Stellungnahme
zu
VZertES

Version 1.0
Juni 2004

Daniel Muster
Bit Pattern Security
Feldblumenweg 43
8048 Zürich

Einleitung

Grundsätzlich geht es bei einer Vernehmlassung bekanntlich darum, auf Unstimmigkeiten hinzuweisen, und nicht darum, zu erwähnen, was alles gut ist oder hervorragend erledigt worden ist. Dies ist aus Sicht der Hersteller der Verordnung und der Bestimmungen etwas undankbar. Doch möchte ich es nicht versäumen, gleich zu Beginn die folgenden positiven Aspekte hervorzuheben:

- Bemühung um Kompatibilität mit anderen Standards und europäisch anerkannten Normen
- Klarheit in der Sprache und im Ausdruck; z.B. das Definieren von Begriffen
- Übersichtlichkeit im Aufbau der Verordnung und in der Vorschrift
- Die Normierung vieler Sachverhalte, welche im Umfeld einer PKI anstehen
- Quellenverweise auf internationale Normen

In Folgendem werden aber nun diejenigen Punkte aufgelistet, welche meines Erachtens nicht oder nicht ausführlich genug geregelt worden sind. Die Auflistung besagter Punkte erfolgt nach jeweiliger Thematik und nicht in der Reihenfolge der Artikel der Verordnung (VzertES) und Kapitel in der Vorschrift über Zertifizierungsdienste im Bereich elektronischer Signatur (VZES).

Ungültigkeitserklärung eines Zertifikats

Wie schnell?

Im Art. 10 Abs. 1 ZertES wird festgelegt, dass die Ungültigkeitserklärung, sprich Herstellung und Publikation der Revokationsliste (CRL), unverzüglich zu erfolgen hat. Es wäre nun wünschenswert gewesen, dass in der Verordnung festgehalten wird, wie schnell dies zu erfolgen hat.

Der Hinweis auf das kostenpflichtige ETSI Dokument 101 456 im Kapitel 3.4.5 der Vorschrift über Zertifizierungsdienste im Bereich elektronischer Signatur (VZES) ist meines Erachtens nicht ausreichend, weil die besagte Information wegen deren Wichtigkeit allgemein klar ersichtlich sein muss.

Authentisierung bei Ungültigkeitserklärung

Änderungsvorschlag zur Formulierung in Art 7 Abs. 1 VZertES. „Diese Anforderung gilt als erfüllt“ sollte durch „Diese Anforderung gilt unter anderem als erfüllt“ ersetzt werden.

Mit der letzteren Formulierung wird klarer ersichtlich, dass es noch weitere Möglichkeiten geben kann, wie eine Person eine Ungültigkeitserklärung verlangen kann. Insbesondere kann der Antrag dann nicht signiert werden, wenn der private Schlüssel des Inhabers oder der Inhaberin eines qualifizierten Zertifikats abhanden gekommen ist.

Verifikation eines Zertifikats

Grundsätzliches

Es sollte grundsätzlich festgehalten werden, nach welchem Modell die Gültigkeit eines Zertifikats geprüft wird, nach dem Ketten- oder Schalenmodell. (Eine einfache Erklärung und Gegenüberstellung beider Modelle befindet sich bei [Ruw])

Nach welchem Modell geprüft wird, hat einen Einfluss auf:

- Den Prozess des CA Schlüsselwechsels einer CA, wenn die Gültigkeit des CA-Zertifikats abgelaufen ist.
- Die Verwendungsdauer der privaten Schlüssel und die Gültigkeitsdauer der Inhaber/in Zertifikate. (Die Verwendungsdauer des privaten Schlüssels wird im Feld private key usage period definiert.)
- Wie lange der private Schlüssel der CA zur Herstellung der Zertifikate verwendet werden darf.
- Wie elektronische Signaturen nach der Revokation oder nach Ablauf der Gültigkeit eines Zertifikats geprüft werden können oder eben nicht.
- Die langfristige Prüfung elektronischer Signaturen und folglich auf die langfristige Aufbewahrung (Archivierung) elektronisch signierter Dokumente.

Aus dem gesamten Wortlaut der Verordnung lässt sich schliessen, dass die Zertifikate nicht nach dem Schalen-, sondern nach dem Kettenmodell geprüft werden sollen. Nach welchem Modell geprüft wird, ist jedoch so wichtig, dass es klar festgehalten werden sollte.

Ungültigkeitserklärung eines Zertifikats

Grundsätzlich muss beschrieben werden, wie die bereits geleisteten, elektronischen Signaturen eines Inhabers eines qualifizierten Zertifikats geprüft werden, welchen Gültigkeitsstatus die zuvor geleisteten Signaturen haben, nachdem das betreffende Zertifikat für ungültig erklärt worden ist oder dessen Gültigkeit abgelaufen ist.

Weiter sollte geregelt werden, wie die langfristige Archivierung elektronischer Signaturen und deren Verifikation vonstatten gehen soll. Zur Problematik der Archivierung der elektronischen Signaturen, siehe auch www.archisg.de.

SW für die Verifikation

In Art 6 ZertES wird aufgeführt, worauf beim Signaturprüfvorgang zu achten ist. Doch dies wird von einer SW durchgeführt, und ein Otto-Normalverbraucher und Anwender dieser SW weiss nicht, ob die von ihm eingesetzte SW den Kriterien gemäss Art.6 ZertES entspricht. Deswegen sollte dem Benutzer eine Liste von SW zur Verfügung gestellt werden, welche sich konform zu Art. 6 ZertES verhält.

> Z. B. in Deutschland führt die Regulierungsbehörde für Telekommunikation und Post (RegTP, www.regtp.de) eine Liste von qualifizierten Anbietern, deren SW sich gemäss Deutschem Signaturgesetz konform verhält.

Im Übrigen ist die Haftung nicht (wie bei anderen möglichen Schadensfällen im Umfeld elektronischer Signaturen) klar geregelt, wenn ein Schaden entsteht; infolge des Einsatzes einer nicht gesetzeskonformen SW zur Prüfung elektronischer Signaturen.

Ausstellung qualifizierter Zertifikate

Bei der Ausstellung der Zertifikate sollte weiter verlangt werden, dass sämtliche ins Zertifikat aufgenommenen Identitätskennungen, wie Email Adresse, URL, usw. auf Richtigkeit, sprich auf Zugehörigkeit des zukünftigen Inhabers oder Inhaberin des Zertifikats geprüft werden sollen. Ansonsten kann die Authentifizierung auf Basis der elektronischen Signatur umgangen werden, siehe dazu [Mus].

Infolge dessen sollte noch Art 5. Abs.1 lit. c in die VZertES eingefügt werden, welcher besagt:

> Sämtliche ins Zertifikat aufgenommenen Identitätskennungen, wie Email Adresse, sind auf Zugehörigkeit zum/r Zertifikatsinhaber/in zu prüfen.

Einstellung der Geschäftstätigkeit

Frist

Die Frist von 30 Tagen für die Einstellung der Geschäftstätigkeit einer Zertifizierungsstelle (CA) ist meines Erachtens als zu kurz gewählt, weil dies für die Kunden der besagten CA unter Umständen (insbesondere während der Ferienzeit) so viel Aufwand bedeutet, dass er in der besagten Zeit nicht oder kaum bewältigt werden kann.

Rückstellungen

Die Einstellung der Geschäftstätigkeit einer CA kann für deren Kunden Kosten verursachen, wie

- Viele Zertifikate sind z.B. etwa 40 Tage vor Einstellung der Geschäftstätigkeit bezogen worden
- Betrieblicher Aufwand für den Wechsel von Zertifikaten (Konfiguration, Kundenanschrift, Kauf neuer Zertifikate zu Unzeiten, usw.)

Deswegen sollte eine akkreditierte CA Rückstellungen für die Entschädigung der allfälligen Aufwände beim Kunden infolge Betriebseinstellung vornehmen oder Reserven bilden müssen.

Weiterführung des Betriebs

Aus Art. 10 Abs. 2 VZertES geht nicht klar hervor, ob die Anerkennungsstelle die Revokationsliste (CRL) aktualisieren oder nur für die Publikation der letzten von der CA hergestellten Liste besorgt sein muss.

Es sollte klarer festgehalten werden, was die Anerkennungsstelle bei Einstellung der Geschäftstätigkeit der CA diesbezüglich zu tun hat.

Dass die Anerkennungsstelle die Liste weiterführen, sprich aktualisieren muss, erachte ich als unverhältnismässig, denn die sich daraus ergebenden Aufwände aus Betrieb und Sicherheit sind zu hoch.

Zertifikatsformate

Allgemeines

Es sollte bei der Festlegung der Zertifikatsformate in der Vorschrift VZES grundsätzlich unterschieden werden, ob es sich um ein CA-Zertifikat oder um einInhaber/in-Zertifikat handelt. Unter Umständen sind die auszufüllenden Felder unterschiedlich, siehe auch:

http://www.bsi.de/aufgaben/projekte/sphinx/verwpki/zertifikat.htm

Die Inhalte der beiden Zertifikatstypen können (müssen) unterschiedlich sein.

Grundsätzlich sollte weiter unterschieden werden, welche der möglichen Felder obligatorisch in ein qualifiziertes Zertifikat aufgenommen werden müssen und welche fakultativen (optionalen) Felder von der CA auf Wunsch des Inhabers oder der Inhaberin des Zertifikats aufgenommen werden müssen.

Zwecks Klarheit und besseren Verständnisses sollte ein Beispiel der beiden Zertifikatstypen angefügt oder ein Hinweis darauf angegeben werden, wo dies ersichtlich ist, analog zum Deutschen Bundesamt für Sicherheit (siehe vorher aufgeführten Link).

Es fehlt meines Erachtens zudem die Definition des CRL Profils.

Zertifikatsinhalte

subject und subject Alt Name

Bei der Darstellung der Zertifikatsinhalte in VZES sollte für die Felder „subject“ und „subject Alt Name“ zwecks Klarheit jeweils eine separate Zeile verwendet werden. Im übrigen ist das Feld „subject“ gemäss RFC 3280 obligatorisch auszufüllen, das andere fakultativ.

Anmerkung: Das Feld „subject Alt Name“ bietet gemäss RFC 3280 und X.509 so viele Konfigurationsmöglichkeiten, dass klar definiert werden muss, welche Felder parametrisiert werden müssen, falls dieses Feld obligatorisch ins Zertifikat aufgenommen werden muss.

issuer

Das Feld „issuer“ sollte auch erwähnt werden, weil es gemäss RFC 3280 obligatorisch eingefügt werden muss.

Issuer Alt Name

Beim Feld „issuer“ und nicht wie in VZES auf Seite 12 in Kolonne 3 dargestellt, muss der X.500 Name eingefügt werden.

Das Feld „issuer“ ist gemäss RFC 3280 obligatorisch, während die Aufnahme des Feldes „issuer Alt Name“ ins Zertifikat fakultativ ist.

Anmerkung: Das Feld „issuer Alt Name“ bietet gemäss RFC 3280 und X.509 so viele Konfigurationsmöglichkeit, dass klar definiert werden muss, welche Felder wie parametrisiert werden müssen, falls dieses Feld ins Zertifikat aufgenommen werden muss.

Basic Constraint

Das Feld „Basic Constraint“ sollte, wie im RFC 2380 als „muss“ empfohlen, in ein CA-Zertifikat eingefügt und als „kritisch“ (engl. critical) konfiguriert werden, siehe auch:

http://www.bsi.de/aufgaben/projekte/sphinx/verwpki/zertifikat.htm

Ansonsten kann Missbrauch betrieben werden, siehe Kapitel 9.8.1 [Mud].

Authority Key Identifier

Das Feld „Authority Key Identifier“ sollte, wie im RFC 2380 als „muss“ empfohlen, in ein Inhaber/in-Zertifikat eingefügt werden; besonders dann, wenn die CA mehrere Signierschlüssel besitzt, siehe auch:

http://www.bsi.de/aufgaben/projekte/sphinx/verwpki/zertifikat.htm

Key Usage

Es sollte definiert werden, welche der verschiedenen, hier zur Verfügung stehenden Parameter zu konfigurieren sind.

Anmerkung: Die Parametrisierung dieses Feldes muss/sollte meines Erachtens abhängig vom Zertifikatstyp gestaltet werden (Inhaber/in- oder CA-Zertifikat).

Extended Key Usage

Die Konfiguration des Feldes „Extended Key Usage“ sollte von der CA optional unterstützt werden. Die Aufnahme des Feldes in ein Zertifikat sollte aber fakultativ sein.

In diesem Feld besteht die Möglichkeit, den Verwendungszweck des Schlüssels für Zeitstempeldienste einzuschränken. (Zeitstempeldienste werden unter anderem in Art. 9 Abs. 1 lit. b Ziff. 2 GebüV gefordert.)

Certificate Policies

Das Feld “Certificate Policies” sollte meines Erachtens bei den CA-Zertifikaten obligatorisch eingefügt werden. Es ermöglicht den Hinweis auf die bestehenden Bestimmungen einer CA, siehe auch:

http://www.bsi.de/aufgaben/projekte/sphinx/verwpki/zertifikat.htm

Private Key Usage Period

Abhängig davon, welches Verifikationsmodell (Schalen- oder Kettenmodell) für die Prüfung der Zertifikate verwendet wird, sollte noch das Feld „Private Key Usage Period“ eingefügt werden. Dies ist zwar im Widerspruch zu RFC 3280, doch [CaSl] ist gleicher Meinung.

QC Statement

Das QC Statement „Wert der Transaktion“ bietet aus folgenden Gründen nicht mehr Sicherheit, sondern eher mehr Unsicherheit:

> Die maximale Anzahl Transaktionen während eines Tages[1] kann so nicht beschränkt werden. Somit können Tausende von Transaktionen gestartet werden; der maximale Wert pro Transaktion ist zwar beschränkt, doch der daraus resultierende, maximale Schaden nicht.
>
> Da die meisten Zertifikate öffentlich sind oder im Klartext übertragen werden, ist jedermann der maximale Wert der Transaktion bekannt. Somit kann jemand sich auf die Attacke derjenigen Inhaber/in eines Zertifikats spezialisieren, welche einen hohen Wert in ihrem Zertifikat aufweisen.

Das Einfügen von Autorisierungsinformationen ist unter anderem aus folgenden Gründen problembehaftet:

- Wenn der maximale Wert der Transaktion des Inhabers/in ändert, muss ein neues Zertifikat gekauft werden.
- Der maximale Wert der Transaktion veranlasst im allgemeinen zur Spekulation, wie solvent der Inhaber oder Inhaber des dazu gehörigen Zertifikats ist. Die Solvabilität kann auch als ein sehr persönliches Gut erachtet werden und sollte unter Umständen vertraulich behandelt werden.

Meines Erachtens soll die Parametrisierung dieses Feldes als fakultativ erachtet werden.

Aufbewahrung der Schlüssel

Es wird in Art. 11 VZertES vorgeschrieben, dass der private Schlüssel auf sich zu tragen ist, doch wird keine Aussage darüber gemacht, in welchem Medium die privaten Schlüssel aufzubewahren sind. Die Wahl dieses Mediums bildet ein Kriterium dafür, wie sicher die Schlüssel aufbewahrt werden. Diese Sicherheit wiederum hat gemäss Art. 59a OR einen Einfluss darauf, wie die Haftung bei Missbrauch des Signaturschlüssels ausfällt.

Ob ein Medium gemäss Art. 59a OR sicher ist oder nicht, kann ein/e Otto-Normalverbraucher/in nicht wissen. Deswegen sollte eine Liste der geeigneten Aufbewahrungsmedien vom Bakom geführt und publiziert werden.

> Z. B. in Deutschland führt die Regulierungsbehörde für Telekommunikation und Post (RegTP, www.regtp.de) eine Liste von qualifizierten Anbietern, deren Aufbewahrungsmedien für private Schlüssel zum Deutschem Signaturgesetz konform sind.

In VZES Kapitel 3.3.9 wird von der CA verlangt, dass sie dem Inhaber sichere Signaturerstellungseinheiten zur Verfügung stellen muss. Für die Gültigkeitskriterien einer sicheren Signaturstellungseinheit wird auf das ETSI Dokument TS 101 456 verwiesen.

---

[1] 1 Tag beträgt die maximale Dauer, bis die Revokation eines Zertifikats vollzogen, sprich die CRL publiziert sein muss.

Zu untersuchen, ob nun ein Produkt die dort aufgeführten Sicherheitskriterien ISO 15408 erfüllt, ist nicht zu unterschätzen.

Schlüsselgenerierung

Allgemeines

Im Kapitel 3.3.1 VZES wird zur Bestimmung der Generierung der Schlüssel auf das (kostenpflichtige) ETSI Dokument 101 456 hingewiesen, doch dort findet man die Information nicht. Es wäre wünschenswert, wenn auf das Dokument „Algorithm and Parameters for Secure Electronic Signature“ [APS] und auf den folgenden Link verwiesen würde:

> http://www.bakom.ch/de/telekommunikation/internet/digsig/index.html

Generierung der Schlüssel in einer Signaturerstellungseinheit

Ob ein Produkt die Schlüssel gemäss den Vorschriften generiert, weiss ein Betreiber einer CA oder ein/e Inhaber/in eines Zertifikats in den allermeisten Fällen nicht. (Der Initialaufwand für eine allfällige Untersuchung bezüglich Schlüsselgenerierung in einer solchen Einheit ist auch nicht zu unterschätzen.)

Deswegen sollte eine Liste der geeigneten Schlüsselgeneratoren vom Bakom geführt und publiziert werden.

> Z. B. in Deutschland führt die Regulierungsbehörde für Telekommunikation und Post (RegTP, www.regtp.de) eine Liste von qualifizierten Anbietern, deren Schlüsselgeneratoren sich zum Deutschem Signaturgesetz konform verhalten.

Haftung rund um die IT-Produkte

Es sollte meines Erachtens klar definiert werden, wie die Haftung bei der Auswahl, beim Vertrieb und der Herstellung der IT Produkte rund um die elektronische Signatur gestaltet ist.

Quellen- und Abkürzungsverzeichnis

[APS]	Algorithm and Parameters for Secure Electronic Signature, http://www.bakom.ch/de/telekommunikation/internet/digsig/index.html
[Bek]	Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung vom 2. Januar 2004, RegTP
[CaSl]	Carlisle Adams, Steve Lloyd, Understandig Public Key Infrastructure, MTP 1999, ISBN 1 57870 166 X
[Mud]	Muster Daniel, Digitale Unterschriften und PKI, 2. Auflage, ISBN 3 9522387 2 4
[Mus]	Muster Daniel, Attacke auf die Authentifizierung, Version 1.3, Juni 2004, als pdf beigelegt und bei www.sgrp.ch „public“.
[Ruw]	Ruben Wolf, Verifikation digitaler Signaturen, Seminararbeit an der technischen Universität Darmstadt, 98 http://www.informatik.tu-darmstadt.de/BS/Lehre/Sem98_99/T11/
Archisig	Archisig, Fachgruppe in Deutschland, welche sich der Problematik der langfristigen Archivierung elektronischer Signaturen angenommen hat. (www.archisig.de)
CA	Certificate Authority, Zertifizierungsstelle
CRL	Certificate Revocation List
D_BSI	Deutsches Bundesamt für Sicherheit (www.bsi.de)
ETSI TS 101 456	Policy Requirements for certification authorities issuing qualified certificates
GebüV	Verordnung über die Führung und Aufbewahrung der Geschäftsbücher
RegTP	Deutsche Regulierungsbehörde für Telekommunikation und Post, (www.regtp.de)
RFC 3280	Internet X.509 Public Key Infrastructure – Certificate and CRL Profile
RFC 3739	Internet X.509 Public Key Infrastructure – Qualified Certificates Profile
VZES	Vorschrift über Zertifizierungsdienste im Bereich elektronischer Signatur
z.B.	Zum Beispiel