Sehr geehrter Herr Fischer,
Sehr geehrter Herr Jenni,

herzlichen Dank für die Zustellung der Entwürfe der Verordnung sowie den technischen und administrativen Vorschriften über Zertifizierungsdienste mit der Bitte, Ihnen dazu eine Stellungnahme abzugeben. Zum heutigen Zeitpunkt finde ich es gut, den europäischen Standard ETSI TS 101 456 und dessen mitgeltenden Dokumente zu übernehmen und in die technischen und administrativen Vorschriften einzubinden. Dies unterstreicht den Willen des Gesetzgebers, sich dem europäischen Gesetzesrahmen anzunähern. Das macht insbesondere auch deshalb Sinn, weil eine elektronische Signatur über das Internet auch länderübergreifend eingesetzt werden kann. Dabei wurde auch berücksichtigt, dass im grossen europäischen Raum auch entsprechende Technologien, welche dem Standard genügen, zur Verfügung stehen und stehen werden.

Stellungnahme zum Entwurf "Technische und administrative Vorschriften"

- Sämtliche Anforderungen des Standards ETSI TS 101 456 des Kapitels 7 wurden übernommen mit Ausnahme des § 7.2.4 Key Escrow, welcher auch für die CSP und für die Inhaber des Zertifikates gilt. Ist in der Schweiz Key Escrow zugelassen?

- 3.3.4 Verwendung des Signaturschlüssels der CSP
b) Dieser Absatz kann meiner Ansicht nach gestrichen werden und ist mittels der Referenzierung § 7.4.8 "Business continuity management and incident handling" sowie § 7.2.6 "End of CA key life cycle" abgedeckt.

-3.4.1 Registrierung
a) Schreibfehler: -> Kapitel 7.3.1 Subscriber registration

3..4.3.1 Felder des Zertifikates

Grundsätzlich sollte hier in der Darstellung zwischen sogenannten Basis Felder des Zertifikates (Basic Certificate Fields) und Erweiterungsfelder (Extensions) des Zertifikates unterschieden werden. Insbesondere bei den Erweiterungsfeldern (Extensions) sollte eine Angabe gemacht werden, ob diese als critical markiert sind oder nicht.

Bei den Basis Felder des Zertifikates (Basic Certificate Fields) fehlen meiner Meinung nach noch folgende Felder:
- version, wichtig, insbesonder für CRL's
- signatureAlgorithm
- signature
- subjectPublicKeyInfo vorhanden, untergeordnete Datenfelder wie algorithm und subjectPublicKey fehlen und sollten aufgeführt werden.

Die geforderten Attribut-Typen wie "title", "countryName" sind in den korrekten Basis Felder des Zertifikates eingetragen; der Attribut-Typ "pseudonym" fehlt und sollte ebenfalls in das Feld "subject" eingetragen werden.

Die geforderten Extensions sollten wie oben vorgeschlagen als Extensions in einem so definerten Teil der Tabelle erscheinen:
- subjectAltName
- issuerAltName
- keyUsage

- cRLDistributionPoints
- qcStatements

Bei der Extension keyUsage ist per Definition RFC 3280 Bit (0) für digitalSignature im BIT STRING {}vorgesehen.

Generelle Bemerkung:
Der Standard ETSI TS 101 456 ist bezüglich Anzahl der formulierten Anforderungen weniger umfangreich als der ANSI Standard X9.79 bzw. ISO 21188-1, dafür erfordert er durch seine Abstraktion mehr Vorstellbarkeit und Interpretationsarbeit bei der Umsetzung - insbesondere bei der Erstellung einer Checkliste zur Zertifizierungsprozedur. Hingegen verweist er klar auf ISO 17799 und RFC 2527. Der ANSI Standard X9.79 bzw. ISO 21188-1 basiert im wesentlichen auf ISO 17799 und ISO 15782-1, beinhaltet wesentlich mehr Controls als ETSI TS 101 456 und ist dem TAV von 2001 sehr ähnlich, insbesondere dem vorangehenden Entwurf.

Stellungnahme zum Entwurf "Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur"

Art.2 : Sehr gut, gibt nun klare Parameter für die Anerkennungsvoraussetzungen an

Art. 7: Vorschlag einer Präzisierung (Anforderungen sind zwar vollständig enthalten, aber für einen Nicht-Profi möglicherweise nicht ganz offensichtlich):
Titel: Ungültigkeitserklärung qualifizierter Zertifikate vor Ablauf der Gültigkeit des Zertifikats. Damit würde meiner Ansicht nach Art. 7 Abs.3 noch etwas klarer.

Art. 11: Für mich etwas zu mechanistisch:. Vorschlag:
Sie oder er muss den Signaturschlüssel, soweit zumutbar, auf sich tragen oder diesen mittels physischen und logischen oder kryptographischen Massnahmen vor unberechtigtem Zugang schützen.

ich hoffe, Ihnen damit gedient zu haben und verbleibe,

mit freundlichen Grüssen

Peter Stadlin
Zugerbergstrasse 56
CH-6300 Zug

Tel: 041-711 56 29
Mobil: 076-398 11 66