Dr. Otto Müller Consulting
Alte Landstrasse 19
8803 Rüschlikon

7. August 2006

Bundesamt für Kommunikation
BAKOM
Zukunftstrasse 44
CH-2501 Biel

Betrifft: Stellungnahme zu Änderungsentwurf der „technischen und administrativen Vorschriften über Zertifizierungsdienste im Bereich der elektronischen Signatur“ (SR 943.032.1) Version 3

Sehr geehrte Damen und Herren,

Entsprechend Ihrem Brief vom 23. Juni 2006 bezüglich des Änderungsentwurfes der „Technischen und administrativen Vorschriften“ zu ZertES nehmen wir dazu wie folgt Stellung:

Allgemeine Bemerkungen:
Wir begrüssen die Absicht, die „Technischen und administrativen Vorschriften“ (TAV) zu ZertES in der Version 3 sowohl den neuesten internationalen Spezifikationen als auch Anforderungen der Praxis anzupassen. Durch dieses Vorgehen werden die Rahmenbedingungen für die Anbieterinnen von Zertifizierungsdiensten verbessert, und den Endbenutzern wird der Umgang mit Zertifikaten erleichtert. Somit werden auch die Verbreitung und Akzeptanz von Zertifikaten anerkannter Anbieterinnen gefördert. Dies gilt nicht nur für qualifizierte Zertifikate, sondern auch für alle anderen von diesen Anbieterinnen ausgestellten Zertifikate.
Gerne nutzen wir die gebotene Möglichkeit zur Stellungnahme.

Detaillierte Bemerkungen:
Um die oben genannten Ziele zu erreichen, bringen wir die folgenden Bemerkungen und Änderungsvorschläge an. Den einzelnen Punkten haben wir eine Priorität beigemessen und sie dementsprechend geordnet. (Punkt 1 hat die höchste Priorität.)

1. **Kapitel 3.4.2 „Format der Zertifikate für Inhaberinnen und Inhaber“ Buchstabe c, sowie Kapitel 3.4.3 „Verwaltung des Zertifikats der CSP“ Buchstabe c: Bezeichnung der Erweiterung „qcStatements“**

   Wir begrüssen ausdrücklich die Berücksichtigung unserer Anregung vom 7. Februar 2005, dass den Anbieterinnen die Entscheidung überlassen wird, ob die Erweiterung „qcStatements“ in Benutzer-Zertifikaten kritisch oder nicht-kritisch gesetzt wird.
   Seit der Version 2 der TAV (wie auch im Entwurf zur Version 3) wird aber auch für das *Zertifikat der* CA *(Certification Authority / Zertifizierungsbehörde)* verlangt, dass darin *„qcStatements“* als *kritische Erweiterung* enthalten sein muss. Durch das Beibehalten dieser Forderung wird weiterhin verhindert, dass in gängigen Applikationen eine fehlerfreie Signatur-Prüfung durchgeführt werden kann.
   Gemäss Standard (RFC 3280) muss eine Applikation die Verarbeitung eines Zertifikates abbrechen, wenn darin eine der Applikation unbekannte kritische Erweiterung enthalten ist. Da die Erweiterung „qcStatements“ nicht in RFC 3280 aufgeführt ist, und qualifizierte Zertifikate vor allem im europäischen Umfeld eine Rolle spielen, wird diese Erweiterung von üblichen US-amerikanischen Produkten bisher nicht unterstützt.
   Weiter beinhaltet die Signatur-Prüfung auch die Validierung des Zertifikats-Pfades (also auch die Verarbeitung aller CA-Zertifikate). Deshalb führt eine kritische Erweiterung „qcStatements“ auch in einem CA-Zertifikat zu Problemen in Applikationen, denen diese Erweiterung unbekannt ist.
   Eine fehlerfreie Signatur-Prüfung ist auch eine der Voraussetzungen für die reibungslose Anzeige von qualifiziert signierten PDF-Dateien des Schweizerischen Handelsamtsblattes (SHAB) in Adobe Reader. Zu diesem Zweck existiert deshalb auch bereits ein CA-Zertifikat einer anerkannten Anbieterin, in dem die Erweiterung „qcStatements“ nicht-kritisch eingestellt ist. Mit dem Beibehalten der Forderung nach einer kritischen Erweiterung „qcStatements“ in der finalen Version 3 der TAV müsste dieses CA-Zertifikat widerrufen werden, was der allgemeinen Akzeptanz qualifizierter Zertifikate abträglich wäre.

   Aus den oben genannten Gründen schlagen wir vor, die Forderung nach einer kritischen Erweiterung „qcStatements“ in CA-Zertifikaten zu streichen.

2. **Kapitel 3.3.3 „Sichere Signaturerstellungseinheiten“ Buchstabe d): Einheit für Signaturerstellung im grossen Massstab**

   Die von der SHAB-Verordnung verlangte qualifizierte Signatur von SHAB-Daten ist in der Praxis nur durch *automatisierte* Signaturen mittels Hardware Security Modules (HSMs) sinnvoll zu bewerkstelligen. Die Zulassung von HSMs ist deshalb folgerichtig, stellt aber aus den folgenden Gründen eine Ausnahmeregelung dar:

   - Die *qualifizierte Signatur* ist der *eigenhändigen Unterschrift* gemäss OR Art. 14 gleichgestellt. Deshalb muss üblicherweise der Zertifikatsinhaber zuerst vom In-

halt des Dokumentes Kenntnis nehmen und selber persönlich elektronisch signieren.
- Dies wird eigentlich auch in Abschnitt 3.3.3 a) der TAV verlangt: „Sie [die sicheren Signaturerstellungseinheiten] dürfen weder [...], noch die signierende Person daran hindern, diesen Inhalt vor dem Signieren genau zur Kenntnis zu nehmen". Abschnitt 3.3.3 d) ist schlecht vereinbar mit dieser Forderung.

Wir schlagen deshalb vor, den Satz

"Wenn eine Signaturerstellungseinheit in einer physisch gesicherten Umgebung betrieben wird, dann gilt sie als sichere Signaturerstellungseinheit, um qualifizierte elektronische Signaturen gemäss ZertES zu erstellen, sofern folgende Anforderungen erfüllt sind:"

im Sinne einer Ausnahmeregelung für automatisierte Signaturerstellung zu formulieren:

"*In Ausnahmefällen* können sichere Signaturerstellungseinheiten für *automatisierte* Signaturerstellung zur Erstellung von qualifizierten elektronischen Signaturen gemäss ZertES verwendet werden, sofern folgende Anforderungen erfüllt sind:

- Die sichere Signaturerstellungseinheit wird in einer physisch sicheren Umgebung betrieben;
- ..."

Weiter ist die Anforderung „Die CSP muss sicherstellen..." praktisch nur erfüllbar, wenn die Signaturerstellung bei der CSP ausgelagert wird. Auch scheint es uns übertrieben, in dieser Frage der CSP die gesamten Pflichten zu übertragen. Es liegt in der Verantwortung des Zertifikatsinhabers, dass der private Schlüssel richtig verwendet wird, die CSP hat nur die Pflicht, diesen auf korrekte Verwendung hinzuweisen. Zudem sollte dem Zertifikatsinhaber die Entscheidung überlassen werden, ob er automatisierte qualifizierte Signaturen selber anbringen will oder nicht.
Zur richtigen Verwendung des Signaturschlüssels ist der Zertifikatsinhaber sowieso gezwungen bzw. motiviert durch die Beweislastumkehr bei qualifizierter Signatur gemäss OR Art. 59a Abs. 1. Es liegt also im Interesse des Zertifikatsinhabers, sich abzusichern gemäss OR Art. 59a Abs. 2: "Die Haftung entfällt, wenn der Inhaber des Signaturschlüssels glaubhaft darlegen kann, dass er die nach den Umständen notwendigen und zumutbaren Sicherheitsvorkehrungen getroffen hat, um den Missbrauch des Signaturschlüssels zu verhindern."
Wichtig in diesem Zusammenhang ist auch VZertES Art. 11 Abs. 1: „Die Inhaberin oder der Inhaber eines qualifizierten Zertifikats darf die Signaturerstellungseinheit keiner anderen Person anvertrauen. [...]". Die Auslagerung der Signaturerstellung ist also an sich ausdrücklich verboten, stellt also auch klar eine Ausnahme dar.

Wir schlagen deshalb vor, die folgende Änderung vorzunehmen:

- „Die CSP muss sicherstellen...“ in sämtlichen Gliederungspunkten von 3.3.3. d) durch „*Die Inhaberin oder der Inhaber des Zertifikats muss sicherstellen...*“ zu ersetzen.
- Den Gliederungspunkt „Die CSP muss sicherstellen, dass die Signaturerstellungseinheit von der Inhaberin oder vom Inhaber des qualifizierten Zertifikats oder von einer bevollmächtigten Person betrieben wird;“ zu streichen und den Satz “*In Ausnahmefällen kann die Inhaberin oder der Inhaber des Zertifikates den Betrieb einer sicheren Signaturerstellungseinheit für automatisierte Signaturerstellung einer bevollmächtigten Person übertragen.*“ anzufügen.

3. Kapitel 3.4.2 „Format der Zertifikate für Inhaberinnen und Inhaber“ Buchst. c: Erweiterung „certificatePolicies“

ETSI TS 101 862 V1.3.2 „Qualified Certificate profile“ empfiehlt in Kapitel 5.3 „Qualified Certificate Indication“ den (auch von ZertES geforderten) Hinweis, dass es sich beim Zertifikat um ein qualifiziertes Zertifikat handelt, nicht nur in der Erweiterung „qcStatements“, sondern auch in der Erweiterung „certificatePolicies“ zu dokumentieren.
Auch wird die Erweiterung „qcStatements“ von den meisten gängigen Applikationen nicht unterstützt (siehe auch Punkt 1). Somit werden die gesetzlich geforderten Hinweise auf Qualifiziertheit des Zertifikates und ebenfalls die Limitierung des Transaktionsbetrages den meisten Benutzern nicht angezeigt. Diese Hinweise sind also eigentlich nicht in einer Form enthalten, die „human-readable“ ist.
Weiter fordern die TAV das Einfügen eines Benutzerhinweises / „User Notice“ (also einer Meldung im Text-Format) in der Erweiterung „certificatePolicies“; sie setzen aber keine konkreten Anforderungen an diesen Text. Dieses Feld würde sich bestens eignen, um diese Hinweise in allgemein lesbarer Form in einem Zertifikat sichtbar zu machen.
Damit würde auch der Zweck des ZertES, nämlich die Gleichstellung der qualifizierten Signatur mit der eigenhändigen Unterschrift gemäss OR Art. 14 , Abs. 2bis zu erreichen, besser erfüllt.

Wir sind deshalb der Meinung, dass die „User Notice“ folgende Hinweise enthalten sollte:

- *Den Hinweis, dass es sich um ein qualifiziertes Zertifikat gemäss schweizerischer Gesetzgebung handelt.*
- *Den Hinweis auf den Wert der Transaktionen, für die das Zertifikat verwendet werden kann.*

Eine genaue Ausformulierung dieser Anforderung sprengt aber den Rahmen dieser Stellungnahme.

4. Kapitel 3.4.3 „Verwaltung des Zertifikats der CSP“ Buchstabe d): Nicht-kritische Erweiterungen

Wir sind der Meinung, dass die Spezifikation für das Zertifikat der CA (Certification Authority / Zertifizierungsbehörde) gemäss RFC 3280 sowie der üblichen Gepflogenheiten definiert werden sollte. Wir schlagen deshalb vor, 3.4.3. d) wie folgt zu ändern:

“Für ihr eigenes Zertifikat muss die CSP sicherstellen, dass entsprechend dem Dokument RFC 3280 [9], Kapitel 4.2, die folgenden nicht-kritischen Erweiterungen der Sequenz tbsCertificate vorhanden sind:
- authorityKeyIdentifier *(für Root-Zertifikate ist diese Erweiterung optional)*;
- *subjectKeyIdentifier;*
- certificatePolicies;
- issuerAltName gemäss Kapitel 3.4.2, Bst. c dieses Dokumentes;
- crlDistributionPoints *(für Root-Zertifikate ist diese Erweiterung optional)*“

Begründung:

- Gemäss RFC 3280 müssen alle CA-Zertifikate die Erweiterung „subjectKeyIdentifier“ enthalten. Diese ist das Gegenstück zur Erweiterung „authorityKeyIdentifier“ in End-Entity- und Sub-CA-Zertifikaten.
  Diese Erweiterung ist auch in den CA-Zertifikaten der bereits anerkannten Anbieterinnen enthalten. Für diese Anbieterinnen entstehen durch diese Forderung also keine Probleme.
- Es ist nicht ausgeschlossen, dass es sich bei einem CA-Zertifikat zur Ausgabe von qualifizierten Zertifikaten um eine Root-CA handelt. Die Erweiterungen „authorityKeyIdentifier“ und „crlDistribution-Points“ sind für Root-Zertifikate optional bzw. unüblich und sollten deshalb nur für Sub-CA-Zertifikate zwingend gefordert werden.

Weiter schlagen wir auch vor, den Titel „Verwaltung des Zertifikats der CSP“ zu ändern in „Verwaltung des Zertifikats der *CA zum Ausstellen qualifizierter Zertifikate*“, da es sich beim beschriebenen Zertifikat nicht um irgendein Zertifikat der CSP (Certification Service Provider / Anbieterin von Zertifizierungsdiensten), sondern *nur* um das Zertifikat der CA (Certification Authority / Zertifizierungsbehörde) zum Ausstellen qualifizierter Zertifikate handelt.

5. Kapitel 3.4.2 „Format der Zertifikate für Inhaberinnen und Inhaber“: Zertifikatseinträge allgemein

Wir schlagen vor, am Ende des Kapitels 3.4.2 „Format der Zertifikate für Inhaberinnen und Inhaber“ die folgenden Sätze anzufügen:

“*Diese Anforderungen stellen Minimal-Anforderungen dar. Zusätzliche Zertifikatseinträge sind erlaubt, sofern diese konform zu den hier referenzierten Spezifikationen sind und deren Inhalt überprüft ist.*“

Begründung:
Die in Kapitel 3.4.2 angeführten Vorschriften sind Minimalanforderungen an den Inhalt eines qualifizierten Zertifikates und verhindern nicht, dass zusätzliche Einträge (Erweiterungen) in das Zertifikate gemacht werden. Dies sollte in aller Deutlichkeit gesagt werden. Allerdings muss sich der Empfänger eines qualifizierten Zertifikates darauf verlassen können, dass der Zertifikatsinhalt korrekt ist.

6. Kapitel 3.4.2 „Format der Zertifikate für Inhaberinnen und Inhaber“ Buchst. c: Erweiterungen des Benutzerzertifikates

Wir schlagen vor, den Text in der ersten Zelle der Tabellenzeile

Objektbezeichner des Schlüssels der CSP, die das Zertifikat signiert hat	Nein	**authorityKeyIdentifier**	Gemäss dem Dokument RFC 3280 [8], Kapitel 4.2.1.1.

zu ändern in:

Identifikator des Schlüssels der CSP, die das Zertifikat signiert hat	Nein	**authorityKeyIdentifier**	Gemäss dem Dokument RFC 3280 [8], Kapitel 4.2.1.1.

Begründung:
Objektbezeichner ist die deutsche Übersetzung des Begriffes „Object Identifier“ (OID). Die angeführte Erweiterung „authorityKeyIdentifier“ enthält normalerweise einen Hash-Wert des öffentlichen Schlüssels der CA; ein „Object Identifier“ ist nicht üblich.

Weiter schlagen wir vor, die folgende Tabellenzeile zu streichen:

Zugangspunkt zum Zertifikat der CSP	Nein	**AuthorityInformation Access**	Gemäss Dokument RFC 3280 [8], Kapitel 4.2.2.1.

Begründung:
Weder ZertES noch die internationalen Standards stellen diese Forderung. Die Entscheidung, ob ein solcher Zugangspunkt in das Zertifikat aufgenommen wird, sollte der CSP überlassen werden.

Abschliessend möchten wir Ihnen für die gebotene Möglichkeit zur Stellungnahme danken. Wir hoffen, mit den oben aufgeführten Punkten zur Akzeptanz von Zertifikaten anerkannter Anbieterinnen beizutragen.

Mit freundlichen Grüssen

Adrian Müller

Otto Müller