Peter Keller
ch. de la Pépinière 54
1752 Villars-sur-Glâne

Email: peter_keller@gmx.net

Villars-sur-Glâne, den 16.7.2004

BAKOM
Zukunftsstrasse 44
2501 Biel

Betrifft: Stellungnahme zu den Vernehmlassungsentwürfen der VZertES und deren technischen und administrativen Vorschriften (TAV)

Sehr geehrter Herr Furrer

Ich gratuliere den an der Redaktion dieser Verordnung und ihrer Ausführungsbestimmungen beteiligten Stellen für ihre Arbeit und bedanke mich für den betriebenen Aufwand und für die Möglichkeit, dazu Stellung zu nehmen. Ich begrüsse und unterstütze die Motivation und die Grundsätze der in der vorliegenden gemachten Regelungen. Im folgenden werden einige Änderungs- oder Ergänzungsvoschläge aufgelistet. Dies bedeutet, dass ich diejenigen Passagen, für die keine Bemerkungen bestehen, vorbehaltlos unterstütze.

Allgemeine Bemerkung

Anforderungen an Registrierungsstellen

Es werden keine spezifischen Anforderungen an die Sicherheit der Infrastruktur und Organisation der Registrierungsstellen gemacht. Es sollte abgeklärt werden, ob sich solche Anforderungen indirekt aus den bestehenden ergeben. Wenn nicht, sollten sie formuliert werden. Generell sollten die Anforderungen an Registrierungsstellen ähnlich hoch sein wie diejenigen an die Anbieterin von Zertifizierungsdiensten selber.

Bemerkungen betreffend die VZertES

Art. 1 Abs 2

Es wäre evtl. vorzuziehen, dass anstatt der SAS das BAKOM oder das BIT die Aufgabe der Anerkennung von Anbieterinnen von Zertifizierungsdiensten übernimmt, in der Annahme dass diese beiden Bundesämter mehr Kompetenzen in diesem Bereich haben und darum besser geeignet sein könnten.

Art. 2, Abs. 1

Die Versicherungssummen sind tendenziell zu hoch und dürften markthemmend wirken. Es ist nicht anzunehmen, dass sich in absehbarer Zeit eine Vielzahl von Anbieterinnen von Zertifizierungsdiensten anerkennen lassen wird und folglich Kunden von solchen Versicherungen werden. Durch die

resultierende wahrscheinlich sehr tiefe Kundenzahl dürften darum die Versicherungsprämien dermassen exorbitant hoch ausfallen, dass diese für eine Anbieterin von Zertifizierungsiensten nicht mehr finanziell tragbar sind. Somit besteht die Gefahr, dass sich in der Schweiz gar keine Anbieterin anerkennen lässt, was dem Grundsatz und der Motivation der ZertES entgegen spricht, nämlich der Förderung des gesicherten elektronischen Geschäftsverkehrs. Als Alternativvorschlag könnten die Versicherungssummen auf 500'000 pro Versicherungsfall und auf 2 Millionen pro Versicherungsjahr gesenkt werden. Tendenziell sollten die geforderten Versicherungssummen eher zu tief als zu hoch angelegt werden, zumindest in der jetzigen Startphase und mangels praktischen Erfahrungen.

Ausserdem dürfte im Moment kein Markt für solche Versicherungen existieren. Die Garantiestellung dürfte darum der Normalfall sein. Daher kann Art. 2 umformuliert werden:

"Die Anbieterin von Zertifizierungsdiensten hat eine Haftungs-Garantie vorzulegen für einen Betrag von mindestens 500'000 Franken pro Ereignis oder 2 Millionen Franken pro Jahr. Die Garantie kann auch in Form einer Versicherung geleistet werden."

Art. 5, Abs. 2

Die Formulierung des letzten Teilsatzes ist fehlerhaft: "…Signaturprüfschlüssel zugeordnet werden kann, dessen Zertifikat erneuert werden soll". Aus der aktuellen Formulierung lässt sich schliessen, dass das neue Zertifikat sich auf den selben Signaturprüfschlüssel bezieht, der bis anhin verwendet wurde. Es ist jedoch gängige Praxis und dürfte unbestritten sein, dass bei einer Erneuerung des Zertifikats, die sich nach Ablauf seiner Gültigkeitsdauer aufzwingt, auch das Schlüsselpaar erneuert wird. Dies darum, weil definitionsgemäss die Gültigkeitsdauer diejenige Zeitperiode bezeichnet, während der mit genügender Gewissheit anzunehmen ist, dass aus dem Signaturprüfschlüssel – und allenfalls aus den hergestellten Signaturen – der Signaturschlüssel nicht abgeleitet werden kann. Das heisst dass nach Ablauf der Gültigkeitsdauer diese Gewissheit nicht mehr besteht. Es würde somit wenig Sinn machen, nach Ablauf der Gültigkeitsdauer ein neues Zertifikat für das selbe Schlüsselpaar zu erstellen. Eine korrekte Formulierungsmöglichkeit wäre: "… Signatur versehen ist, die anhand des alten Signaturschlüssels erzeugt wurde." Oder: "…Signaturprüfschlüssel zugeordnet werden kann, dessen Zertifikat abläuft."

Es sollte ausserdem ergänzt werden (hier oder in den TAV), dass ein solcher mit dem alten Signaturschlüssel signierter Erneuerungsantrag vor Ablauf der Gültigkeitsdauer des Zertifikats zu erfolgen hat.

Art. 7

Der erste Satz in Abs. 1 ist eine Wiederholung des Art. 10 Abs. 2 ZertES. Dies sollte am Anfang erwähnt werden.

Es sollte ausserdem ergänzt werden (hier oder in den TAV), dass eine Ungültig-Erklärung eines Zertifikats nicht rückgängig gemacht werden darf.

Zudem sollte eine maximale Zeitspanne nach Eingang eines Antrags auf Ungültig-Erklärung gefordert werden, vor der die Anbieterin von Zertifizierungsdiensten die Behandlung des Antrags abgeschlossen haben muss (Überprüfung der Rechtmässigkeit des Antrags, markieren des betroffen Zertifikats als ungültig in der Zertifikatsliste). Diese Zeitdauer kann z.B. 18 Stunden sein.

Ausserdem sollte ergänzt werden, dass falls CRL's als Methode der Statusabfrage eingesetzt werden, dass die nächste Ausgabe der CRL, die nach Abschluss der Behandlung des Antrags auf Ungültig-Erklärung herausgegeben wird, die Seriennummer des soeben ungültig erklärten Zertifikat beinhalten muss. Falls eine online Abfrage als Methode der Statusabfrage eingesetzt wird, sollte gefordert werden, dass der neue Status binnen der oben erwähnten Zeitdauer nach Eingang des Antrags als Antwort auf Abfragen herausgegeben wird.

Schlussendlich sollte, falls CRLs eingesetzt werden, eine maximale Zeitdauer zwischen den veröffentlichten Ausgaben gefordert werden, z.B. 8 Stunden. Somit ergibt sich vom Zeitpunkt der Einreichung des Antrags bis zur Auswirkung auf die online Abfrage max. 18 Stunden und auf die CRL max. 18+8=26 Stunden. Bei Verlust des Private Keys erhöhen sich diese Zeiten zwischen Feststellung des Verlusts und Auswirkung auf die Statusabfrage um 24 Stunden. (Ein Überprüfer einer Signatur wird somit in der Praxis wohl mind. 42 bzw. 50 Stunden nach dem Zeitpunkt der Signatur warten, bis er den Status des Zertifikats abfragt und in der Folge der Signatur vertraut, und darauf basierend diejenige Handlung oder Transaktion einleitet, die durch die Signatur bezweckt wird. Darum sind diese Zeitspannen möglichst kurz, gleichzeitig aber zumutbar und wirtschaftlich, zu halten.)

Art. 10, Abs. 2

Es fehlen Bestimmungen für den Fall, dass die betreffende anerkennende Stelle nicht mehr existiert. Vorschlag: "Existiert diese anerkennende Stelle nicht mehr, beauftragt das Bundesamt [oder die SAS] eine andere Anerkennungsstelle. Existiert keine anerkennende Stelle mehr, übernimmt das Bundesamt diese Aufgabe."

Art. 13, Abs. 2

Es sollte folgendes ergänzt werden: "Das gleiche gilt, wenn das Zertifikat keine Gewähr mehr bietet für die Zuordnung des Signaturprüfschlüssels zum Inhaber des Zertifikats, nota bene wenn Anlass besteht anzunehmen, dass eine andere Person oder Stelle Kenntnis über den Signaturschlüssel erlangt hat, d.h. dass der Signaturschlüssel kompromittiert wurde."

Bemerkungen zu den Ausführungsvorschriften

Schlüssellängen

Es sollten pro in der Praxis gängigem Signaturalgorithmus eine minimale Schlüssellänge für die Schlüssel der Anbieterin sowie der Schlüsselinhaber gefordert werden, z.B. für RSA jeweils mind. 1024 bit.

Gültigkeitsdauer der Zertifikate

Es sollte pro in der Praxis gängigem Zertifikats-Signatur-Algorithmus eine maximale Gültigkeitsdauer der Zertifikate gefordert werden, z.B. für RSA 1024 Bit jeweils max. 5 Jahre.

Pflichten der Inhaber

Es wird nicht auf das Kap. 6.2 in der ETSI Norm [6] verwiesen. Ein entsprechendes Kapitel mit Anforderungen nach diesem Text sollte jedoch eingefügt werden. Sollte dies trotzdem nicht getan werden, sollte im Kap. 3.4.1 der Absatz 7.3.1 h) in der dort referenzierten Norm [6] wegbedungen werden, da dieser sich auf das Kap. 6.2 in [6] bezieht.

Kapitel 3.2.1 b)

Es werden keinerlei regelmässige Kontrollen der Anbieterinnen gefordert. Es sollte jedoch zumindest verlangt werden, dass die Prüfberichte der internen Audits jeweils der Anerkennungsstelle auszuhändigen und von diesen 11 Jahre lang aufzubewahren sind.

Es sollte ausserdem geregelt werden, wie vorzugehen ist, wenn es die Anerkennungsstelle nicht mehr gibt. Vorschlag: Analog zum Vorschlag zum Art. 10 VZertES oben.

Kap. 3.2.2

Grammatikfehler: "Aussage ~~der~~ über die Zertifizierungspraxis (CPS)". Alternative: lediglich "Zertifizierungspraxis (CPS)"

Kap. 3.4.3.1, Tabelle

3. Reihe "subjectAltName"
Zur Zeit besteht keinerlei Forderung für das Format Attributs "subjectAltName". Es sollte gefordert werden, dass es gemäss dem RFC 3280 Kap. 4.2.1.7 zu erstellen ist.

8. Reihe "issuerAltName"
Es fehlt ein Feld, das den expliziten Text mit der Angabe enthält, dass die Anbieterin anerkannt ist. Dass sich dies aus dem Kontext dieser Vorschriften und der Erwähnung der Anerkennungsstelle ergibt, dürfte für viele Überprüfer von qualifizierten Zertifikaten nicht klar sein. Es sollte darum ein solches Feld gefordert werden, z.B. als Attribut "QCStatements".

8. Reihe
Die Abkürzungen EA und SAS sollten durch ihre ausgeschriebenen Versionen ersetzt werden. Sie dürften vielen Personen nicht geläufig sein.

9. Reihe "keyUsage"
Es sollte nicht nur Bit Nummer 1 gesetzt werden, sondern alle anderen auf Null gesetzt werden, mit Ausnahme derer die nötig sind damit mit dem Zertifikat auch ein Login bzw. ein Authentifikationsprozess gemacht werden kann (z.B. SSL Client Authentifikation oder Windows Logon). Ein qualifiziertes Zertifikat sollte auch für Logins benützt werden können.

11. Reihe "QCStatements", Wert
Grammatikfehler: "Der Maximalwert der Transaktion ~~sind~~ ist in der …"

11. Reihe "QCStatements"
"… Kapitel 3.2.6, ~~in Form~~ unter Verwendung eines …". Der Wert wird nicht in Form des OID angegeben sondern ergibt sich aus dem INTEGER und dem EXPONENT gemäss RFC.

Mit freundlichen Grüssen

Peter Keller