

Begutachtung des Konzeptes für die Public Key Infrastruktur der EAN (Schweiz) - TC TrustCenter AG

Version final
1. Oktober 2002

Die Eidgenössische Steuerverwaltung ESTV verlangt:

„Der Gutachter hat in seinem Gutachten

- a) nachzuweisen, dass er über die notwendigen Qualifikationen verfügt, um beurteilen zu können, ob die zu prüfenden Unterlagen die nach Art. 12 Abs. 2 und Art. 2 a und c notwendigen Nachweise liefern;
- b) zu bestätigen, dass er unabhängig vom Verfasser der Analyse (auf Grundlage der Checkliste) und dessen Auftraggebern handelt und sämtliche Verbindungen offen legt, die in irgendeiner Weise zu Interessenkollisionen oder –konflikten in seiner Funktion als Gutachter Anlass geben könnten;
- c) eindeutig das Ergebnis seiner formellen und materiellen Prüfungen hinsichtlich der Konformität zu Art. 12 Abs. 2 und Art. 2 Abs. 2 a und c zu erklären und einlässlich zu begründen;
- d) zu erklären, dass er mit der Offenlegung seiner Identität als Gutachter durch die Eidgenössische Steuerverwaltung einverstanden ist.“

a) Nachweis der notwendigen Qualifikation

Diesen Nachweis erbringe ich aufgrund der nachfolgenden Angaben; diese sind zeitlich geordnet, beginnend mit der Tätigkeit im Jahr 2002:

- Review of project LA MER (Public Key Infrastructure Based on Smart Cards in South Eastern Europe) of the European Commission, DG Information Society.
- Im Auftrag von BIT Mitwirkung in der Arbeitsgruppe PKI-Koordination Bund und Kantone:
 - Organisationshandbuch für die PKI-Koordination BVerw und Kantone;
 - Standard für den Einsatz von Smartcards für End-Benutzer im PKI-Umfeld;
 - Weisung zur Aufnahme einer Zertifizierungsdienst-Anbieterin in die „Trusted List“ der Bundesverwaltung
- Mitwirkung beim Aufbau des Zertifizierungsdienstes der Swisskey AG als Weiterentwicklung von DigiSigna (gemeinsames Projekt der CH-Handelskammern und Telekurs)
- Im Auftrag von CS und UBS Teilnahme am Projekt „Global Trust Authority – GTA“ einer Reihe von Europäischen Grossbanken; dabei Aufsetzen einer Certification Authority für Testzwecke (Baltimore Unicert und MS Win2000 Certification Services).
- Seitens Zürcher Handelskammer Partner im EU-Projekt COSACC (Coordination Of Security Activities of Chambers of Commerce); dabei Aufsetzen einer Certification Authority (Baltimore Unicert).
- Aufbau eines EDI-Clearing Centers Swisscos, welches 1992 von der damaligen PTT übernommen wurde und später in den e-commerce Bereich von Swisscom integriert wurde.
- Teilnahme an EU-Projekten FAST (First Attempt to Secure Trade) und EDIRA (EDI Registration Authority)
- Vorgängig Leitung der Firma Oerlikon Bühle Rechenzentrum AG und der Informatik Stabsstelle im Oerlikon Bühle Konzern; verantwortlich für komplexe Informatikinfrastrukturen.
- Tätigkeit als Privatdozent für Operations Research und Informatik an der Universität Zürich.
- Leitung einer Beratungsabteilung bei Fides Treuhand-Vereinigung (heute in KPMG aufgegangen)
- Oberassistent am ersten Rechenzentrum der Universität Zürich.

- Studienaufenthalt am Operations Research Center des MIT, Cambridge, Mass, USA
- Studium Betriebswirtschaft an der HSG und Uni Zürich mit Zusatzausbildung in Mathematik; Abschluss Dr. oec. publ.

b) Bestätigung der Unabhängigkeit

Ich bestätige, dass ich gegenüber TC-TrustCenter (Verfasser der Analyse) und deren Auftraggeber EAN (Schweiz), Syntrade AG in Pfäffikon SZ, sowie der Firma KeyON AG in Rapperswil SG unabhängig bin. Mit keiner dieser Firmen besteht zur Zeit ein Vertragsverhältnis. Mit Syntrade AG bestand 2001 ein Beratungsmandat bezüglich „Elektronische Signatur für MWSt-relevante Dokumente“, darin eine Stellungnahme zum Entwurf des EIDI-V.

c) Ergebnis der formellen und materiellen Prüfungen hinsichtlich Konformität zu Art. 12 Abs. 2 und Art. 2 Abs. 2 a und c

Aufgrund der Vorgaben seitens ESTV für die Abschnitte *EIDI-V* und *ZertDV* habe ich die formelle und materielle Prüfung vorgenommen. Ich erkläre, dass die Ausstellung der Zertifikate und die Zertifikate selbst konform zu EIDI-V Art. 12 Abs. 2 und Art. 2 Abs. 2 a und c sind. Die einlässliche Begründung erfolgt in den Abschnitten *EIDI-V* und *ZertDV* dieses Dokumentes.

d) Einverständnis mit der Offenlegung der Identität als Gutachter

Ich bin einverstanden mit der Offenlegung meiner Identität:

Dr. Otto Müller

Inhaber der im Handelsregister eingetragenen Einzelfirma

Dr. Otto Müller Consulting

Alte Landstr. 19

8803 Rüschlikon

e-mail: omueller@zurichcci.ch

Begutachtung gemäss Checkliste Analyse Art.12 Abs. 2 EIDI-V

EIDI-V (Verordnung des EFD über elektronisch übermittelte Daten und Informationen)

Art.	Abs.	Kommentar
2	2a	<p>Aus dem Abschnitt <i>ZertDV</i> geht hervor, dass</p> <ul style="list-style-type: none"> - die Zertifikate von einem Zertifizierungsdienst-Anbieter (TC-Trustcenter AG) ausgestellt werden, welcher einer mit ZertDV vergleichbaren gesetzlichen Regelung unterliegt; - der Inhalt der Zertifikate der ZertDV entspricht und der Standard X.509 v3 eingehalten wird. <p>Die im Abschnitt <i>ZertDV</i> erwähnten Abweichungen können begründet werden. Somit beruhen die Zertifikate auf den Bestimmungen von ZertDV.</p>
2	2c	<p>Als Träger-Medien des privaten Schlüssels sind gemäss Basis-Konzept Smartcards von Gieseke & Devrient sowie Hardware Security Modules von nCipher vorgesehen.</p> <p>Smartcard: Enthält RSA-Chip (Philips P8WE 5032) mit StarCOS SPK 2.3 Betriebssystem und StarCert 2.2-Applikation. Sowohl der Chip als auch dessen Betriebssystem sind ITSec E4 hoch evaluiert. Das gesamte System ist SigV-zertifiziert (vgl. T-Systems. 02078.TE.12.2001).</p> <p>Die Schlüssel-Generierung erfolgt bei TC TrustCenter nach RegTP-Richtlinien für anerkannte Zertifizierungsdienst-Anbieter, welche Schlüssel-Hinterlegung beim Zertifizierungsdienst nicht erlaubt. Somit ist die Anforderung der alleinigen Kontrolle erfüllt.</p> <p>Hardware Security Module (HSM): Als HSMs kommen nShield-Produkte des Herstellers nCipher zum Einsatz. Alle nShield-Produkte sind FIPS 140-1 Level 2 oder 3 evaluiert (vgl. NIST: FIPS 140-1 Validation Certificates 221-224).</p> <p>Die Prozedur für HSMs sieht vor, dass der Inhaber des Schlüssels diesen im HSM generiert und unter alleiniger Kontrolle des Inhabers bleibt. Somit ist die Anforderung der alleinigen Kontrolle erfüllt.</p>

ZertDV (Zertifizierungsdiensteverordnung)

Legende:

- vergleichbare Gesetzgebung erforderlich
- ZertDV-Konformität erforderlich (gestützt auf EIDI-V)
- vergleichbare Gesetzgebung und ZertDV-Konformität erforderlich

Art.	Abs.	Kommentar
2		
	f	Die Definition der digitalen Signatur im ZertDV besagt, dass es sich um die Verwendung öffentlicher und der zugehörigen privaten Schlüssel, also asymmetrischer Schlüssel-Paare handelt. In der EAN-PKI wird gemäss Basis-Konzept der RSA-Algorithmus verwendet, also ein asymmetrisches Schlüsselverfahren. Dies entspricht der Anforderung dieses Artikels exakt.
	g	SigG § 18 "Anerkennung von Prüf- und Bestätigungsstellen" (1): <i>„Die zuständige Behörde erkennt eine natürliche oder juristische Person auf Antrag als Bestätigungsstelle nach [...] an, wenn diese die für die Tätigkeit erforderliche Zuverlässigkeit, Unabhängigkeit und Fachkunde nachweist. ...“</i> Gemäss SigG kann ein private Stelle im Sinne einer Anerkennungsstelle gem. ZertDV zugezogen werden. Im ZertDV ist eine solche Stelle zuständig. Die Vergleichbarkeit ist somit gegeben. TC-TrustCenter ist von der Regulierungsbehörde für Telekommunikation und Post (Reg TP) am 4.12.01 direkt anerkannt worden. RegTP ist die zuständige Behörde gemäss Gesetz zur digitalen Signatur. Somit wurde TC-TrustCenter von einer vergleichbaren Anerkennungs-/Akkreditierungs-Stelle anerkannt. (Vgl. TUVIT.09403.SE.12.2001 - RegTP-Akkreditierungsurkunde vom 4.12.2001.)
3		
	1	ZertDV sagt aus, dass eine Anbieterin von Zertifizierungsdiensten sich anerkennen lassen kann, wenn sie in der Lage ist, Zertifikate gemäss der Verordnung auszustellen und zu verwalten. Falls die Anbieterin von Zertifizierungsdiensten die Anforderungen erfüllt, muss sie meiner Ansicht nach anerkannt werden. Die „kann – Formulierung“ ist somit kein Gegensatz zur Formulierung nach deutschem Signaturgesetz, wonach die Anerkennung erfolgen muss, wenn der notwendige Nachweis erbracht werden kann.(SigG § 15 „Freiwillige Akkreditierung von Zertifizierungsdiensteanbietern“ (1): <i>„Zertifizierungsdiensteanbieter können sich auf Antrag von der zuständigen Behörde akkreditieren lassen; die zuständige Behörde kann sich bei der Akkreditierung privater Stellen bedienen. Die Akkreditierung ist zu erteilen, wenn der Zertifizierungsdiensteanbieter nachweist, dass die Vorschriften nach diesem Gesetz und der Rechtsverordnung nach § 24 erfüllt sind. ...“</i>) Die Vergleichbarkeit ist somit gegeben.

Art.	Abs.	Kommentar
	2	<p>ZertDV erfordert, dass für die Anerkennung der Anbieterin von Zertifizierungsdiensten durch SAS eine akkreditierte Anerkennungsstelle in Anspruch genommen wird, falls eine solche existiert (was in der CH zutrifft). Gemäss deutschem Signaturgesetz kann sich RegTP für die Anerkennung der Anbieterin von Zertifizierungsdiensten einer privaten Stelle bedienen. (SigG § 15 „Freiwillige Akkreditierung von Zertifizierungsdiensteanbietern“ (1): <i>„Zertifizierungsdiensteanbieter können sich auf Antrag von der zuständigen Behörde akkreditieren lassen; die zuständige Behörde kann sich bei der Akkreditierung privater Stellen bedienen. Die Akkreditierung ist zu erteilen, wenn der Zertifizierungsdiensteanbieter nachweist, dass die Vorschriften nach diesem Gesetz und der Rechtsverordnung nach § 24 erfüllt sind. ...“</i>) Daraus ergibt sich kein Widerspruch. Die Vergleichbarkeit ist somit gegeben.</p>
4		
	1	<p>Die Anforderungen gemäss a-f werden durch die deutsche SigV insbesondere im § 1 „Form, Inhalt und Änderung der Anzeige“ (2) generell abgedeckt: <i>„Die Anzeige muss folgende Angaben und Unterlagen umfassen:</i></p> <ol style="list-style-type: none"> <i>1. den Namen und die Anschrift des Zertifizierungsdiensteanbieters,</i> <i>2. die Namen der gesetzlichen Vertreter,</i> <i>3. aktuelle Führungszeugnisse nach § 30 Abs. 5 des Bundeszentralregistergesetzes für den Zertifizierungsdiensteanbieter und seine gesetzlichen Vertreter,</i> <i>4. einen aktuellen Handelsregisterauszug oder eine vergleichbare Unterlage,</i> <i>5. Belege zum Nachweis der erforderlichen technischen, administrativen und juristischen Fachkunde nach § 4 Abs. 2 Satz 3 des Signaturgesetzes,</i> <i>6. ein Sicherheitskonzept mit einer genauen Darlegung, wie dieses umgesetzt ist, einschließlich der Übertragung von Aufgaben an Dritte nach § 4 Abs. 5 des Signaturgesetzes, und</i> <i>7. einen Nachweis der Deckungsvorsorge nach § 12 des Signaturgesetzes.</i> <p><i>Ändern sich die Umstände nach Satz 1 Nr. 1 oder Nr. 2 oder sicherheitserhebliche Umstände nach Satz 1 Nr. 6, ist die zuständige Behörde schriftlich oder mittels eines mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehenen elektronischen Dokuments zu informieren. § 2 bleibt unberührt.“</i>Somit ist die Vergleichbarkeit mit ZertDV 4.1. a-e gegeben. ZertDV 4.1 f regelt die Deckungsvorsorge für Haftung ohne Verschulden mittels Regelung in den Allgemeinen Geschäftsbedingungen. SigV § 1 (2) 7 regelt diese Deckungsvorsorge nach § 12 des SigG. Somit ist die Vergleichbarkeit mit ZertDV 4.1. f auch gegeben. Durch die Erfüllung von SigV wird das anwendbare deutsche Recht erfüllt. Somit ist auch die Vergleichbarkeit mit ZertDV 4.1.g gegeben.</p>
5		
	2	<p>SigG §16 „Zertifikate der zuständigen Behörde“ (2): <i>„Die zuständige Behörde hat</i></p> <ol style="list-style-type: none"> <i>1. die Namen, Anschriften und Kommunikationsverbindungen der akkreditierten Zertifizierungsdiensteanbieter,</i> <i>2. den Widerruf oder die Rücknahme einer Akkreditierung,</i> <i>3. die von ihr ausgestellten qualifizierten Zertifikate und deren Sperrung und</i> <i>4. die Beendigung und die Untersagung des Betriebes eines akkreditierten Zertifizierungsdiensteanbieters jederzeit für jeden über öffentlich erreichbare Kommunikationsverbindungen nachprüfbar und abrufbar zu halten.“</i> <p>Die Vergleichbarkeit ist somit gegeben.</p>

Art.	Abs.	Kommentar
6		<p>ZertDV verweist auf die Ausführungsvorschriften (OSCERT). Die deutsche SigV vom 16. November 2001 verweist auf Anlage 1 (zu § 11 Abs. 3, § 15 Abs. 5 und § 16 Abs. 2) „Vorgaben für die Prüfung von Produkten für qualifizierte elektronische Signaturen“.</p> <p>Gemäss den Ausführungsvorschriften (OSCERT) gilt:</p> <p>2.10.2 „Generierung des Schlüssels der Antragstellerin eines Zertifikats“:</p> <p><i>„Anforderung 2: Um die Schlüssel für die Antragstellerinnen der Zertifikate zu generieren, muss die CSP einen Algorithmus verwenden, der den Empfehlungen [7] der Gruppe ALGO von EESSI entspricht. In der Aussage der Zertifizierungspraxis (CPS) muss die CSP die für die Generierung der Schlüssel der Antragstellerinnen verwendeten Parameter veröffentlichen.</i></p> <p><i>Anforderung 3: Wenn die CSP die Schlüssel einer Antragstellerin des Zertifikats generiert, muss sie:</i></p> <ul style="list-style-type: none"> - <i>den privaten Schlüssel in einer Einrichtung sichern, die gegen alle Eindringversuche geschützt ist (unverletzliche Einrichtung) und kein Kopieren oder Extrahieren des privaten Schlüssels aus der Einrichtung (z. B. einer Chipkarte) erlaubt.</i> <p><i>Anforderung 6: Die Antragstellerin eines Zertifikats, die ihre Schlüssel generiert, muss einen Algorithmus verwenden, der den Empfehlungen [7] der Gruppe ALGO von EESSI entspricht.</i></p> <p><i>Um ihre Schlüssel zu generieren, muss die Antragstellerin eine Einrichtung verwenden, die gegen alle Eindringversuche geschützt ist (unverletzliche Einrichtung) und kein Kopieren oder Extrahieren des privaten Schlüssels aus der Einrichtung (z. B. einer Chipkarte) erlaubt.“</i></p> <p>SIGV Anlage 1 verlangt für die Signaturestellungseinheit des Kunden eine Zertifizierung nach Common Criteria „EAL3“ bzw. nach ITSEC „E2“. Die erlaubten Algorithmen werden im Bundesanzeiger publiziert. („Die Eignung ist jährlich sowie bei Bedarf neu zu bestimmen.“)</p> <p>Die Vergleichbarkeit ist somit gegeben.</p>

Art.	Abs.	Kommentar
7		
	1	<p>Da die EAN-PKI die Zertifikate gemäss X.509 Standard ausstellt, sind die Mindestangaben gemäss ZertDV wie folgt erfüllt:</p> <ul style="list-style-type: none"> a. Seriennummer: durch X.509 Standard gegeben b. Hinweis auf ZertDV: Kann durch TC TrustCenter nicht erfüllt werden. Jedoch wird ein Hinweis eingefügt, dass es für die digitale Signatur von Mehrwertsteuerbelegen verwendet werden kann. c. Nutzungsbeschränkungen: Keine Beschränkungen vorgesehen, deshalb ist kein Hinweis nötig. d. Name des Inhabers: gemäss Basis-Konzept 4.2.18.1 besteht der Name des Inhabers aus der Angabe der juristischen Person und der Angabe der verantwortlichen natürlichen Person. Gemäss TC-TrustCenter Certificate Policy ist die Angabe der natürlichen Person zwingend. e. öffentlicher Schlüssel: durch X.509 Standard gegeben f. Gültigkeitsdauer: durch X.509 Standard gegeben g. Name/digitale Signatur des Ausstellers: durch X.509 Standard gegeben <p>Kommentar:</p> <ul style="list-style-type: none"> b. kann nicht erfüllt werden, da die Zertifikate EIDI-V Art.12 konform und nicht ZertDV-konform sind. Diese EIDI-V-12-Konformität wird mittels eines „Policy Qualifier CPS URI“ hergestellt. Dies ist ein URI innerhalb der Domäne von TC-Trustcenter. d. Gemäss Besprechung vom 9.8.02 mit den Herren Egger und Scheuner war dieser Punkt noch offen. Nunmehr verlangt die TC-TrustCenter Certificate Policy zwingend die Nennung einer natürlichen Person im Common Name. <p>Ich bin der Meinung, dass die Formulierung von b. die Forderung von ZertDV analog erfüllt. Unter diesem Vorbehalt sind somit die Anforderungen der ZertDV exakt erfüllt.</p>

Art.	Abs.	Kommentar
	2	<p>Zertifikatsformat gemäss Ausführungs-Bestimmungen 2.9.1 & 2.9.2: 2.9.1. Anforderung 2 : ist erfüllt, mit Ausnahme des fehlenden Eintrages der e-mail-Adresse im Distinguished Name.</p> <p>Kommentar: Meiner Meinung nach ist das Einfügen der e-mail-Adresse aus folgenden Gründen nicht notwendig:</p> <ul style="list-style-type: none"> - Die vorgesehene Applikation implementiert keine e-mail-Funktion. Aus technischer Sicht ist die e-mail-Adresse überflüssig. - Gemäss Basis-Konzept 3.5.1 wird die e-mail-Adresse der technischen Kontaktperson bei der Registrierung aufgenommen. Folglich ist der RA die e-mail-Adresse bekannt. - Für die Eindeutigkeit des Distinguished Names ist die e-mail-Adresse nicht notwendig. Der Eintrag im O-Feld erfolgt gemäss HR-Auszug (oder entsprechend) und ist deshalb eindeutig. <p>2.9.2 Anforderung 1: keyUsage: Die Ausführungs-Bestimmungen verlangen: „...das zusätzliche Feld keyUsage einfügen, um anzuzeigen, dass das Zertifikat ausschliesslich zur Überprüfung der Unterschrift und für die Authentifizierung verwendet wird“. Im Gegensatz dazu wird im Zertifikats-Profil der EAN-PKI aber im Feld keyUsage auch noch „Key Encipherment“ gesetzt. Dies ist nötig, weil gängige Browser (fälschlicherweise) dieses „Key Encipherment“ bei SSL-Client-Zertifikaten verlangen. SSL-Client-Authentifizierung wiederum wird benötigt, damit der End-User die Revokation des Zertifikates bei TC-TrustCenter mit seinem privaten Schlüssel vornehmen kann (vgl. CPS 3.4). certificatePolicies: Object Identifier (OID) für ZertDV-Erfüllung darf nicht eingefügt werden. Vgl. 7.1. dieses Dokumentes crlDistributionPoint: erfüllt</p> <p>Kommentar: Durch das Setzen von „Key Encipherment“ in den Zertifikaten, wird es möglich, diese auch für Verschlüsselungs-Zwecke einzusetzen. Da der private Schlüssel nur einmal auf der Smartcard / dem HSM vorhanden sein darf, kann der Verlust des privaten Schlüssels zu Daten-Verlust führen. Die Zertifikate sind also für Verschlüsselung ungeeignet. Darauf sollte der End-User hingewiesen werden: Keine Archivierung verschlüsselter Information, vor allem nicht MWSt-relevanter Daten.</p> <p>Aussage: Die Anforderungen von ZertDV sind nicht exakt erfüllt. Die Abweichungen sind aber klar begründet.</p>
8		
	1	<p>Das Basiskonzept regelt die Registrierung bei der EAN-Registrierstelle. Danach sind die in Art. 8 gestellten Anforderungen gemäss Basis-Konzept 3.2.1 „Identifizierung und Registrierung“ alle erfüllt.</p>
	2	<p>ZertDV erlaubt bei der Erneuerung die Verwendung des alten Zertifikates, sofern die Erstregistrierung weniger als 10 Jahre zurückliegt. TC-TrustCenter erwähnt in CPD 4.4. (Class 3 Zertifikate) die Möglichkeit einer Zertifikatserneuerung aufgrund des alten Zertifikates nicht. Folglich ist sie nicht erlaubt. Die Richtlinie von TC-TrustCenter ist einschränkender als ZertDV. Somit ist die Anforderung exakt erfüllt.</p>

9	Vergleichbarkeit	Erfüllung
1	<p>SigV §6 „Ausgestaltung der Unterrichtung“ regelt die Unterrichtung des Antragstellers und setzt Mindestanforderungen. Auch Dritte müssen auf Antrag informiert werden. Wie diese Information zu erfolgen hat, ist nicht vorgeschrieben. Die Vergleichbarkeit ist somit gegeben.</p>	<p>CPD und allgemeine Geschäftsbedingungen sind auf der Website von TC-TrustCenter verfügbar. Somit ist exakte Erfüllung gegeben.</p>
2	<p>In SigV wird die Information über die Folgen eines möglichen Missbrauchs nicht explizit verlangt. Aus §6 „Ausgestaltung der Unterrichtung“ geht sie aber implizit hervor. („... 1. die Aufbewahrung und Anwendung der sicheren Signaturerstellungseinheit und geeignete Maßnahmen im Verlustfalle oder bei Verdacht des Mißbrauchs, 2. die Geheimhaltung von persönlichen Identifikationsnummern oder anderen Daten zur Identifikation des Signaturschlüssel-Inhabers gegenüber der sicheren Signaturerstellungseinheit, ...“) Somit ist die Vergleichbarkeit gegeben.</p>	<p>In den auf der Website von TC-TrustCenter publizierten Allgemeinen Geschäftsbedingungen AGB sind in B „Pflichten des Kunden 4 Sorgfalts- und Mitwirkungspflichten des Zertifikatsinhabers“ die Folgen eines möglichen Missbrauchs detailliert beschrieben, nämlich in 4.1 Sperrung des Zertifikates bei Verlust der Smartcard in 4.2 Geheimhaltung von Identifikationsnummern und Passwörtern Somit sind die Anforderungen exakt erfüllt.</p>
10	<p>SigG § 5 (4) und §17 (3) verbieten eine Speicherung des privaten Signier-Schlüssels ausserhalb der Signaturerstellungseinheit. (§ 5 „Vergabe von qualifizierten Zertifikaten“ (4): „... Er [der Zertifizierungsdiensteanbieter] hat weiter Vorkehrungen zu treffen, um die Geheimhaltung der Signaturschlüssel zu gewährleisten. Eine Speicherung von Signaturschlüsseln außerhalb der sicheren Signaturerstellungseinheit ist unzulässig.“ § 17 „Produkte für qualifizierte elektronische Signaturen“ (3): „Die technischen Komponenten für Zertifizierungsdienste müssen Vorkehrungen enthalten, um 1. bei Erzeugung und Übertragung von Signaturschlüsseln die Einmaligkeit und Geheimhaltung der Signaturschlüssel zu gewährleisten und eine Speicherung außerhalb der sicheren Signaturerstellungseinheit auszuschließen,...“) Die Vergleichbarkeit ist somit gegeben. Im übrigen wird bei TC-TrustCenter der Schlüssel auf einer zertifizierten Smartcard generiert, und kann somit nicht exportiert werden. Die Anforderungen von ZertDV sind erfüllt.</p>	

11		
	1	<p>SigG § 8 „Sperrung von qualifizierten Zertifikaten“ (1): <i>„Der Zertifizierungsdiensteanbieter hat ein qualifiziertes Zertifikat unverzüglich zu sperren, wenn ein Signaturschlüssel- Inhaber oder sein Vertreter es verlangt. ...“</i> Somit ist die Vergleichbarkeit gegeben.</p>
	2	<p>SigV § 7 „Sperrung von qualifizierten Zertifikaten“ (2): <i>„Der Zertifizierungsdiensteanbieter hat sich vor Sperrung auf geeignete Weise von der Identität des zur Sperrung Berechtigten zu überzeugen.“</i> Die in ZertDV erwähnte Möglichkeit, die Sperrung mit dem Schlüssel des zu sperrenden Zertifikates vorzunehmen, ist eine Möglichkeit unter anderen. Somit ist die Vergleichbarkeit gegeben.</p>
	3	<p>SigG § 8 „Sperrung von qualifizierten Zertifikaten“ (1): <i>„...wenn[...] das Zertifikat auf Grund falscher Angaben zu § 7 ausgestellt wurde“</i>. In § 7 werden die notwendigen Angaben zum Inhaber des Zertifikates aufgezählt. Somit ist die Vergleichbarkeit zum ersten Satz von Abs. 3 gegeben. Der zweite Satz von ZertDV Abs. 3 lautet <i>„... wenn (die Zertifikate)[...] keine Gewähr mehr für die Zuordnung zu einer bestimmten Person oder Verwaltungseinheit bieten“</i>. Im deutsch Recht findet sich keine Entsprechung, die Aussage ist aber implizit vorhanden. Somit ist die Vergleichbarkeit bedingt gegeben.</p>
	4	<p>Im SigG, resp. SigV ist eine Suspendierung von Zertifikaten nicht vorgesehen. Somit ist keine vergleichbare Bestimmung vorhanden. Gemäss ZertDV besteht keine Verpflichtung, Suspendierung anzubieten. Suspendierung ist in der EAN-PKI auch nicht vorgesehen. Das deutsche SigG setzt engere Bedingungen als ZertDV. Somit kann von einer Erfüllung von ZertDV ausgegangen werden. Die Vergleichbarkeit steht nicht zur Diskussion.</p>
	5	<p>Die Verpflichtung zur Benachrichtigung des Inhabers des gesperrten Zertifikates ist im SigG, resp. SigV nicht gegeben. Es wird offenbar davon ausgegangen, dass der sofortige Eintrag in die Sperrliste genügt. Eine vergleichbare Bestimmung existiert nicht. In der Praxis erfüllt die EAN-PKI diese Anforderung (vgl. Basis-Konzept 4.2.14 Emails)</p>

12		Vergleichbarkeit	Erfüllung
	1	<p>SigV § 4 „Führung eines Zertifikatsverzeichnisses“ verpflichtet die Anbieterin von Zertifizierungsdiensten einen Verzeichnisdienst zu führen. Somit ist die Vergleichbarkeit gegeben.</p>	<p>Gemäss Basis-Konzept werden alle Zertifikate in ein Webverzeichnis eingetragen. Sie können über ein Web-basiertes Interface abgefragt werden. In den Ausführungs-Bestimmungen zur ZertDV werden detaillierte Anforderungen an den Verzeichnisdienst gemacht, wie etwa ein LDAP-Zugang zum Verzeichnis. Die Implementation dieses Protokolls ist nicht vorgesehen. Die Bedürfnisse der ESTV können jedoch durch den vorgesehenen Web-basierten Zugang zum Verzeichnis abgedeckt werden.</p> <p>Kommentar: Das Verzeichnis dient der ESTV zum Suchen von Zertifikaten. Die EIDI-V-Anwendungen benötigen keinen Zugriff auf das Verzeichnis. Die Partner sind im Voraus bekannt und ihre Anzahl beschränkt. Moderne Anwendungen (z.B. EDIFACT) können das verwendete Signaturzertifikat analog zu S/MIME in der Nachricht mitsenden.</p>
	2	<p>SigG § 8 „Sperrung von qualifizierten Zertifikaten“ sieht die Sperrung von Zertifikaten vor. Mit welcher Technologie die Sperrliste implementiert wird, wird in SigV nicht spezifiziert. Der Gesetzgeber wollte selbst in SigV nicht technologiespezifisch sein. Mit dem Satz in SigG § 8 „...Die Sperrung muss den Zeitpunkt enthalten, von dem an sie gilt.“ ist die Hauptanforderung von ZertDV bezüglich Sperrliste erfüllt. Die Vergleichbarkeit ist somit gegeben.</p>	
	3	<p>SigG § 5 „Vergabe von qualifizierten Zertifikaten“ (1) verlangt „...dieses [das Zertifikat] jederzeit für jeden über öffentlich erreichbare Kommunikationsverbindungen nachprüfbar und abrufbar zu halten“. „abrufbar“ bedeutet, Einsichtmöglichkeit in das Zertifikat, falls es im Verzeichnis steht, „nachprüfbar“ bedeutet, dass seine Gültigkeit überprüfbar sein muss, d.h. die Sperrliste verfügbar sein muss. Die Vergleichbarkeit ist gegeben, obwohl der Wortlaut von SigG und SigV nicht direkt vergleichbar ist.</p>	
	4	<p>SigG, respektive SigV enthält bezüglich Verzeichnisdienste keinen Hinweis auf Ausführungsbestimmungen im Sinne von OSCERT SR 784.103.1 . Die Vergleichbarkeit ist somit nicht gegeben. Da die deutsche Gesetzgebung nicht technologiespezifisch sein will, genügt die Forderung, dass ein Verzeichnisdienst existieren muss. Meiner Ansicht nach ist die Vergleichbarkeit mittelbar gegeben.</p>	

13		Vergleichbarkeit	Erfüllung
	1	<p>SigG § 10 und SigV §4 regeln die Aufbewahrungsdauer: 30 Jahre nach Ablauf der Gültigkeit.</p> <p>SigG § 10 „Dokumentation“ (1): <i>„Der Zertifizierungsdiensteanbieter hat die Sicherheitsmaßnahmen zur Einhaltung dieses Gesetzes [...] sowie die ausgestellten qualifizierten Zertifikate nach Maßgabe des Satzes 2 so zu dokumentieren, dass die Daten und ihre Unverfälschtheit jederzeit nachprüfbar sind. Die Dokumentation muss unverzüglich so erfolgen, dass sie nachträglich nicht unbemerkt verändert werden kann. Dies gilt insbesondere für die Ausstellung und Sperrung von qualifizierten Zertifikaten.“</i></p> <p>SigV §4 „Führung eines Zertifikatsverzeichnisses“ (2): <i>„Ein akkreditierter Zertifizierungsdiensteanbieter hat die von ihm ausgestellten qualifizierten Zertifikate, [...] ab dem Zeitpunkt ihrer Ausstellung für den im jeweiligen Zertifikat angegebenen Gültigkeitszeitraum sowie mindestens 30 weitere Jahre ab dem Schluss des Jahres, in dem die Gültigkeit des Zertifikates endet, in einem Verzeichnis [...] zu führen.“</i></p> <p>Somit ist die Vergleichbarkeit gegeben.</p>	<p>Das Basiskonzept hält in 4.2.17 „Archivierung“ fest: <i>„4.2.17.1 CRLs Alle revozierten Zertifikate müssen mindestens 6 Jahre nach Ablauf ihrer Gültigkeit in der aktuellen CRL verbleiben. In archivierten CRLs müssen revozierte Zertifikate mindestens 11 Jahre nach Ablauf ihrer Gültigkeit (manuell) bereitgestellt werden können.“</i></p> <p>4.2.17.2 Zertifikate <i>Alle Zertifikate müssen für einen Zeitraum von mindestens elf Jahren nach Ablauf ihrer Gültigkeit aufbewahrt werden. Die Bereitstellung der Zertifikate muss für einen Zeitraum von mindestens sechs Jahren nach Ablauf der Zertifikatsgültigkeit online über die Web-Seite von TC TrustCenter und ohne zusätzliche Kosten für den Anfrager erfolgen. Nach Ablauf dieses 6-Jahre Zeitraumes müssen die Zertifikate mindestens manuell (gegen Bezahlung) bis 11 Jahre nach Ablauf ihrer Gültigkeit bereitgestellt werden können.“</i></p> <p>Somit sind die Anforderungen exakt erfüllt.</p>
	2	<p>SigV §4 „Führung eines Zertifikatsverzeichnisses“ (1) verlangt: <i>„Der Zertifizierungsdiensteanbieter hat die von ihm ausgestellten qualifizierten Zertifikate, vorbehaltlich eines späteren Zeitpunktes nach § 5 Abs. 2 Satz 2, ab dem Zeitpunkt ihrer Ausstellung für den im jeweiligen Zertifikat angegebenen Gültigkeitszeitraum sowie mindestens fünf weitere Jahre ab dem Schluss des Jahres, in dem die Gültigkeit des Zertifikates endet, in einem Verzeichnis gemäß den Vorgaben nach § 5 Abs. 1 Satz 2 des Signaturgesetzes zu führen.“</i></p> <p>Die Unentgeltlichkeit wird hier nicht erwähnt.</p> <p>Die Vergleichbarkeit ist bedingt gegeben.</p>	<p>Siehe oben 13.1 .</p> <p>Die Anforderung ist somit exakt erfüllt.</p>

14		
	1	<p>SigG § 10 „Dokumentation“ (1): <i>„Der Zertifizierungsdiensteanbieter hat die Sicherheitsmaßnahmen zur Einhaltung dieses Gesetzes und der Rechtsverordnung nach § 24 Nr. 1, 3 und 4 sowie die ausgestellten qualifizierten Zertifikate nach Maßgabe des Satzes 2 so zu dokumentieren, dass die Daten und ihre Unverfälschtheit jederzeit nachprüfbar sind. Die Dokumentation muss unverzüglich so erfolgen, dass sie nachträglich nicht unbemerkt verändert werden kann. Dies gilt insbesondere für die Ausstellung und Sperrung von qualifizierten Zertifikaten.“</i> Damit ist auch das Tätigkeitsjournal angesprochen. Die Vergleichbarkeit ist somit gegeben.</p>
	2	<p>In SigG und SigV ist das Tätigkeitsjournal nicht explizit angesprochen. Die verlangte Aufbewahrungsdauer der Zertifikate erfüllt aber die verlangte Frist, um sich konform zu ZertDV 14 Abs. 2 zu verhalten. Die damit beabsichtigte Zertifikatserneuerung ohne persönliches Erscheinen ist aber nach den TC-TrustCenter Richtlinien nicht möglich. Die Vergleichbarkeit ist somit nicht gegeben, aber auch nicht notwendig.</p>
15		
	1	<p>SigG § 13 regelt die Einstellung der Tätigkeit (1): <i>„Der Zertifizierungsdiensteanbieter hat die Einstellung seiner Tätigkeit unverzüglich der zuständigen Behörde anzuzeigen. ...“</i> Die Vergleichbarkeit ist gegeben.</p>
	2	<p>SigG § 13 (2) lautet <i>„Der Zertifizierungsdiensteanbieter hat die Dokumentation nach § 10 an den Zertifizierungsdiensteanbieter, welcher die Zertifikate nach Absatz 1 übernimmt, zu übergeben. Übernimmt kein anderer Zertifizierungsdiensteanbieter die Dokumentation, so hat die zuständige Behörde diese zu übernehmen. Die zuständige Behörde erteilt bei Vorliegen eines berechtigten Interesses Auskunft zur Dokumentation nach Satz 2, soweit dies technisch ohne unverhältnismäßig großen Aufwand möglich ist.“</i> Unterschied zur ZertDV: (a) Gemäss SigG hat die Anbieterin selbst eine Nachfolgeorganisation zu beauftragen; gemäss ZertDV beauftragt SAS einen anderen Anbieter. (b) Gemäss SigG muss nicht revoziert werden bei einer Übernahme; gemäss ZertDV muss revoziert werden. Die Vergleichbarkeit ist somit gegeben.</p>
	3	<p>SigG macht den Unterschied zwischen freiwilliger Aufgabe und Konkursfall nicht. Damit gilt die obige Aussage zu ZertDV 15 Abs. 2 auch hier. Die Vergleichbarkeit ist somit gegeben.</p>
16		
	1	<p>SigG § 14 „Datenschutz“ (1) lautet: <i>„Der Zertifizierungsdiensteanbieter darf personenbezogene Daten nur unmittelbar beim Betroffenen selbst und nur insoweit erheben, als dies für Zwecke eines qualifizierten Zertifikates erforderlich ist. Eine Datenerhebung bei Dritten ist nur mit Einwilligung des Betroffenen zulässig. Für andere als die in Satz 1 genannten Zwecke dürfen die Daten nur verwendet werden, wenn dieses Gesetz es erlaubt oder der Betroffene eingewilligt hat.“</i> Die Vergleichbarkeit ist gegeben.</p>
	2	<p>Im SigG § 14 ist keine entsprechende Klausel vorhanden. Nach meiner Meinung ist sie aber implizit vorhanden.</p>

17		
	1	<p>SigG § 19 „Aufsichtsmassnahmen“ Abschnitt (2) lautet: <i>„Die Aufsicht über die Einhaltung dieses Gesetzes und der Rechtsverordnung nach § 24 obliegt der zuständigen Behörde; diese kann sich bei der Durchführung der Aufsicht privater Stellen bedienen. Mit der Aufnahme des Betriebes unterliegt ein Zertifizierungsdiensteanbieter der Aufsicht der zuständigen Behörde.“</i></p> <p>Unterschied: Gemäss SigG können private Stellen zugezogen werden; gemäss ZertDV sind die privaten Stellen (Anerkennungsstellen) zuständig. Die Vergleichbarkeit ist somit gegeben.</p>
	2	<p>SigG § 19 „Aufsichtsmaßnahmen“ (3) regelt im Detail unter welchen Umständen ein Entzug der Anerkennung erfolgt: <i>„... wenn Tatsachen die Annahme rechtfertigen, dass er</i></p> <ol style="list-style-type: none"> <i>1. nicht die für den Betrieb eines Zertifizierungsdienstes erforderliche Zuverlässigkeit besitzt,</i> <i>2. nicht nachweist, dass die für den Betrieb erforderliche Fachkunde vorliegt,</i> <i>3. nicht über die erforderliche Deckungsvorsorge verfügt,</i> <i>4. ungeeignete Produkte für qualifizierte elektronische Signaturen verwendet oder</i> <i>5. die weiteren Voraussetzungen für den Betrieb eines Zertifizierungsdienstes nach diesem Gesetz und der Rechtsverordnung nach § 24 nicht erfüllt und Maßnahmen nach Absatz 2 keinen Erfolg versprechen.“</i> <p>Die Vergleichbarkeit ist gegeben.</p>
19		
	1	<p>Im SigG besteht keine analoge Regelung. Vermutlich ist diese Möglichkeit in Deutschland auch gegeben. Sie wird aber nicht erwähnt. Somit besteht keine Vergleichbarkeit, was meiner Ansicht nach vernachlässigt werden kann.</p>
20		<p>Ausführungsbestimmungen analog zu OSCERT SR 784.103.1 existieren gemäss SigG nicht. In SigV § 15 „Anforderungen an Produkte für qualifizierte elektronische Signaturen“ (6) wird aber auf die EU-Signatur-Richtlinien hingewiesen: <i>„Soweit im Rahmen des Verfahrens nach Artikel 3 Abs. 5 und Artikel 9 der Richtlinie 1999/93/EG in der jeweils geltenden Fassung Referenznummern für allgemein anerkannte Normen für Produkte für qualifizierte elektronische Signaturen festgelegt und im Amtsblatt der Europäischen Gemeinschaften veröffentlicht werden, haben diese abweichend von den Absätzen 1 bis 5 Geltung, mit Ausnahme der Produkte nach § 15 Abs. 7 des Signaturgesetzes. ...“</i> Umzusetzen sind die Anhänge II und III der EU-Signatur-Richtlinie. Die daraus resultierenden aktuellen Anforderungen werden im Bundesanzeiger veröffentlicht. Die Vergleichbarkeit ist gegeben.</p>

Zürich, 29. August 2002

Dr. Otto Müller

Quellenverzeichnis

- Deutsches Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz - SigG) vom 16. Mai 2001 (BGBl I S. 876)
- Deutsche Verordnung zur elektronischen Signatur (Signaturverordnung - SigV) vom 16. November 2001
- Schweizerische Verordnung über Dienste der elektronischen Zertifizierung (Zertifizierungsdiensteverordnung, ZertDV) 784.103 vom 12. April 2000
- SR 784.103.1 Technische und administrative Vorschriften über Dienste der elektronischen Zertifizierung (OSCERT)
- Schweizerische Verordnung des EFD über elektronisch übermittelte Daten und Informationen (EIDI-V) vom 30. Januar 2002
<http://www.admin.ch/ch/d/as/2002/259.pdf>
- *ESTV*:
Art. 12 Abs. 2 EIDI-V Erläuterungen vom 22.07.2002
- Richtlinie des Europäischen Parlaments und des Rates über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen vom 18. November 1999
ftp://ftp.pca.dfn.de/pub/pca/docs/SigG/Europe/EISig_Rat-konsolidierteFassung_991118.doc
- *TC TrustCenter AG*:
Basis-Konzept – Konzept der EAN-PKI Version 5.2
- *TC TrustCenter AG*:
Anforderungsanalyse einer TC Class 3 PKI für EAN Schweiz Version 10.2
- *TC TrustCenter AG*:
Certification Practice Statement (CPS) Version 1.2 of May 23rd, 2002
- *TC TrustCenter AG*:
Zertifizierungsrichtlinien Fassung vom 12. Juni 2002 (CPD)
http://www.trustcenter.de/legal/policy/policy_de/tc-trustcenter_zertrichtlinien_juni2002_de.pdf
- *TC Trustcenter AG*
Allgemeine Geschäftsbedingungen für digitale Zertifikate (AGB) vom 12. Juni 2002
http://www.trustcenter.de/legal/generalterms/de/tc-trustcenter_agb_juni2002_de.pdf
- *Deutsche Regulierungsbehörde für Telekommunikation und Post*:
TUVIT.09403.SE.12.2001 - RegTP-Akkreditierungsurkunde vom 4.12.2001
- *T-Systems. 02078.TE.12.2001*:
Bestätigung von Produkten von qualifizierten elektronischen Signaturen:
Signaturerstellungseinheit „Prozessorchipkarte mit Prozessor P8WE5032V0G und STARCOS SPK 2.3 v 7.0 with Digital Signature Application StarCert v 2.2“
http://www.t-systems-zert.de/pdf/ein_02_sig_pro/zf_02078_d.pdf
- *NIST*:
FIPS 140-1 Validation Certificates 221-224 für nCipher nShield F2/F3 und F2/F3 Ultrasign
<http://cs-www.ncsl.nist.gov/cryptval/140-1/140crt/140crt221.pdf> - [140crt224.pdf](http://cs-www.ncsl.nist.gov/cryptval/140-1/140crt/140crt224.pdf)