Dr. Otto Müller Consulting
Alte Landstrasse 19
8803 Rüschlikon

30. Juni 2004

Bundesamt für Kommunikation
BAKOM
Zukunftstrasse 44
CH-2501 Biel

Betrifft: Stellungnahme zu „Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur (VZertES) und Technische und administrative Vorschriften (TAV)“

Sehr geehrte Damen und Herren,

Entsprechend Ihrem Brief vom 1. Juni 2004 nehmen wir dazu wie folgt Stellung:

1. Wir begrüssen die Absicht, die „Technischen und administrativen Vorschriften“ (TAV) zur Verordnung über Zertifizierungsdienste möglichst auf internationale Normen abzustützen. Damit wird nicht nur die Etablierung einer schweizerischen Zertifizierungsdienst-Anbieterin gefördert sondern auch die Anerkennung ausländischer Zertifizierungsdienst-Anbieterinnen durch eine schweizerische Anerkennungsstelle erleichtert.

2. Das Gesetz für Zertifizierungsdienste im Bereich der elektronischen Signatur (ZertES) wird durch die VZertES und die TAV umgesetzt. Die entsprechenden Dokumente bilden die Grundlage für operationelle Implementierungen durch Zertifizierungsdienstanbieterinnen. Es stellt sich deshalb die Frage, ob die VZertES und die TAV in der vorliegenden Form genügen, um den Willen des Gesetzgebers umzusetzen oder ob sie ergänzt werden müssen. Wir sind zum Schluss gekommen, dass die VZertES und die TAV ergänzt werden müssen. In den nachfolgenden Abschnitten begründen wir diese Auffassung.

3. Die im Gesetz für Zertifizierungsdienste im Bereich der elektronischen Signatur (ZertES) in Art. 7 Abs. 1 Ziff. f vorgesehene Bestimmung, wonach ein qualifiziertes Zertifikat die qualifizierte elektronische Signatur der Anbieterin von Zertifizierungsdiensten enthalten muss, erschwert oder verunmöglicht bei wörtlicher Auslegung des Gesetzestextes sowohl die Etablierung einer schweizerischen Zertifizierungsdienstanbieterin als auch die Anerkennung einer ausländischen Anbieterin.

   Begründung:
   Eine qualifizierte Signatur der Zertifizierungsdienstanbieterin erfordert, dass auch ihre notwendigen Eigenzertifikate[1] qualifiziert sind. In qualifizierten Zertifikaten ist die Nennung einer natürlichen Person als Inhaberin des Signaturschlüssels vorgeschrieben.
   Damit beruht die automatische Erstellung von Endbenutzer-Zertifikaten auf einer

[1] Von der Zertifizierungsdienstanbieterin auf sich selbst ausgestellte Zertifikate

elektronischen Signatur, welche einer handschriftlichen Unterschrift gleichgestellt ist. Die rechtliche Wirkung der Signatur aus einem solchen automatischen Vorgang ist umstritten.
Schwerwiegender jedoch ist die Tatsache, dass bei Ausscheiden der genannten Person aus der Zertifizierungsdienstanbieterin, diese gezwungen ist, neue Eigenzertifikate zu erstellen und diese zu publizieren, damit weiterhin Endbenutzer-Zertifikate ausgestellt werden können.
Aus diesen Gründen sind in den Eigenzertifikate existierender anerkannter Anbieterinnen im Ausland als Inhaber oder Inhaberinnen keine natürlichen Personen zu finden. Die ausländischen Gesetze verlangen beim Einsatz der elektronischen Signatur für Eigenzertifikate der Zertifizierungsdienst-Anbieterinnen lediglich eine fortgeschrittene elektronische Signatur, für welche mindestens die gleichen technischen Anforderungen gelten wie für eine qualifizierte elektronische Signatur. Die zugehörigen Zertifikate können aber auf eine juristische Person lauten. Im Übrigen existiert der Begriff „qualifizierte elektronische Signatur“ in der Direktive über die elektronische Signatur des Europäischen Parlamentes und der Europäischen Kommission nicht explizit.

4. Gemäss Auskunft des BAKOM hat der Gesetzgeber den Begriff „qualifizierte elektronische Signatur“ geschaffen, um die Rechtssicherheit im Bereich der elektronischen Signatur zu erhöhen. Dies betrifft aber nur Endbenutzer-Zertifikate, die zugehörigen Signaturschlüssel und die sicheren Signaturerstellungseinheiten. Die Erstellung von Eigenzertifikaten der Zertifizierungsdienstanbieterinnen muss deshalb unter diesem Gesichtspunkt betrachtet, d.h. besonders behandelt werden.

5. Zur Klarstellung dieser Situation für künftige Anbieterinnen von Zerifizierungsdiensten in der Schweiz schlagen wir deshalb folgende Ergänzung der Verordnung vor:
3. Abschnitt: Qualifizierte Zertifikate
Artikel 4
Abs. 1 wie bisher: Das Bundesamt regelt das Format der qualifizierten Zertifikate
Abs. 2 (neu): Für qualifizierte Zertifikate, welche die Anbieterin von Zertifizierungsdiensten für sich selbst und für den Zeitstempeldienst verwendet, gelten besondere Vorschriften über die Angaben in diesen Zertifikaten.
Die alleinige Nennung einer juristischen Person als Inhaberin ist zulässig.

Diese Ergänzung der Verordnung sowie zusätzliche Überlegungen führen in den Technischen und administrativen Vorschriften zu entsprechenden Ergänzungen in Abschnitt „3.4.3.1 Felder des Zertifikats“. Wir schlagen vor:

- Die Einleitung „Die CSP muss Zertifikate entsprechend den Vorschriften in diesem Kapitel generieren.“ sollte wie folgt ergänzt werden:
  “**Die folgend genannten Eintragungen sind Minimalanforderungen. Zusätzliche Eintragungen sind erlaubt, sofern diese von der CSP überprüft und standard-konform sind.**“

- Die Anforderungen an Endbenutzer-, Zertifizierungsinstanz[2]- und Zeitstempeldienst-Zertifikate werden getrennt behandelt.
    - Für Endbenutzer-Zertifikate schlagen wir vor:
      Belassen gemäss ursprünglichen Anforderungen, mit Ausnahme des Inhaltes des Nutzungsbereiches (keyUsage):
      "Bit Nr. 1 setzen, um anzuzeigen, dass das Zertifikat ausschliesslich zur Überprüfung der Unterschrift verwendet wird."
      Ändern in:
      „**Bit 1 (Non-Repudiation) muss gesetzt werden, um anzuzeigen, dass das Zertifikat zur Überprüfung der qualifizierten elektronischen Signatur (im Sinne des ZertES) verwendet wird.**
      Optional kann auch das Bit 0 (Digital Signature) gesetzt werden.
      Die restlichen Bits (2-8) dürfen nicht gesetzt werden."

      Kommentar: Die bestehende Formulierung scheint uns unpräzise. Mit der neu vorgeschlagenen Formulierung wird folgenden Umständen Rechnung getragen:
      Einerseits wird der Einsatzzweck der Dokument-Signatur durch alleiniges Setzen des Non-Repudiation-Bits in qualifizierten Endbenutzer-Zertifikaten abgedeckt. Aus sicherheitstechnischer Sicht wäre eine Begrenzung auf Non-Repudiation zu begrüssen. Andererseits besteht die Möglichkeit, dass bestehende Applikationen nur mit Zertifikaten arbeiten, in denen auch das Digital-Signature-Bit gesetzt ist. (Die Standards sind hier unklar.) Der Einsatz solcher Applikationen sollte durch die Vorschriften nicht verunmöglicht werden.

    - Für Eigenzertifikate der CSP schlagen wir vor:

Beschreibung	Feld/Erweiterung/Attribut	Inhalt
Seriennummer	**serialNumber**	Seriennummer des Zertifikats gemäss den Dokumenten ITU-T X.509, Kapitel 7, und RFC 3280 [10], Kapitel 4.1.2.2.
Name/Pseudonym und spezifische Attribute des Inhabers	**subject** **title** **subjectAltName**	Name der CSP und Niederlassungsstaat gemäss dem Dokument RFC 3739 [11], Kapitel 3.1.1.
Schlüssel und Algorithmus zur Prüfung der Signatur	**subjectPublicKeyInfo**	Schlüssel und Bezeichnung des Algorithmus zur Prüfung der Signatur des Zertifikatsinhabers gemäss dem Dokument RFC 3280 [10], Kapitel 4.1.2.7.
Gültigkeitsdauer	**validity**	Gültigkeitsdauer gemäss dem Dokument RFC 3280 [10], Kapitel 4.1.2.5.

[2] Als Zertifizierungsinstanz wird das technische Modul zur Signierung von Zertifikaten und der Liste der ungültig erklärten Zertifikate bezeichnet, englisch Certificate Authority, CA.

Name der CSP und Niederlassungsstaat der CSP	**issuer countryName**	Name der CSP und Niederlassungsstaat gemäss dem Dokument RFC 3739 [11], Kapitel 3.1.1.
Qualifizierte elektronische Signatur der CSP	**signatureValue**	Qualifizierte elektronische Signatur der CSP gemäss dem Dokument RFC 3280 [10], Kapitel 4.1.1.3.

- Für Zertifizierungsinstanz-Zertifikate, unter denen Zertifikate ausgegeben werden, schlagen wir die folgende zusätzliche Angabe vor:

Angabe, dass es sich um ein Zertifizierungsinstanz -Zertifikat handelt	**basicConstraints**	In Basic Constraints muss der Wert CA auf true gesetzt werden gemäss dem Dokument RFC 3280 [10], Kapitel 4.2.1.10

- Für Zeitstempeldienst-Zertifikate schlagen wir die folgende zusätzliche Angabe vor:

Angabe, dass es sich um ein Zeitstempeldienst-Zertifikat handelt	**extendedKeyUsage**	Information, dass das Zertifikat nur für Zeitstempeldienst gebraucht wird, in Form eines Objektbezeichners (OID) gemäss den Dokumenten RFC 3280 [10], Kapitel 4.2.1.13 und RFC 3161, Kapitel 2.3.

Kommentar: Die Anforderungsliste für Eigenzertifikate ist bewusst kurz gehalten, um den organisatorischen Aufwand zu begrenzen. So sollte etwa einer ausländischen CSP, die sich in der Schweiz anerkennen lässt, die Möglichkeit belassen werden, qualifizierte Zertifikate nach ZertES unter dem selben Stammzertifikat auszustellen, unter welchem auch ausländische qualifizierte Zertifikate ausgegeben werden.

6. Zu „5. Abschnitt: Haftung für Signaturschlüssel: Sicherheitsvorkehrungen“:

6.1. Ein Hinweis in der VZertES, dass die Signaturschlüssel nicht mit unsicheren Systemen eingesetzt werden sollen, ist angebracht. Zudem ist dem Umstand Rechnung zu tragen, dass für den Missbrauch auch die Verfügung über die sichere Signaturerstellungseinheit, das heisst Smartcard, USB Token oder HSM notwendig ist.
Unser Vorschlag:
Art. 11 Signaturschlüssel
Absatz 1(Änderung): “Die Inhaberin oder der Inhaber des Signaturschlüssels darf diesen keiner anderen Person anvertrauen. Sie oder er muss den Signaturschlüssel **bei Nicht-Gebrauch**, soweit zumutbar, auf sich tragen oder diesen wegschliessen.“
Absatz 2(neu): “**Die Inhaberin oder der Inhaber des Signaturschlüssels muss darauf hingewiesen werden, dass der Signaturschlüssel nicht mit vermutlich unsicheren Systemen eingesetzt werden soll.**“

Kommentar: Es ist wichtig, dass ein Endbenutzer auf die Gefahren von unsicheren Systemen hingewiesen wird. Zum Beispiel kann ein manipuliertes System dem Benutzer ein anderes Dokument anzeigen, als er in Wirklichkeit signiert.
Ein absolut sicheres System zu fordern ist unmöglich, deshalb wurde die Formulierung „vermutlich unsicher“ gewählt. Hingegen sollte der Benutzer auf gängige Sicherheitsregeln hingewiesen werden, zum Beispiel auf den Einsatz von Anti-Viren-Software.

6.2. Der Art. 12 „Passwort“ Abs. 1 befriedigt nicht: „Passwörter, die Zugang zum Signaturschlüssel verschaffen, müssen eine Länge von mindestens vier Zeichen (Zahlen oder Buchstaben) aufweisen.“ Diese Formulierung steht im Widerspruch zu den strengen Haftungsregelungen im Gesetz und den hohen Anforderungen an die Sicherheit, welche in den TAV zum Ausdruck kommen.
Es ist klar, dass auch ein Passwort mit einer Länge von mehr als vier Zeichen ausgespäht werden kann, solange der Zugang zum Signaturschlüssel über die PC-Tastatur erfolgt. Trotzdem sollte ein Passwort wie „1234“ ausgeschlossen sein.
Unser Vorschlag:
Art. 12 Passwort
Abs. 1 „Passwörter, die Zugang zum Signaturschlüssel verschaffen, müssen eine Länge von mindestens **sechs** Zeichen (**Ziffern und Buchstaben**) aufweisen.„

7. Konsequenzen der Einführung des ZertES, VZertES und TAV für den elektronischen Geschäftsverkehr in der Schweiz:
   7.1. Eine wichtige Anwendung der bisherigen Verordnung ZertDV vom 12. April 2000, welche durch die neue VZertES per 1.1.2005 abgelöst wird, betrifft die Anerkennung von MWSt relevanten Dokumenten (elektronische Rechnungen) durch die Eidgenössische Steuerverwaltung (ESTV). Die elektronische Signatur der Rechnung gewährleistet gegenüber der ESTV als aussenstehender Drittpartei die Herkunft der Rechnung und deren Integrität, welche die ESTV bei einer Revision kontrollieren kann. Der Rechnungsempfänger kann so den Vorsteuerabzug geltend machen. Bezüglich des Rechtsverhältnisses zwischen Rechnungsteller und Rechnungsempfänger ist eine qualifizierte elektronische Signatur gemäss ZertES aber nicht erforderlich, da eine Rechnung nicht unterschrieben werden muss. Somit kann die ESTV wie bisher auch Rechnungen für den Vorsteuerabzug anerkennen, wenn diese mit einer fortgeschrittenen elektronischen Signatur versehen sind. Die ESTV ist frei, wie bisher entsprechende Verordnungen zu erlassen und Systeme anzuerkennen, welche die notwendige Sicherheit gewährleisten. Insbesondere ist für die ESTV bei der Anerkennung eines Systems wichtig, dass der Inhaber den Signaturschlüssel unter seiner alleinigen Kontrolle halten kann.
   7.2. Die Anerkennung einer qualifizierten elektronischen Signatur gemäss ZertES durch die ESTV zur Geltendmachung des Vorsteuerabzuges ist nicht zwingend, zur Förderung des Gebrauchs der elektronischen Signa-

tur aber zu begrüssen. Deshalb sollten die Bestimmungen in der VZert-ES und in den TAV bezüglich der sicheren Signaturerstellungseinheiten im Einklang mit den Anforderungen der ESTV an die Anerkennung von Zertifizierungsdienstanbieterinnen sein.
In diesem Sinne sind auch unsere Bemerkungen in Punkt 6 zu verstehen.

Mit freundlichen Grüssen

Otto Müller Adrian Müller

Die Firma Dr. Otto Müller Consulting ist eingetragen im HR unter CH-020.1.021.491-5
Sie ist Mitglied der Zürcher Handelskammer, siehe: 02801737