Form nach §126 BGB.

Eine Veröffentlichung des Zertifikats ist erst nach Zustimmung durch eine vertretungsberechtigte Person der Organisation möglich.

Werden dem Herausgeber der Nachweis der Existenz und die Pflichteinträge des Zertifikats von einem geeigneten Register übermittelt oder ist der Herausgeber oder sein Erfüllungsgehilfe selbst die Register führende Stelle, kann ein elektronisches Verfahren zur Ausstellung und Verteilung genutzt werden.

Die Beantragung und die Zustimmung können elektronisch erfolgen, wenn eine sichere Methode zur Authentifizierung der vertretenden Person zur Verfügung steht, hierfür kommt eine qualifizierte elektronische Signatur der vertretenden Person in Betracht. Für die Beantragung eines Folgezertifikats kann ein vereinfachtes Antragsverfahren zugelassen werden. Der Herausgeber von Organisationszertifikaten kann zu einem früheren Zeitpunkt erhobene Daten des Antragstellers unter Beachtung der datenschutzrechtlichen Belange des Antragstellers zum Zweck der Identifizierung nutzen, wenn die Identifizierung zuverlässig entsprechend den oben stehenden Anforderungen erfolgt ist, die Daten aktuell sind und der Antragsteller in die Verwendung dieser Daten für diesen Zweck eingewilligt hat.

Die Register führende Stelle und der Herausgeber sind zur Sperrung des Zertifikates berechtigt, wenn gewichtige Gründe (z. B. Veränderung im Register) dafür vorliegen. Die

zertifikationsführende Organisation ist verpflichtet diese Änderung dem Herausgeber mitzuteilen.

Der Herausgeber von Organisationszertifikaten muss die Antragsteller über den sicheren Umgang mit dem Schlüsselmaterial aufklären.

4.4 Technische Anforderungen an Organisationszertifikate

Organisationszertifikate müssen zum Standardprofil ISIS-MTT Core Part [7] konform sein. Ihre Struktur wird detailliert in Kapitel 6 dargestellt.

4.5 Gültigkeitsprüfung von Organisationszertifikaten

Die Zertifikatsprüfung sollte mit allen gängigen Signaturanwendungskomponenten möglich sein. Gegenwärtig ist es deshalb erforderlich, sowohl Sperrlisten als auch OCSP zu unterstützen.

Für die Prüfung über Sperrlisten (CRL) ist der Sperrlistenverteilungspunkt (URL) im Zertifikat unter `crlDistributionPoint` zu hinterlegen.

Für die Prüfung über OCSP ist die Adresse des OCSP-Responders in der Zertifikatserweiterung `AuthorityInfoAccess` anzugeben.

Prinzipiell ist nicht davon auszugehen, dass sich alle Organisationszertifikate in eine einzige hierarchische Struktur einbetten lassen. Trust Service Provider Lists (TSL) können branchenübergreifend Vertrauensinformationen bereitstellen.

5 Registrierung des Inhabers eines Organisationszertifikats

Wie in Abschnitt 4.3 beschrieben erfolgt die Registrierung durch einen Herausgeber von Organisationszertifikaten, dem gegenüber sich die Organisation geeignet legitimiert. Der Herausgeber erstellt ein Organisationszertifikat, das technisch und vom Aufbau her personenbezogenen Zertifikaten gemäß ISIS-MTT [7] entspricht, wobei

- anstelle des Namens der natürlichen Person der Name der Organisation tritt, das bedeutet, dass Pseudonyme nicht zugelassen sind,
- das Organisationszertifikat Angaben zu dem Sitz (Adresse) der Organisation enthält,
- eine eindeutige Zuordnung zu den zugehörigen Einträgen der geeigneten Register vorgenommen werden kann,
- eine Nutzungsbeschränkung enthalten sein kann und
- die Angabe einer geeignet zu spezifizierenden Rolle optional ist.

Die Angabe einer Rolle kann unterbleiben und liegt in der alleinigen Verantwortung des Zertifikatsinhabers. Beispiele für Rollen des Organisationszertifikats sind

- Behörde <NAME>, Postausgangsstelle,
- Telefongesellschaft <NAME>, Technischer Support,
- Bank <NAME>, Steuerbescheinigungen für Zwecke des Kapitalertragssteuerabzugsverfahrens.

6 Zusammenstellung von Namensdarstellung und Identifizierung

Die zum Einsatz kommenden kryptografischen Verfahren müssen den Anforderungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) für zulässige Algorithmen und Schlüssellängen entsprechen. Zur Sicherstellung der technischen Interoperabilität müssen die Vorgaben des Signaturbündnisses und von ISIS-MTT Core Part [7] berücksichtigt werden.

Die Spezifikation von Namen und die eindeutige Identifizierung von Organisationen in Organisationszertifikaten soll sich orientieren an

- Internationalen Standards für X.509-Zertifikate (ITU X.509, PKIX)
- Nationalen Profilierung (ISIS-MTT)
- Kompatibilität mit existierenden Anwendungen.

6.1 Feld subject

Der Inhaber eines X.509-Zertifikats wird im Feld `subject` benannt. Das Feld `subject` muss in einem Organisationszertifikat enthalten sein.

Ein Eintrag für dieses Feld ist eine Folge von Attributen. Die Attribute sind Paare von Type und Wert. Ein typischer Eintrag für `subject` sieht bei einem Personenzertifikat etwa so aus:

```
commonName             = Max Mustermann
serialNumber           = XY123456789
organizationName       = Musterfirma GmbH
organizationalUnitName = Vertrieb
countryName            = DE
```

Bei einer Organisation wäre ein geeigneter Eintrag

```
commonName             = Musterfirma - Vertrieb
serialNumber           = XY123456789
organizationName       = Musterfirma GmbH
organizationalUnitName = ID-Nr. Register
organizationalUnitName = Vertrieb
countryName            = DE
```

Die mögliche Menge an Attributen ist potentiell unbegrenzt. Wegen der Interoperabilität und der Möglichkeit zur maschinellen Verarbeitung sollen nur Attribute benutzt werden, die in ISIS-MTT benannt werden ([7], Tabelle 7).

Zusätzlich sind dort Längenbegrenzungen für die verwendeten Werte definiert:

#	Attribut	Type	Länge	Empfehlung[5]
1	commonName	DirectoryString	64	++
2	surName	DirectoryString	64	-
3	givenName	DirectoryString	64	-
4	serialNumber	PrintableString	64	++
5	title	DirectoryString	64	-
6	organizationName	DirectoryString	64	++
7	organizationalUnitName	DirectoryString	64	+
8	businessCategory	DirectoryString	128	0
9	streetAddress	DirectoryString	128	++
10	postalCode	DirectoryString	40	++
11	localityName	DirectoryString	128	++
12	stateOrProvinceName	DirectoryString	128	+
13	countryName	PrintableString	2	++
14	distinguishedNameQualifier	PrintableString	64	0
15	initials	DirectoryString	64	-
16	generationQualifier	DirectoryString	64	-
17	emailAddress	IA5String	128	--
18	domainComponent			0
19	postalAddress	SEQUENCE SIZE (1..6) OF DirectoryString	6 x 30	0
20	pseudonym	DirectoryString	64	--
21	dateOfBirth	GeneralizedTime	YYYYMMDD000000Z	--

[5] Legende:

++ Das entsprechende Datenelement ist verpflichtend bei der Erstellung von Zertifikaten und CRLs, d.h. es muss vorhanden sein. Dieses Zeichen ist gleichbedeutend mit den in der internationalen Standardisierung vernutzen Begriffen "MUST", "SHALL", "MANDATORY".

\+ Es wird empfohlen, das entsprechende Datenelement als Option bei der Erstellung von Zertifikaten und CRLs mit aufzunehmen, d.h. es sollte vorhanden sein. Dieses Zeichen ist gleichbedeutend mit den in der internationalen Standardisierung vernutzen Begriffen "SHOULD", "RECOMMENDED".

0 Das entsprechende Datenelement ist optional bei der Erstellung von Zertifikaten und CRLs, d.h. es kann oder auch nicht vorhanden sein. Dieses Zeichen ist gleichbedeutend mit den in der internationalen Standardisierung vernutzen Begriffen "MAY", "OPTIONAL".

\- Es wird davon abgeraten, das entsprechende optionale Datenelement bei der Erstellung von Zertifikaten und CRLs zu verwenden, d.h. es sollte nicht vorhanden sein. Dieses Zeichen ist gleichbedeutend mit den in der internationalen Standardisierung vernutzen Begriffen "SHOULD NOT", "NOT RECOMMENDED".

-- Das entsprechende optionale Datenelement darf bei der Erstellung von Zertifikaten und CRLs nicht verwendet werden. Dieses Zeichen ist gleichbedeutend mit den in der internationalen Standardisierung vernutzen Begriffen "MUST NOT".

#	Attribut	Type	Länge	Empfehlung[5]
22	placeOfBirth	DirectoryString	128	--
23	gender	PrintableString	1	--
24	countryOfCitizenship	PrintableString	2	--
25	countryOfResidence	PrintableString	2	--
26	nameAtBirth	DirectoryString	64	--

6.2 Eindeutige Bennennung des Zertifikatsinhabers

Die Attribute des Feldes `subject`, in denen der Name der Organisation hinterlegt werden kann, haben Längenbegrenzung von 64 Zeichen. Deshalb können lange Organisationsnamen nicht vollständig in diesen Attributen und somit auch nicht im Feld `subject` dargestellt werden, wenn eine zu den allgemein anerkannten Standards konforme Darstellung erfolgen soll.

Da diese Problematik allgemein gegeben ist, wird einer Organisation, die in einem bestimmten Anwendungskontext gemeldet ist, in der Regel eine – in diesem Anwendungsbezug eindeutige – Identifikationsnummer zugeordnet. Beispiele hierfür sind Umsatzsteuer-Identifikationsnummer oder Handelsregisternummer. Wenn Organisationszertifikate für diesen Anwendungskontext genutzt werden sollen, ist eine Angabe der eindeutigen Identifikationsnummer hilfreich.

Andererseits agieren Organisationen in verschiedenen Anwendungskontexten, so dass einer Organisation durchaus verschiedene Identifikationsnummer zugeordnet sein können. Die Aufnahme mehrerer Identifikationsmerkmale verschiedener Register ins Zertifikat sollte deshalb nicht ausgeschlossen werden.

6.3 Lösungsvorschlag

Das Feld `subject` eines Organisationszertifikats enthält einen Kurznamen der Organisation. Die Bildung dieses Kurznamens liegt im Ermessen der registerführenden Einrichtung. Die Eindeutigkeit des Felds `subject` muss dabei im Kontext des Zertifikatsausstellers (Issuer) gegeben sein. Darüber hinaus soll es optional möglich sein, in das Zertifikat eine oder mehrere Identifikationsnummern aufzunehmen. Hierfür ist das Attribut `organizationalUnitName` zu verwenden, da dieses Attribut mehrfach genutzt werden kann.

Um Identifikationsnummern unterschiedlicher Register voneinander unterscheiden zu können, sollten diese eine Semantik nach ISO 6523[6] abbilden. Hierfür müssten die in den geeigneten Registern genutzten Identifikationsschemata bei der ISO 6523-Registrierungsstelle angemeldet werden.

Weitere Identifikationsnummern nach ISO 6523 können als `dnsName` Felder im `subjectAltName` aufgenommen werden, da sie dort auch von Standard-Zertifikatsviewern angezeigt werden.

Angabe einer E-Mail-Adresse oder URL

6 Der Text der ISO-Norm 6523 ist unter http://www.nic.it/NA/iso6523.txt abrufbar.
Die Liste der registrierten Identifizierungsschemata ist unter http://www.edira.org/download/icd-list.pdf abrufbar

Wenn das Organisationszertifikat eine E-Mail-Adresse enthalten soll, ist dafür ein `rfc822Name` im `subjectAltName` zu verwenden. Analog kann dort eine zugehörige URL der Organisation als `uniformResourceIdentifier` aufgenommen werden.

Angabe des vollständigen Organisationsnamens

Bei Bedarf kann ein vollständiger Organisationsname in der Extension `AdditionalInformation` {isis-mtt-at 15} vermerkt werden. Mit 2048 Zeichen sollte jeder Organisationsname darstellbar sein.

Strukturinformationen für Workflow-Unterstützung

Flexible Strukturinformationen für künftige Workflow-Unterstützung sollten in einer Extension abgebildet werden. Das Konzept hierfür muss noch weiter ausgearbeitet werden.

6.4 Beispiele für Organisationszertifikate:

Vorlage für die Zertifikatsstruktur

Zertifikatsfeld	Inhalt	Kommentar
version	v3	
serialNumber	<Seriennummer>	
signatureAlgorithmIdentifier	<OID>	
issuer	Ausstellerdaten	Trustcenter
commonName	<...>	
organizationName	<...>	
organizationalUnitName	<...>	
countryName	DE	
Validity		
notBefore	<Tag der Erstellung>	
notAfter	<Tage der Erstellung + n Jahre>	garantierter Zeitraum der Bereitstellung der Statusinfo: n Jahre
Subject		
commonName	<Kurzname der Organisation>	obligatorisch
organizationName	<Name der Organisation>	obligatorisch
organizationalUnitName	<ID-Nr. Register 1>	obligatorisch
organizationalUnitName	<ID-Nr. Register 2>	

Zertifikatsfeld	Inhalt	Kommentar
organizationalUnitName	<ID-Nr. Register 3>	
organizationalUnitName	<Untereinheit>	
streetAddress	<Straße Nr.>	obligatorisch
postalCode	<PLZ>	obligatorisch
localityName	<Standort>	obligatorisch
countryName	<Land>	obligatorisch
algorithm	<OID>	
subjectPublicKey	<Schlüssel>	
extensions		
authorityKeyIdentifier	<ID>	Kennung des CA-Schlüssels
subjectKeyIdentifier	<ID>	Kennung des Zer-tifikats-Schlüssels
certificatePolicies	<Adresse der CP/CPS>	
subjectAlternativeName	<E-Mail-Adresse oder URL>	
crlDistributionPoint	<LDAP- oder HTTP-Adresse>	CRL-Bezug
authorityInfoAccess	<HTTP-Adresse>	OCSP-Responder
keyUsage	DigitalSignature, Non-Repudiation	

Bespielzertifikat: Zertifikat der Deutsche Rentenversicherung Bund (ehem. BfA), ausgestellt von der CA des IVBB:

Zertifikatsfeld	Inhalt
version	v3
serialNumber	31 26
signatureAlgorithmIdentifier	sha1RSA
issuer	
commonName	CN = CA IVBB Deutsche Telekom AG 05
organizationalUnitName	OU = Bund
organizationName	O = PKI-1 Verwaltung
countryName	C = DE
Validity	
notBefore	Montag, 4. Juli 2005 13:31:38
notAfter	Samstag, 28. Juni 2008 1:59:00
Subject[7]	
commonName	CN = GRP: Bundesversicherungsanstalt für Angestellte (BfA)
localityName	L = Berlin
organizationalUnitName	OU = BfA
organizationalUnitName	<ID-Nr. Register 1>
organizationalUnitName	<ID-Nr. Register 2>
organizationalUnitName	<ID-Nr. Register 3>
organizationName	O = Bund
streetAddress	
postalCode	
countryName	C = DE
subjectPublicKeyInfo	
algorithm	<OID>
subjectPublicKey	<Schlüssel>

[7] Das subject-Feld enthält außerdem das lt. ISIS-MTT [7] nicht zugelassene Attribut emailAddress: E = bfa@bfa.de

Zertifikatsfeld	Inhalt
extensions	
authorityKeyIdentifier	<ID>
subjectKeyIdentifier	<ID>
certificatePolicies	<Adresse der CP/CPS>
subjectAlternativeName	RFC822-Name = bfa@bfa.de
crlDistributionPoint	URL = ldap://x500.bund.de/CN=CA IVBB Deutsche Telekom AG 05,OU=Bund,O=PKI-1 Verwaltung,C=DE?certificateRevocationList
authorityInfoAccess	<HTTP-Adresse>
keyUsage	DigitalSignature, Non-Repudiation, KeyEncipherment

7 Abkürzungen

BSI	Bundesamt für Sicherheit in der Informationstechnik
CA	Certification Authority
CRL	Certificate Revocation List
ETSI	Europäisches Institut für Telekommunikationsnormen
ISIS-MTT	Industrial Signature Interoperability Standard-MailTrusT
ITSG	Informationstechnischen Servicestelle der Gesetzlichen Krankenversicherung GmbH
ITU	International Telecommunication Union
OSCP	Online Certificate Status Protocol
PKI	Public Key Infrastructure
PKIX	Public-Key Infrastructure (X.509)
T7	Arbeitsgemeinschaft der Trustcenterbetreiber
TESTA	Trans European Services for Telecommunication between Administrations
URL	Uniform Resource Locator
OSCI	Online Service Computer Interface
SigG	Signaturgesetz

8 Referenzierte Dokumente

[1] Bericht der EU-Kommission an das Europäische Parlament und den Rat über die Anwendung der Richtlinie 1999/93/EG über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen vom 15. März 2006

[2] Richtlinie des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen (1999/93/EG) [www.iukdg.de]

[3] ETSI TS 102 042 (2005): Policy requirements for certification authorities issuing public key certificates [www.etsi.org]

[4] Sicherheitsleitlinien der Wurzelzertifizierungsinstanz der Verwaltung, Bundesamt für Sicherheit in der Informationstechnik, Version 3.2, 9. Januar 2003

[5] Zertifikatsrichtlinie für Mitglieder der European Bridge-CA, Version 1.0, 1. April 2006

[6] IETF RFC 3280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, April 2002

[7] ISIS-MTT Core Specification Version 1.1, 16. März 2004 [www.isis-mtt.org]