

---

Aufsichtsstelle für elektronische Signaturen

Positionspapier zu § 2 Z 3 lit. a bis d SigG  
(„fortgeschrittene elektronische Signatur“)

Version 1.0

13.04.2004

---

Aufsichtsstelle für elektronische Signaturen

Telekom-Control-Kommission & Rundfunk und Telekom Regulierungs-GmbH  
Mariahilfer Straße 77–79, 1060 Wien, Tel. +43/1/58058-0, Fax: +43/1/58058-9191  
<http://www.signatur.rtr.at/>, [signatur@signatur.rtr.at](mailto:signatur@signatur.rtr.at)

## Inhaltsverzeichnis

Inhaltsverzeichnis .....	2
1. Ausgangslage .....	2
2. Zur Auslegung von § 2 Z 3 lit. a bis d SigG .....	3
2. a) „ausschließlich dem Signator zugeordnet“ .....	4
2. b) „die Identifizierung des Signators ermöglicht“ .....	4
2. c) „alleinige Kontrolle“ .....	4
2. d) „so verknüpft ..., dass jede nachträgliche Veränderung der Daten festgestellt werden kann“ .....	5
3. Fragen zu Serversignaturen .....	5
4. Vorgangsweise der Aufsichtsstelle .....	7
5. Empfehlungen .....	8
5.1. Empfehlungen für Personen, die fortgeschrittene elektronische Signaturen erstellen wollen .....	8
5.2. Empfehlungen für Personen, welche eine fortgeschrittene elektronische Signatur prüfen wollen .....	8
5.3. Empfehlungen für Zertifizierungsdiensteanbieter .....	9
Anhang .....	10

### 1. Ausgangslage

Am 23.12.2003 wurde im Bundesgesetzblatt die „Verordnung des Bundesministers für Finanzen, mit der die Anforderungen an eine auf elektronischem Weg übermittelte Rechnung bestimmt werden“ kundgemacht (BGBl. II Nr. 583/2003, vgl. den Anhang). Diese Verordnung verweist im Wesentlichen auf § 2 Z 3 lit. a bis d Signaturgesetz (SigG). § 2 Z 3 lit. a bis d SigG entspricht der Definition der „fortgeschrittenen elektronischen Signatur“ nach Art. 2 Z 2 der Signaturrichtlinie 1999/93/EG. Auf Grund der Verordnung haben Zertifizierungsdiensteanbieter und Anwender an die Aufsichtsstelle zahlreiche Anfragen zur Auslegung des § 2 Z 3 lit. a bis d SigG gerichtet.

Zertifizierungsdiensteanbieter unterliegen gemäß § 13 SigG der Aufsicht durch die Telekom-Control-Kommission als Aufsichtsstelle für elektronische Signaturen. Gemäß § 6 Abs. 4 SigG haben Zertifizierungsdiensteanbieter die in ihrem Sicherheits- und Zertifizierungskonzept dargelegten Angaben sowohl bei der Aufnahme als auch während der Ausübung ihrer Tätigkeit zu erfüllen. Gemäß § 13 Abs. 2 Z 1 SigG hat die Aufsichtsstelle die Umsetzung der Angaben im Sicherheits- und im Zertifizierungskonzept zu überprüfen; bei Verletzung der Anforderungen hätte die Aufsichtsstelle Aufsichtsmaßnahmen nach § 14 SigG zu ergreifen.

Wenn ein Zertifizierungsdiensteanbieter in seinem Sicherheits- und Zertifizierungskonzept den Anspruch erhebt, dass die basierend auf den von ihm ausgestellten Zertifikaten

erstellten Signaturen die Anforderungen des § 2 Z 3 lit. a bis d SigG erfüllen und somit für elektronische Rechnungen geeignet sind, ist von der Aufsichtsstelle zu überprüfen, ob die Anforderungen in § 2 Z 3 lit. a bis d SigG tatsächlich erfüllt sind.

Dieses Positionspapier beschreibt die Auslegung des § 2 Z 3 lit. a bis d SigG durch die Telekom-Control-Kommission als Aufsichtsstelle für elektronische Signaturen. Es ist darauf hinzuweisen, dass die Rechtsansicht der Telekom-Control-Kommission für die Finanzbehörden nicht bindend ist und dass die Telekom-Control-Kommission und die Finanzbehörden auch unterschiedliche Betrachtungsweisen anlegen. Die Telekom-Control-Kommission prüft die von Zertifizierungsdiensteanbietern angebotenen Zertifizierungsdienste, für die Finanzbehörden sind die einzelnen elektronischen Rechnungen relevant. Es ist möglich, dass ein Zertifizierungsdienst zwar nach Ansicht der Telekom-Control-Kommission die Anforderungen des § 2 Z 3 lit. a bis d SigG erfüllt, dass eine Finanzbehörde aber im Einzelfall feststellt, dass bei der Signatur einer konkreten elektronischen Rechnung Sicherheitsvorkehrungen verletzt wurden und die Echtheit oder Unverfälschtheit der Rechnung daher nicht gegeben ist. Umgekehrt wird auch bei Verwendung von Zertifizierungsdiensten, die in ihrer Gesamtheit den Anforderungen des § 2 Z 3 lit. a bis d SigG nicht entsprechen, im Einzelfall oft nachgewiesen werden können, dass die Anforderungen bei der Signatur der konkreten elektronischen Rechnung erfüllt waren.

Die Aufsichtsstelle will – nicht zuletzt durch die Veröffentlichung dieses Positionspapiers – dazu beitragen, dass solche Zweifelsfälle möglichst selten auftreten, indem für die Signatur von elektronischen Rechnungen von vornherein entsprechende Zertifizierungsdienste und technische Komponenten verwendet werden. Die Aufsichtsstelle wird daher auch auf ihrer Website Zertifizierungsdienste als für die fortgeschrittene elektronische Signatur geeignet kennzeichnen, wenn der Zertifizierungsdiensteanbieter in seinem Sicherheits- und Zertifizierungskonzept gewährleistet, dass die Anforderungen aus § 2 Z 3 lit. a bis d SigG bei allen im Rahmen des Zertifizierungsdienstes ausgestellten Zertifikaten erfüllt sind (siehe Kapitel 4).

Da sich gerade bei der Signatur elektronischer Rechnungen oft auch Fragen stellen, wie elektronische Signaturen von juristischen Personen und von Servern erstellt werden können, enthält dieses Positionspapier auch Ausführungen zu dieser Thematik (siehe Kapitel 3).

## **2. Zur Auslegung von § 2 Z 3 lit. a bis d SigG**

Eine Signatur, welche die Anforderungen nach § 2 Z 3 lit. a bis d SigG erfüllt, ist eine elektronische Signatur, die

- a) ausschließlich dem Signator zugeordnet ist,
- b) die Identifizierung des Signators ermöglicht,
- c) mit Mitteln erstellt wird, die der Signator unter seiner alleinigen Kontrolle halten kann und
- d) mit den Daten, auf die sie sich bezieht, so verknüpft ist, dass jede nachträgliche Veränderung der Daten festgestellt werden kann.

Diese vier Anforderungen entsprechen dem Begriff der „fortgeschrittenen elektronischen Signatur“ des Art. 2 Z 2 der Signaturrechtlinie 1999/93/EG. Von dem in Österreich verwendeten Begriff der „sicheren elektronischen Signatur“ (§ 2 Z 3 lit. a bis e SigG) unterscheidet sich dieser Begriff dadurch, dass die Signatur nicht notwendigerweise auf einem qualifizierten Zertifikat beruht (das bedeutet unter anderem, dass vor der Ausstellung des Zertifikates nicht unbedingt ein Lichtbildausweis geprüft werden muss) und dass die

Signatur nicht notwendigerweise mit einer sicheren Signaturerstellungseinheit (wie z. B. einer entsprechend geprüften und bescheinigten Chipkarte) erstellt werden muss.

Die Definitionen im Signaturgesetz und in der Signaturrechtlinie sind technologieneutral. In der Praxis wird die elektronische Signatur aber meist durch asymmetrische kryptographische Verfahren realisiert, daher beziehen sich die folgenden Ausführungen ausschließlich auf solche Implementierungen.

## **2. a) „ausschließlich dem Signator zugeordnet“**

Aus dieser Anforderung kann abgeleitet werden, dass das selbe Schlüsselpaar nicht mehreren Personen zugeordnet werden darf und dass der Zertifizierungsdiensteanbieter wissen muss, welches Schlüsselpaar er welcher Person zugeordnet hat.

## **2. b) „die Identifizierung des Signators ermöglicht“**

Diese Anforderung ist weniger streng als die Anforderung, welche Anhang II d) der Signaturrechtlinie bzw. § 7 Abs. 1 Z 4 SigG an die Ausstellung von qualifizierten Zertifikaten stellt (§ 7 Abs. 1 Z 4 SigG: „anhand eines amtlichen Lichtbildausweises die Identität ... zuverlässig zu überprüfen). Aus dieser Anforderung kann Folgendes abgeleitet werden:

- Das Zertifikat wird an einen „Signator“ ausgestellt, also nach der Definition des § 2 Z 2 SigG an eine natürliche Person (oder einen Zertifizierungsdiensteanbieter) und nicht an eine juristische Person oder einen Server.
- Der Zertifizierungsdiensteanbieter muss die Identität des Signators prüfen, bevor er das Zertifikat ausstellt. Der Prozess der Identitätsprüfung muss aber nicht die hohen Anforderungen erfüllen, die für qualifizierte Zertifikate verlangt werden. Zum Vergleich sei auf die im Anhang wiedergegebenen Auszüge aus den beiden ETSI-Standards für qualifizierte Zertifikate (ETSI TS 101 456) und für andere Zertifikate (ETSI TS 102 042) verwiesen.
- Die Verwendung eines Pseudonyms, das als solches bezeichnet ist, im Zertifikat ist zulässig (§ 5 Abs. 1 SigG lässt die Verwendung von Pseudonymen auch in qualifizierten Zertifikaten zu), aber der Zertifizierungsdiensteanbieter muss die Identität des Signators kennen.

## **2. c) „alleinige Kontrolle“**

### **Erzeugung und Speicherung der Signaturerstellungsdaten (private Schlüssel)**

Die meisten Anforderungen an die Erzeugung und Speicherung der Signaturerstellungsdaten beruhen nicht auf § 2 Z 3 lit. c) SigG, sondern auf § 18 SigG und der Signaturverordnung (im Europarecht: auf der Definition der „sicheren Signaturerstellungseinheit“ in Art. 2 Z 6 und Anhang III sowie auf Anhang II lit. j der Signaturrechtlinie).

§ 2 Z 3 lit. c) fordert aber, dass die elektronische Signatur mit Mitteln erstellt wird, die der Signator unter seiner „alleinigen Kontrolle“ halten kann. Dies bedeutet nicht zwangsläufig, dass als Signaturerstellungseinheiten spezielle Hardware (nicht auslesbare Datenträger wie Chipkarten oder HSMs) verwendet werden muss, aber es bedeutet, dass – insbesondere dann, wenn der private Schlüssel ausschließlich auf auslesbaren Datenträgern gespeichert wird – Sicherheitsmaßnahmen eingesetzt werden müssen, damit der Signator die Kontrolle über den Schlüssel halten kann (z. B. Verschlüsselung der Datei, in welcher der private Schlüssel gespeichert ist, sowie Zugangs- und Zugriffsbeschränkungen zum Computer und zu dieser Datei).

Wenn die Aufsichtsstelle die Frage zu beurteilen hat, ob ein Zertifizierungsdienst in seiner Gesamtheit die Anforderung des § 2 Z 3 lit. c) SigG erfüllt, wird sie daher prüfen, ob der Zertifizierungsdiensteanbieter mit dem Sicherheits- und Zertifizierungskonzept dieses Zertifizierungsdienstes sicherstellt, dass Zertifikate nur ausgestellt werden, wenn der Signator entweder nicht auslesbare Datenträger (z. B. Chipkarten oder HSMs) verwendet oder wenn der Zertifizierungsdiensteanbieter den Signator zu entsprechenden Sicherheitsmaßnahmen zum Schutz eines auf auslesbaren Datenträgern gespeicherten Schlüssels vertraglich verpflichtet.

### **Anforderungen an kryptographische Algorithmen**

Die meisten Anforderungen an Algorithmen beruhen nicht auf § 2 Z 3 lit. c) SigG, sondern auf § 18 SigG und den Anhängen der Signaturverordnung (im Europarecht: auf der Definition der „sicheren Signaturerstellungseinheit“ in Art. 2 Z 6 und Anhang III der Signaturrechtlinie). Aus der Anforderung, dass der Signator in der Lage sein muss, die Schlüssel unter seiner „alleinigen Kontrolle“ zu halten, kann aber abgeleitet werden, dass die Schlüssellänge nicht zu kurz sein darf, da der private Schlüssel sonst aus dem öffentlichen Schlüssel errechnet werden könnte.

In der Praxis sollte es für Nutzer der elektronischen Signatur kein Problem darstellen, jene Algorithmen und Parameter zu verwenden, welche in den Anhängen der Signaturverordnung für die sichere elektronische Signatur vorgesehen werden. Dies entspricht auch der europäischen Praxis, welche für sichere Signaturerstellungseinheiten nach Anhang III der Signaturrechtlinie und für die fortgeschrittene elektronische Signatur in qualifizierten Zertifikaten (Anhang II f der Signaturrechtlinie) die gleichen Algorithmen und Parameter verlangt.

### **2. d) „so verknüpft ..., dass jede nachträgliche Veränderung der Daten festgestellt werden kann“**

Diese Anforderung kann leicht erfüllt werden, indem geeignete kryptographische Algorithmen als Hashverfahren und für die Erstellung der elektronischen Signatur verwendet werden – insbesondere die in den Anhängen der Signaturverordnung für die sichere elektronische Signatur genannten Algorithmen.

## **3. Fragen zu Serversignaturen**

Im Zusammenhang mit fortgeschrittenen Signaturen und mit der Signatur elektronischer Rechnungen wird oft die Frage gestellt, wie ein Server so konfiguriert werden kann, dass er für eine juristische Person eine große Anzahl von Signaturen automatisch erstellen kann. Dasselbe gilt auch, wenn ein Server für eine natürliche Person oder eine Personengesellschaft signieren soll, im Folgenden wird der Einfachheit halber ausschließlich das Beispiel erörtert, dass ein Server für eine juristische Person signieren soll.

Gemäß § 2 Z 2 SigG ist ein Signator eine „natürliche Person, der Signaturerstellungsdaten und die entsprechenden Signaturprüfdaten zugeordnet sind und die entweder im eigenen oder im fremden Namen eine elektronische Signatur erstellt, [oder ein Zertifizierungsdiensteanbieter, der Zertifikate für die Erbringung von Zertifizierungsdiensten verwendet]“.

Praktische Lösungen, wie ein Server automatisch für eine juristische Person signieren kann, können daher wie folgt beschrieben werden. Es sei darauf hingewiesen, dass es sich bei allen hier beschriebenen Varianten um Beispiele handelt und dass es eine Vielzahl von Möglichkeiten gibt, Serversignaturen zu implementieren:

- Das Zertifikat für den vom Server verwendeten Schlüssel wird nicht an den Server oder an die juristische Person ausgestellt, sondern an eine natürliche Person, die für den Server verantwortlich ist – den „Signator“. Im Subject-Feld des Zertifikates wird entweder der Name dieser natürlichen Person eingetragen (typischerweise im Attribut commonName – „CN“ – oder in den Attributen givenName und surname bzw. in der Extension subjectAltName) oder ein Pseudonym der Person wird im pseudonym-Attribut eingetragen. Eine übliche Lösung ist auch, dass statt dem Namen der Person der Domainname des Servers im CN-Attribut eingetragen wird und der Domainname des Servers sozusagen als ein Pseudonym des Signators verstanden wird, das nicht ausdrücklich als solches gekennzeichnet ist. Welche Variante gewählt wird, richtet sich in der Praxis meist nach den Angeboten der Zertifizierungsdiensteanbieter.
- Schon aus allgemeinen zivilrechtlichen Überlegungen ergibt sich, dass jemand, der für eine andere Person signiert, entsprechend vertretungsbefugt sein muss. Die Vertretungsbefugnis für eine juristische Person kann beispielsweise eine im Firmenbuch eingetragene organschaftliche Vertretung, aber auch eine Vollmacht sein. Es ist nicht erforderlich, dass der Vertreter Angestellter des Unternehmens ist, welches er vertritt. Beispielsweise kann ein Unternehmen, das IT-Dienstleistungen auslagern will, einen Systemadministrator des Auftragnehmers dazu bevollmächtigen, als Signator für den Auftraggeber zu handeln. Eine solche Vollmacht könnte mit dem Auftrag verbunden werden, ausschließlich bestimmte Arten von Dokumenten mittels eines bestimmten Servers zu signieren.
- Aus dem Signaturrecht ergeben sich keine Anforderungen, dass in der Signatur oder dem Zertifikat selbst darauf verwiesen wird, dass der Signator für jemand anderen signiert. In manchen rechtlichen Zusammenhängen ist es erforderlich, dass ein Auftreten als Vertreter offengelegt wird (z. B. wenn man für den Vertretenen einen Vertrag abschließen will). Aber auch in Fällen, in denen die Vertretungsbefugnis nicht offengelegt werden muss, ist diese Offenlegung oft erwünscht. Im Zusammenhang mit elektronischen Signaturen gibt es unter anderem die folgenden Möglichkeiten:
  - Technisch am einfachsten umsetzbar ist es, einfach im signierten Dokument auf die Vertretungsbefugnis zu verweisen. Mit dieser Möglichkeit können auch Grenzen oder Besonderheiten der Vertretungsbefugnis am flexibelsten dargelegt werden.
  - In manchen Fällen erscheint es wünschenswert, im Zertifikat auf eine juristische Person zu verweisen. Dazu wird üblicherweise das organizationName-Attribut („O“) im Subject-Feld des Zertifikates verwendet. Im Sicherheits- und Zertifizierungskonzept beschreibt der Zertifizierungsdiensteanbieter, was er in das organizationName-Attribut des Zertifikates einträgt, d. h. wie dieses Attribut in seinen Zertifikaten zu interpretieren ist. Der Zertifizierungsdiensteanbieter kann z. B. zusichern, dass er nicht nur die Identität der natürlichen Person, sondern auch die Identität der juristischen Person prüft und dass er auch prüft, dass die natürliche Person von der juristischen Person bevollmächtigt wurde, ein Zertifikat zu beantragen. In diesem Fall sollte der Zertifizierungsdiensteanbieter in seinem Sicherheits- und Zertifizierungskonzept auch vorsehen, dass die juristische Person berechtigt ist, einen Widerruf des Zertifikates zu verlangen, wenn die natürliche Person nicht mehr dazu bevollmächtigt ist. Es ist auch empfehlenswert, die juristische Person (welche diese Art von Zertifikaten typischerweise bestellen wird) im Vertrag dazu zu verpflichten, in diesem Fall auch einen Widerruf zu verlangen.
  - Anstatt die Vertretungsbefugnis auf die beschriebene Weise im Zertifikat selbst zum Ausdruck zu bringen, könnten auch Attributzertifikate verwendet werden.

- Der Signator muss in der Lage sein, den privaten Schlüssel unter seiner alleinigen Kontrolle zu halten. Der Server muss daher so konfiguriert werden, dass nur die natürliche Person, welche als Signator agiert, Zugriff zum privaten Schlüssel hat. Es ist daher zweckmäßig, wenn ein Systemadministrator als Signator agiert.
- Die Signatur muss ausschließlich dem Signator zugeordnet sein, das heißt, der private Schlüssel darf nur einer Person zugeordnet werden. Wenn die natürliche Person, die für den Server verantwortlich ist, das Unternehmen verlässt und durch eine andere Person ersetzt wird, dann muss auch der private Schlüssel gewechselt werden und ein neues Zertifikat verwendet werden. Dies ist auch erforderlich, wenn statt des Namens des Signators ein Pseudonym verwendet wird und das Pseudonym nicht geändert wurde.
- Für Massensignaturen gibt es in der Praxis zwei Möglichkeiten: Entweder die Applikation sammelt zunächst alle zu signierenden Dokumente und eine Person löst dann für einen ganzen Stapel von Dokumenten willentlich die Signaturerstellung aus oder die Signaturen sollen in Echtzeit ohne Willensakt einer Person erstellt werden. Für die erste Variante ist der Einsatz der sicheren elektronischen Signatur möglich und empfehlenswert. § 7 Abs. 3 SigV verlangt nicht, dass der Signator jedes einzelne Dokument vor der Auslösung der Signatur liest, der Signator muss aber wissen, wie viele Dokumente er durch seine PIN-Eingabe signiert und er muss die einzelnen Dokumente lesen können. Für die zweite Variante ist es nicht möglich, die sichere elektronische Signatur einzusetzen. Stattdessen wird man besondere Sicherheitsmaßnahmen beim Server vornehmen, der die Signaturen auslöst (insbesondere Zutritts- und Zugriffsbeschränkungen und Restriktionen betreffend die auf dem Server installierte Software). Auch bei der zweiten Variante muss es eine natürliche Person geben, die als Signator agiert und für die erstellten Signaturen verantwortlich ist. Es ist aber bei der zweiten Variante in der Regel nicht erforderlich, dass diese Person permanent anwesend ist, da man den Server so konfiguriert, dass der Signator die Signaturerstellungsdaten einmal aktiviert und die Signaturen in weiterer Folge ohne sein Zutun ausgelöst werden. Dennoch sollte vorgesorgt werden, dass man den Schlüssel und das Zertifikat leicht auswechseln kann, wenn der Signator das Unternehmen verlässt oder in einen anderen Bereich wechselt und daher die alleinige Kontrolle über die Signaturerstellungsdaten nicht mehr ausüben kann.

## 4. Vorgangsweise der Aufsichtsstelle

Auf der Website der RTR-GmbH werden jene Zertifizierungsdienste, bei denen Zertifikate für fortgeschrittene elektronische Signaturen angeboten werden, gesondert markiert (<http://www.signatur.rtr.at/de/providers/services.html>). Eine solche Markierung signalisiert, dass alle im Rahmen dieses Dienstes ausgestellten Zertifikate zur Erstellung fortgeschrittener elektronischer Signaturen geeignet sind (umgekehrt lässt sich aber aus dem Fehlen einer solchen Markierung nicht ableiten, dass die im Rahmen des Dienstes ausgestellten Zertifikate nicht zum Erstellen fortgeschrittener elektronischer Signaturen geeignet sind, vgl. Kapitel 1 und 5.2).

Die Prüfung, ob die im Rahmen eines Zertifizierungsdienstes ausgestellten Zertifikate zum Erstellen fortgeschrittener elektronischer Signaturen geeignet sind, erfolgt aufgrund folgender Kriterien:

- Identifizierung des Signators: Das Sicherheits- und Zertifizierungskonzept muss beschreiben, auf welche Weise die Identität des Signators geprüft wird (vgl. Kapitel 2 b). Zertifikate dürfen nur an natürliche Personen ausgestellt werden. Wenn im Zertifikat eine Vertretungsbefugnis zum Ausdruck gebracht werden soll, muss im Sicherheits- und Zertifizierungskonzept beschrieben werden, auf welche Weise dies überprüft wird.

- Dokumentation: Das Sicherheits- und Zertifizierungskonzept muss beschreiben, welche Informationen der Zertifizierungsdiensteanbieter in seine Dokumentation aufnimmt. Die Dokumentation muss zumindest folgende Angaben umfassen: welche öffentliche Schlüssel welchen Personen zugeordnet sind (vgl. Kapitel 2 a), Angaben zur Identitätsprüfung (insbesondere bei Verwendung von Pseudonymen) und allfälligen Prüfungen der Vertretungsbefugnis, Angaben zum Widerruf des Zertifikates, Verträge zwischen Signator bzw. Machtgeber und Zertifizierungsdiensteanbieter.
- Speicherung der Signaturerstellungsdaten: Das Sicherheits- und Zertifizierungskonzept muss beschreiben, ob die privaten Schlüssel in nicht auslesbaren Signaturerstellungseinheiten gespeichert werden. Falls auslesbare Signaturerstellungseinheiten eingesetzt werden, muss das Sicherheits- und Zertifizierungskonzept vorsehen, dass die Signatoren vertraglich zu entsprechenden Sicherheitsmaßnahmen verpflichtet werden (vgl. Kapitel 2 c).
- Algorithmen und Parameter: Das Sicherheits- und Zertifizierungskonzept muss vorsehen, dass nur Algorithmen und Parameter eingesetzt werden, die auch für sichere elektronische Signaturen geeignet sind.

## 5. Empfehlungen

### 5.1. Empfehlungen für Personen, die fortgeschrittene elektronische Signaturen erstellen wollen

Personen, die fortgeschrittene elektronische Signaturen erstellen wollen, wird zunächst empfohlen, zu prüfen, ob sie dafür qualifizierte Zertifikate für die sichere elektronische Signatur einsetzen können. Dies kann insbesondere dann eine geeignete Lösung sein, wenn wenige Signaturen erstellt werden und es daher möglich ist, jede einzelne Signaturerstellung durch PIN-Eingabe auszulösen. Bei Verwendung der sicheren elektronischen Signatur sind die höchstmöglichen Sicherheitsanforderungen erfüllt und es stellen sich keine Zweifelsfragen, ob die Anforderungen des § 2 Z 3 lit. a bis d SigG erfüllt sind.

Wenn es sich nicht als praktikabel erweist, einzelne Signaturen zu erstellen, sollten die oben in Kapitel 3 beschriebenen Möglichkeiten, wie man mittels eines Servers signieren kann, geprüft werden. Zu beachten ist dabei insbesondere, dass das verwendete Zertifikat an eine natürliche Person ausgestellt werden muss. Aus Sicherheitsgründen empfehlenswert ist es, für die Speicherung des privaten Schlüssels spezielle Hardware (nicht auslesbare Datenträger wie Chipkarten und HSMs) zu verwenden. Wenn dies nicht möglich ist, müssen zumindest Sicherheitsmaßnahmen ergriffen werden, die es gewährleisten, dass sich der private Schlüssel unter der alleinigen Kontrolle der betreffenden Person befinden.

Einen Überblick über die österreichischen Zertifizierungsdienste bietet die Aufsichtsstelle auf ihrer Website (<http://www.signatur.rtr.at/de/providers/services.html>).

### 5.2. Empfehlungen für Personen, welche eine fortgeschrittene elektronische Signatur prüfen wollen

Prüfen Sie das Zertifikat, auf welchem die Signatur beruht. Aus dem Issuer-Feld des Zertifikates können Sie den Namen des Zertifizierungsdiensteanbieters entnehmen, weiters geht daraus die Bezeichnung des Zertifizierungsdienstes hervor. Wenn es sich um einen österreichischen Zertifizierungsdienst handelt, finden Sie weitere Informationen zu diesem Zertifizierungsdienst auf der Website der Aufsichtsstelle (<http://www.signatur.rtr.at/de/providers/services.html>).

Über das sichere Verzeichnis der Aufsichtsstelle (<http://www.signatur.rtr.at/de/directory/>) können Sie außerdem eine Zertifikatskette bis zum TOP-Zertifikat der Aufsichtsstelle prüfen und so Gewissheit darüber erlangen, dass es sich tatsächlich um einen der Aufsichtsstelle bekannten Zertifizierungsdienst handelt. Handelt es sich um einen ausländischen Zertifizierungsdienst, dann finden Sie möglicherweise auf der Website der Aufsichtsstelle des jeweiligen Landes weitere Informationen zum betreffenden Zertifizierungsdienst. Unter <http://www.signatur.rtr.at/de/links/> finden Sie Links zu zahlreichen Aufsichtsstellen.

Handelt es sich um einen Zertifizierungsdienst, bei dem qualifizierte Zertifikate für sichere elektronische Signaturen ausgestellt werden, dann sind die Anforderungen des § 2 Z 3 lit. a bis d SigG an die Signatur zweifellos erfüllt. Darüber hinaus kann man – da es sich um sichere elektronische Signaturen handelt und auch § 2 Z 3 lit. e SigG erfüllt ist – davon ausgehen, dass für die Erstellung der Signatur Technologie verwendet wurde, welche die höchstmöglichen Sicherheitsanforderungen erfüllt und dass die Identität des Signators vor der Ausstellung des Zertifikates anhand eines amtlichen Lichtbildausweises geprüft worden ist. Aus der Signatur ergibt sich allerdings nicht eine allfällige Vertretungsbefugnis. Beispielsweise könnte eine Rechnung zwar sicher elektronisch signiert worden sein, der Signator aber gar nicht bevollmächtigt gewesen sein, Rechnungen für das im Text der Rechnung genannte Unternehmen zu signieren.

Ist auf der Website der Aufsichtsstelle zum betreffenden Zertifizierungsdienst angegeben, dass bei diesem Zertifizierungsdienst Zertifikate für fortgeschrittene elektronische Signaturen angeboten werden, dann hat sich der Zertifizierungsdiensteanbieter in seinem Sicherheits- und Zertifizierungskonzept zur Einhaltung der oben in Kapitel 4 genannten Punkte verpflichtet. Man kann daher davon ausgehen, dass die Identität des Signators vor der Ausstellung des Zertifikates geprüft worden ist, dass sich die Signaturerstellungsdaten in seiner alleinigen Kontrolle befinden und dass daher die Anforderungen des § 2 Z 3 lit. a bis d SigG an die Signatur erfüllt sind. Im Einzelfall wäre aber denkbar, dass diese Anforderungen nicht erfüllt sind, z. B. wenn der private Schlüssel auf auslesbaren Datenträgern gespeichert wurde und der Signator vertragliche Verpflichtungen, fremden Zugriff auf den privaten Schlüssel zu verhindern, nicht ausreichend beachtet hat.

Ist auf der Website der Aufsichtsstelle zum betreffenden Zertifizierungsdienst weder angegeben, dass dieser für sichere elektronische Signaturen bestimmt ist, noch, dass er für fortgeschrittene elektronische Signaturen bestimmt ist, dann wäre im Einzelfall zu prüfen, ob die Anforderungen des § 2 Z 3 lit. a bis d SigG an die Signatur erfüllt sind.

### **5.3. Empfehlungen für Zertifizierungsdiensteanbieter**

Zertifizierungsdiensteanbietern, die keine qualifizierten Zertifikate für die sichere elektronische Signatur anbieten, die aber einen Zertifizierungsdienst aufnehmen wollen, der die Anforderungen des § 2 Z 3 lit. a bis d SigG erfüllt, wird Folgendes empfohlen:

- bei diesem Zertifizierungsdienst die Unterstützung von nicht auslesbaren Signaturerstellungseinheiten (z. B. Chipkarten, HSMs) anzubieten oder mehrere, klar voneinander unterscheidbare Zertifizierungsdienste anzubieten: einen, bei dem die privaten Schlüssel ausschließlich in solcher Hardware gespeichert werden, und einen, bei dem die privaten Schlüssel auch auf auslesbaren Datenträgern gespeichert werden können;
- wenn die privaten Schlüssel auch auf auslesbaren Datenträgern gespeichert werden können, die Signatoren vertraglich zu Sicherheitsmaßnahmen zu verpflichten und auch in das Sicherheits- und Zertifizierungskonzept aufzunehmen, dass Zertifikate nur an Personen ausgestellt werden, die sich dazu vertraglich verpflichtet haben;

- im Sicherheits- und Zertifizierungskonzept folgendes klar zu beschreiben: welche Attribute im Subject-Feld des Zertifikates verwendet werden (z. B. commonName, organizationName) und was die Bedeutung dieser Attribute ist (z. B. dass durch eine Eintragung im organizationName eine Vertretungsbefugnis für diese Organisation ausgedrückt werden soll), dass Zertifikate nur an natürliche Personen ausgestellt werden, wie die Überprüfung der Angaben im Zertifikat erfolgt (z. B.: Überprüfung der Identität der natürlichen Person, Überprüfung der Existenz und Identität der wahlweise ins organizationName-Attribut einzutragenden juristischen Person und Überprüfung, dass die natürliche Person für die juristische Person vertretungsbefugt ist);
- wenn das organizationName-Attribut dazu verwendet wird, eine Vertretungsbefugnis zum Ausdruck zu bringen, im Sicherheits- und Zertifizierungskonzept vorzusehen, dass die eingetragene Organisation von der Ausstellung des Zertifikates informiert wird und sie die Möglichkeit (bzw. evtl. auch die vertragliche Verpflichtung) hat, das Zertifikat widerrufen zu lassen, wenn die Vertretungsbefugnis erlischt.

## Anhang

### **Verordnung des Bundesministers für Finanzen, mit der die Anforderungen an eine auf elektronischem Weg übermittelte Rechnung bestimmt werden, BGBl. II Nr. 583/2003.**

Auf Grund des § 11 Abs. 2 UStG 1994, BGBl. Nr. 663/1994, in der Fassung BGBl. I Nr. 71/2003 wird verordnet:

Die Echtheit der Herkunft und die Unversehrtheit des Inhalts einer auf elektronischem Weg übermittelten Rechnung ist gewährleistet,

1. wenn die Rechnung mit einer Signatur versehen ist, die den Erfordernissen des § 2 Z 3 lit. a bis d Signaturgesetz entspricht und auf einem Zertifikat eines Zertifizierungsdiensteanbieters im Sinne des Signaturgesetzes beruht, oder
2. wenn die Rechnung durch elektronischen Datenaustausch (EDI) gemäß Artikel 2 der Empfehlung 1994/820/EG der Kommission vom 19. Oktober 1994 über die rechtlichen Aspekte des elektronischen Datenaustausches (ABl. EG Nr. L 338, S 98) übermittelt wird, wenn in der Vereinbarung über diesen Datenaustausch der Einsatz von Verfahren vorgesehen ist, die die Echtheit der Herkunft und die Unversehrtheit der Daten gewährleisten, und zusätzlich eine zusammenfassende Rechnung auf Papier oder unter den Voraussetzungen der Z 1 auf elektronischem Weg übermittelt wird.

### **ETSI TS 101 456 V 1.2.1 (2002-04)**

#### **Policy requirements for certification authorities issuing qualified certificates**

7.3.1. c): “The service provider shall verify by appropriate means in accordance with national law, the identity and, if applicable, any specific attributes of the person to which a qualified certificate is issued. Evidence of the identity shall be checked against a physical person either directly or indirectly using means which provides equivalent assurance to physical presence (see note 3). Submitted evidence may be in the form of either paper or electronic documentation. NOTE 3: An examples of evidence checked indirectly against a physical person is documentation presented for registration which was acquired as the result of an application requiring physical presence.”

**ETSI TS 102 042 V1.1.1 (2002-04)**

**Policy requirements for certification authorities issuing public key certificates**

7.3.1. c): “The service provider shall collect either direct evidence, or an attestation from an appropriate and authorized source, of the identity (e.g. name) and, if applicable, any specific attributes of subjects to whom a certificate is issued. Submitted evidence may be in the form of either paper or electronic documentation. Verification of the subject's identity shall be by appropriate means and in accordance with national law.”