SICTA
Swiss Information
and Communications
Technology Association

BAKOM
Bundesamt für Kommunikation
Telecomdienste
Herr Peter Fischer, Stellvertretender Direktor
Zukunftsstrasse 44
3201 Biel

Bern, 16. Juli 2004

Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur
Technische und Administrative Vorschriften:
Konsultation

Sehr geehrter Herr Fischer

Wir danken Ihnen für die Einladung zur Stellungnahme zur Konsultation über die Dokumente zur Umsetzung des Bundesgesetzes über Zertifizierungsdienste im Bereich der elektronischen Signatur, ZertES.

Viele der in SICTA eingebundenen Schweizer Unternehmen der Telekommunikationsbranche werden mit den Auswirkungen der Umsetzung unmittelbar betroffen sein, sind sich möglicherweise der Tragweite aber noch nicht bewusst.

Wegen der internationalen Verflechtung sind schweizerische Sonderlösungen nicht angebracht. Durch Referenzierung der relevanten Dokumente und Ausrichtung der TAV wird diesem Umstand Rechnung getragen.

Bemerkungen zu den referenzierten ETSI-Dokumenten

Es ist eigentlich erstaunlich, dass einerseits das EU / EFTA-Mandat M279 ‚Electronic Signature' mit ETSI-Dokument ES 201 733 dokumentiert ist, anderseits kein einziges ETSI-Dokument die verbindlichere Form einer EN aufweist. Zumindest ES 201 733 wurde jedoch den ETSI-Mitgliedern zur Abstimmung vorgelegt. Das mittlerweile mehr als 4-jährige Dokument ist heute unter TS 101 733 (V.1.5.1) bereits viermal revidiert worden. Als Referenz ist dieses in den Erläuterungen zur TAV aufgeführt, nicht aber in der TAV selber.

Grundsätzlich ist die Anlehnung an die ETSI-Standards sehr zu begrüssen, stärkt sie doch auch den Stellenwert dieses europäischen Normeninstitutes. Dass IETF, ITU-T etc. Grundlagen bereitgestellt haben schmälert den Wert der ETSI-Dokumente nicht.

SICTA
Laupenstrasse 18a
Postfach 7923
CH-3001 Bern
URL www.sicta.ch
E-mail office@sicta.ch
Tel +41 31 380 11 80
Fax +41 31 380 11 81

Verbindlichkeit der ETSI TS

Die Form der TS (Technical Specification) bedeutet beim ETSI, dass die Technical Committees, welche die verschiedenen ETSI TS ausgearbeitet haben, diese ohne weitere Konsultation veröffentlichen konnten (keine Länder- oder Mitglieder-Vernehmlassungen / -Abstimmungen erforderlich). Dies bedeutet einerseits einen Zeitgewinn (Time to Market), anderseits geht grundsätzlich die Verbindlichkeit verloren. Sämtliche ETSI-Dokumente weisen also weder einen Status als ‚Harmonized Standard' auf, noch ist die Ausarbeitung als ‚Mandated Work EU / EFTA' zu identifizieren.

Es ist aber auch denkbar, dass bewusst nicht die Form der harmonisierten EN gewählt wurde, weil einzelne Länder bereits Zertifizierungssysteme nach anderen Standards eingeführt hatten.

Version und zukünftige Updates

Einerseits ist es korrekt, in der TAV neben der Nummer auch die Version der referenzierten Dokumente aufzuführen. Das kann aber auch zu einem beträchtlichen Aufwand zur à jour Haltung der TAV führen, weil aufgrund der verschiedenen Versionen der letzten Jahre und der weiteren Entwicklungen kaum davon auszugehen ist, dass diese Dokumente über einen längeren Zeithorizont stabil bleiben werden.

Vollständigkeit referenzierter Dokumente

Die Aufzählung relevanter Dokumente in den Erläuterungen unter 2.1.3.3, Veröffentlichungen der EESSI, ist möglicherweise nicht vollständig. Zudem sind unter EESSI Dokumente aufgeführt, welche in der TAV nicht referenziert sind, aber wohl trotzdem zum Umfang gehören.

Dok #	*Titel*	*Ausgabe*	*Bemerkung*
ETSI TS 102 231	Electronic Signatures and Infrastructures (ESI); Provision of harmonized Trust Service Provider;status information	2003-10-06	
ETSI TS 102 023	Electronic Signatures and Infrastructures (ESI); Policy requirements for time stamping authorities	2003-01-14	In TAV referenziert, fehlt unter EESSI
ETSI TS 102 158	Electronic Signatures and Infrastructures (ESI); Policy requirements for Certification Services; Providers issuing attribute certificates usable with Quaified certificates	2003-10-09	
ETSI TS 101 733	Electronic Signature Formats	2000-05-09	Fehlt in TAV - weil dort nicht weiter referenziert?
ETSI TS 101 903	XML Advanced Electronic Signatures (XAdES)	2004-04-02	Fehlt in TAV - weil dort nicht weiter referenziert?
ETSI TS 101 861	Time Stamping Profile	2002-03-	Fehlt in TAV - weil dort nicht weiter referenziert?

Korrekte Bezeichnung der ETSI TS

In der TAV fehlt an verschiedenen Stellen die Bezeichnung ‚TS':
- unter 1.2 Referenzen (Seite 4): ETSI **TS** 102 023
- unter 3.4.3 Format der Zertifikate (Seite 12): ETSI **TS** 101 862
- unter 3.5 Zeitstempel (Seite 14): ETSI **TS** 102 023

SICTA
Laupenstrasse 18a
Postfach 7923
CH-3001 Bern

URL www.sicta.ch
E-mail office@sicta.ch
Tel +41 31 380 11 80
Fax +41 31 380 11 81

Bemerkungen zu einzelnen Punkten ‚VZertES'

Artikel 5: Ausstellung qualifizierter Zertifikate

Absatz 2

Aus der Formulierung lässt sich schliessen, dass ein neues Zertifikat sich auf den gleichen Signaturprüfschlüssel bezieht, der bis anhin verwendet wurde. Es ist jedoch gängige Praxis, dass bei einer Erneuerung des Zertifikats - nach Ablauf seiner Gültigkeitsdauer - auch das Schlüsselpaar erneuert wird. Dies insbesondere, da die Gültigkeitsdauer per Definition diejenige Zeitperiode bezeichnet, während der mit Gewissheit angenommen werden kann, dass aus dem Signaturprüfschlüssel - und allenfalls aus den hergestellten Signaturen - der Signaturschlüssel nicht abgeleitet werden kann. Dies bedeutet, dass nach Ablauf der Gültigkeitsdauer diese Sicherheit nicht mehr besteht. Somit ist es in Hinblick auf das Rechtssicherheitsbedürfnis nicht sinnvoll, nach Ablauf der Gültigkeitsdauer ein neues Zertifikat für das gleiche Schlüsselpaar zu erstellen. Aus diesen Gründen schlagen wir folgende Formulierung vor:

„Beantragt eine vor weniger als sechs Jahren gemäss Absatz 1 identifizierte Person ein neues elektronisches Zertifikat, können die anerkannten Anbieterinnen von Zertifizierungsdiensten einen Antrag entgegennehmen, der mit einer elektronischen Signatur versehen ist, die anhand des noch gültigen Signaturschlüssels erzeugt wurde. Der Antrag hat vor Ablauf der Gültigkeitsdauer des Zertifikats zu erfolgen."

Artikel 7: Ungültigerklärung qualifizierter Zertifikate

Absatz 1 Verzeichnis für ungültig erklärte qualifizierte Zertifikate

Es fehlen Vorschriften im Zusammenhang mit der Führung von Verzeichnissen für ungültig erklärte Zertifikate. Hierzu gehören u.A. auch Bestimmungen, innerhalb welcher Zeit (z.B. 12 Stunden) eine anerkannte Anbieterin die Verzeichnisse nachzuführen hat. Wünschenswert wäre demnach eine Verpflichtung aufzunehmen, wonach die anerkannten Anbieterinnen die gemäss Absatz 2 aufgelisteten Anforderungen zweimal täglich in solchen Verzeichnissen nachzuführen hätten.

Artikel 10 Einstellung der Tätigkeit

Art. 13 ZertES führt wohl dazu, dass ein CSP über eine auch im Konkursfall privilegierte (Bank-) Garantie verfügt, welche die kostendeckende Übernahme und Weiterführung der ausgestellten Zertifikate bis zum Ende der Gültigkeit dieser Zertifikate deckt. Das kann bei Schweizer Anbieterinnen wohl verlangt werden, jedoch kaum bei internationalen CSPs.
Ausländischen CSP können diese Aufgaben kaum überbunden werden, es sei denn, sie suchen in der Schweiz um Anerkennung als Anbieter nach. Geht nur der Schweizer Ableger in Konkurs, so wäre wohl die Weiterführung der Dienste sichergestellt, jedoch nicht im Falle des Konkurses des internationalen Anbieters.
Das würde wohl bedeuten, dass die SAS ein System aufbauen müsste, welches die Übernahme der Daten im Falle eines Konkurses für alle akkreditierten Systeme sicherstellen könnte. Aus dieser Sicht müssten die Anforderungen an in der Schweiz akkreditierte CSP näher spezifiziert werden.
Die wohl auf lange Sicht uneinheitliche Ausgestaltung von elektronischen Signaturen - die zwar den grundsätzlichen Anforderungen entsprechen - dürften die Übertragung der Aufgabe im Falle der Aufgabe der Tätigkeit eines anerkannten CSP stark beeinträchtigen.

Artikel 11 Signaturschlüssel

Die Inhaberin oder der Inhaber des Signaturschlüssels, welcher in einer Smart Card oder Token gespeichert werden muss, darf diesen keiner anderen Person anvertrauen. Zudem soll der Signaturschlüssel, soweit zumutbar, auf sich getragen oder weggeschlossen werden.

SICTA
Laupenstrasse 18a
Postfach 7923
CH-3001 Bern
URL www.sicta.ch
E-mail office@sicta.ch
Tel +41 31 380 11 80
Fax +41 31 380 11 81

Diese restriktive Handhabung verhindert de facto die verschlüsselte Speicherung des Signaturschlüssels auf einem Server im Internet sowie das dynamische Herunterladen, Entschlüsseln und Einsatz des Signaturschlüssels auf diversen Endgeräten. Der Vorteil einer solchen Vorgehensweise ist offensichtlich und liegt in der geographischen Mobilität sowie in der Flexibilität bezüglich des Einsatzes verschiedener Endgeräte. Zudem bestehen heute bereits ausreichende technische Möglichkeiten, um eine entsprechende Verschlüsselung sicherzustellen. Wir schlagen deshalb vor, die Ausführungsbestimmungen dahingehend mit neuen Sicherheitsanforderungen anzupassen, dass eine solche Verwendung des Signaturschlüssels durch den Inhaber oder die Inhaberin ohne Übernahme von zusätzlichen Haftungsrisiken erfolgen kann.

Artikel 12 Passwort

Die Verwendung von Passwörtern zum Wegschliessen von Passwörtern ist zu begrüssen. Wohl wissend, dass eine Kontrolle kaum zu bewerkstelligen ist, sollte trotzdem eine schärfere Form als ‚vier Zahlen oder Buchstaben' gewählt werden.

Dies könnte zum Beispiel mit der Formulierung wirkungsvoller so definiert werden:
‚Passwörter, die Zugang zum Signaturschlüssel verschaffen, müssen eine Länge von mindestens acht Zeichen aufweisen. Sie müssen zusammengesetzt sein aus Zahlen, Gross- und Kleinbuchstaben und Sonderzeichen, unter Ausschluss von persönlichen Daten oder Wörtern aus Wörterbüchern.

Artikel 13 Meldung bei Verlust

Absatz 1

Der Satz aus Absatz 3 könnte der Einfachheit halber problemlos am Ende des Absatz 1 eingefügt werden.

Registrierungsstellen

Registrierungsstellen sind im ZertES Art. 8 Abs. 4 erwähnt, finden jedoch keinen Niederschlag in der VZertES. Dies ist eigentlich nicht zu beanstanden, sofern keine spezielle Anforderungen gestellt werden sollen. Durch Überbindung der Haftung an die Registrierungsstelle werden den Registrierungsstellen enge Grenzen gesetzt. Sie werden zwangsläufig durch die verantwortlichen Anbieterinnen von CSP kontrolliert.

Wenn sich der Markt entwickeln soll, so sollten hier keine weiteren Präzisierungen erfolgen. Damit könnten wohl nicht nur Handelskammern, Notare etc. diese Aufgaben erfüllen können, sondern auch z.B. Banken, Post Einwohnerkontrollen (e-Government!) etc.

Bemerkungen zu den ‚Technische und administrative Vorschriften'

Aktuelle Zertifizierungspraxis

Die Anforderungen basieren auf Europäischen Standards, speziell den ETSI-Standards, oder auf RFCs der IETF. Dieser Ansatz ist prinzipiell zu begrüssen, da ein Schweizer Certification Service Provider (CSP) eine Kompatibilität auf der europäischen Ebene anstreben sollte.

SICTA
Laupenstrasse 18a
Postfach 7923
CH-3001 Bern
URL www.sicta.ch
E-mail office@sicta.ch
Tel +41 31 380 11 80
Fax +41 31 380 11 81

‚Europa der unterschiedlichen Geschwindigkeiten' führt wohl dazu, dass in einzelnen Ländern unterschiedliche Standards angewendet werden. Hier spielt wohl der Umstand eine grosse Rolle, dass die relevanten ETSI-Standards auf der Basis der EU-Richtlinie 1999/93/EG erst innerhalb des letzten Jahres bereitgestellt wurden - nach mehreren Überarbeitungen.
Ob eine langfristige Harmonisierung nationaler Zertifizierungssysteme überhaupt erreichbar sein wird bleibt wohl offen. Ebenso offen bleint zur Zeit die Frage, welche Standards sich letztlich durchsetzen werden - hier entscheidet wohl der Markt.

Generierung der Zertifikate

Es ist zu begrüssen, dass der CPS das Schlüsselpaar für qualifizierte Zertifikate im Auftrag des Antragstellers selber in einer sicheren Umgebung generieren kann und danach das Schlüsselpaar auf eine Secure-creation device (SSCD) speichern kann. Dieses Vorgehen kann betriebliche Vorteile bieten. Es ermöglicht dem CPS die Mengen-Produktion von Zertifikaten. Im Weiteren ist ein Verfahren zur Erstellen der Zertifikate möglich, das keine Interaktion mit dem Endbenutzer erfordert. Zudem wird sichergestellt, dass die Zertifikate bzw. Schlüssel bei einer zentralisierten Lösung immer unter Einhaltung von einem hohen Sicherheitsstandard abgespeichert werden, was bei lokalen Lösungen wie Chipkarten nicht immer der Fall ist.

Ziffer 3.2.1 b) Organisation

Es wäre begrüssenswert festzuhalten, dass die Ergebnisse der internen Audits dem Tätigkeitsjournal beizufügen und entsprechend aufzubewahren sind.

Ziffer 3.2.2 Verwaltung der Politik

Im zweiten Absatz ist „Aussage der Zertifizierungspraxis (CPS)" durch „Aussage über die Zertifizierungspraxis (CPS)" zu ersetzen.

Ziffer 3.4.3.1 Felder des Zertifikats

Feld: "keyUsage": Hier wäre es sinnvoll nicht nur Bit Nr. 1 zu setzen, sondern alle anderen auf Null zu setzen, mit Ausnahme derer die nötig sind damit mit dem Zertifikat auch ein Login bzw. eine Authentifikation durchgeführt werden kann (z.B. SSL Client Authentifikation oder Windows Logon). Ein qualifiziertes Zertifikat sollte auch für Logins benützt werden können.

Feld: "QCStatements / Präzisierung des Zertifikats": Der Wert wird nicht in Form des OID angegeben sondern ergibt sich aus dem INTEGER und dem EXPONENT gemäss RFC. Deshalb sollte „…. Kapitel 3.2.6, in Form eines Objektbezeichners…." durch „……Kapitel 3.2.6, unter Verwendung eines Objektbezeichners….." ersetzt werden.

3. Generelle Bemerkungen.

Wir messen der internationalen Verwendung elektronischer Signaturen und deren rechtliche Anerkennung hohen Stellenwert bei, da dies der Entwicklung eines intensiveren elektronischen Handels über die Grenzen hinweg förderlich ist. Daher wäre es begrüssenswert, wenn der Bundesrat die internationale Verwendung und Anerkennung elektronischer Signaturen gemäss Art. 19 ZertES baldmöglichst anstrebt. Zudem erachten wir es als sinnvoll und richtig, sich stark an die europäischen Vorschriften anzulehnen.

SICTA
Laupenstrasse 18a
Postfach 7923
CH-3001 Bern
URL www.sicta.ch
E-mail office@sicta.ch
Tel +41 31 380 11 80
Fax +41 31 380 11 81

Freundliche Grüsse

SICTA

sig.	sig.
Gilbert Bieri	Josef Erni
Geschäftsleiter	Technik und Ausbildung

SICTA ist der Anbieterverband der Telekommunikationsbranche und vereinigt wichtige Firmen und Organisationen unter ihrem Dach. SICTA vertritt die spezifischen Interessen der Branche im nationalen und internationalen Umfeld und unterstützt damit die Wettbewerbsfähigkeit der im Telekommunikations-Bereich angesiedelten Unternehmen sowie des Wirtschaftsstandortes Schweiz.

URL www.sicta.ch
E-mail office@sicta.ch
Tel +41 31 380 11 80
Fax +41 31 380 11 81
SICTA
Laupenstrasse 18a
Postfach 7923
CH-3001 Bern