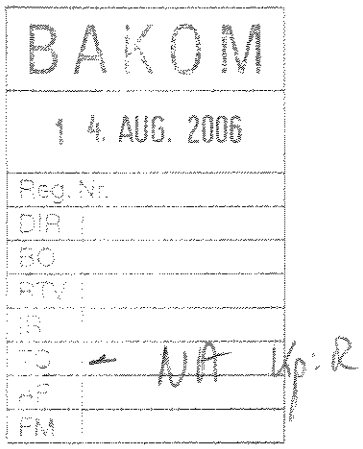
Technoparkstrasse 1, CH-8005 Zürich
Telefon +41 43 268 26 90, Fax +41 43 268 26 91
rektorat-t@hsz-t.ch, www.hsz-t.ch

Anwendungsorientierte
Forschung
und Entwicklung

HOCHSCHULE
FÜR TECHNIK
ZÜRICH



Einschreiben

Bundesamt für Kommunikation
Abteilung Elektronische Signatur
Zukunftstrasse 44
2501 Biel

Zürich, 11. August 2006

Stellungnahme zu den Technische und Administrative Vorschriften

Sehr geehrte Damen und Herren,

anbei die Stellungnahme zur Vernehmlassung der Technischen und Administrativen Vorschriften des Bakom.

Falls Sie etwelche Fragen zu meinem Bericht haben, dann stehe ich Ihnen gerne zur Verfügung.

Mit freundlichen Grüssen

Daniel Muster

Hochschule für Technik Zürich

Beilage: Erwähnt

Anmerkung: Die Stellungnahme wurde auch per E-Mail mit der Adresse digsig@bakom.admin.ch eingereicht.

Hochschule für Technik Zürich
Lagerstrasse 45 - Postfach 1568
CH-8021 Zürich
Tel.: +41 (0)43 268 25 22, Fax: +41 (0)43 268 25 30

HOCHSCHULE FÜR TECHNIK ZÜRICH

Stellungnahme zu den Technischen und Administrativen Vorschriften des Bakom [TAV]

Im Unterschied zur Verordnung des Datenschutzgesetzes (VDSG) geht aus den Technischen und Administrativen Vorschriften [TAV] viel klarer hervor, was und wie ein fachkundiger Informatiker oder Techniker umzusetzen hat. Die [TAV] enthalten, basieren und verweisen auf international anerkannte Informatikstandards. Damit wird eine Interoperabilität mit anderen Ländern ermöglicht.

Einige der hier aufgeführten Änderungsvorschläge betreffen aber nicht alleine die neue Version der [TAV], sondern auch die ältere Version. Diese Änderungsvorschläge sind aber eher von geringerer Bedeutung, doch tragen sie meines Erachtens zur Klarheit bei, was wiederum etwelche Fragen erübrigt. Im Rahmen der geplanten Überarbeitung der [TAV] könnten eventuell auch die hier zusätzlich erwähnten Punkte mitberücksichtigt werden.

Grundsätzliches

Falls Änderungen oder Anpassungen vorgenommen werden, sollte m.E. in [TAV] aufgeführt werden, welche Übergangsfristen nach Inkrafttreten der Vorschrift für die bereits anerkannten Zertifizierungsdienstanbieter gelten. Es sollte also vermerkt werden, ab wann sie die neuen Anforderungen erfüllen müssen und bis wann dies von der Anerkennungsstelle bestätigt werden soll.

Zurzeit sind 2 Zertifizierungsdienstanbieter bereits anerkannt.

Schlüsselgenerierung des(r) Antragstellers(in) Kapitel 3.3.2

Einen expliziten Hinweis in Absatz b) auf die Einhaltung des Standards ETSI TS 102 176-1, wie dies in einer früheren Version erfolgt ist, sollte wieder beigefügt werden, damit ersichtlich wird, dass auch dieser Standard einzuhalten ist.

Vorteil der expliziten Erwähnung dieses Standards: Angenommen, in einem anderen Kontext werden die Anforderungen an die kryptographischen Schlüssel definiert. Folglich kann man vereinfacht auf diesen Standard in der [TAV] verweisen. Wenn der betreffende Standard in einer Verordnung explizit erwähnt wird, erhält er in der Schweiz auch insgeheim mehr an Bedeutung,

Allgemeines zu Kapitel 3.4

Vielleicht ist es angebracht, für alle zu behandelnden Zertifikatstypen wie z.B. die CRL eine Erläuterung in Form einer Tabelle beizufügen, wie dies für das qualifizierte Zertifikat der Benutzer gemacht worden ist, s. Kapitel 3.4.2 [TAV].

Wichtig scheint mir noch der Hinweis, dass gegebenenfalls mehr Felder und Angaben, als in der TAV erwähnt, in die Zertifikate oder in die CRL aufgenommen werden dürfen. Vielleicht muss dies pro Zertifikatstyp (CA Zertifikat, CRL oder Benutzerzertifikat) separat betrachtet werden.

M.E. macht es aber in gewissen Situationen durchaus Sinn, in die qualifizierten Zertifikate weitere Informationen, wie „Subject Alternative Name", „Subject Directory

Daniel Muster
Hochschule für Technik Zürich
anwendungsorientierte Forschung und Entwicklung
Technoparkstrasse 1
CH-8005 Zürich

Hochschule für Technik Zürich
Lagerstrasse 45 - Postfach 1568
CH-8021 Zürich
Tel.: +41 (0)43 268 25 22, Fax: +41 (0)43 268 25 30

Attributes" oder „Biometric Information", [RFC 3739] beizufügen. Diese Informationen können die online[1] Identifizierung des Zertifikatsinhabers unter Umständen überhaupt erst ermöglichen und somit die Identifizierung als solches vereinfachen und erleichtern.

Kapitel 3.4.1

Absatz b). Eventuell könnte man das Feld „CRL Entry Extension" mit dem Attribut „Reason Code" vorschreiben, so dass die gewünschte Information auch in der CRL enthalten und somit für andere sichtbar ist.

Kapitel 3.4.2

Titel: Zwecks Klarheit könnte man den Titel des Kapitels in „Format der qualifizierten Zertifikate für Inhaberinnen und Inhaber" umbenennen.

Im Hinblick darauf, dass eine anerkannte CA nicht nur qualifizierte Zertifikate ausstellt, ist es vielleicht auch angebracht, zu definieren, wie nicht qualifizierte Zertifikate einer anerkannten CA gestaltet sein dürfen/müssen, insbesondere festzulegen, welche Felder sie nicht beinhalten dürfen.

qc-Statements

Ich nehme an, dass die Anforderung an das „qc-Statements" im Benutzerzertifikat gelockert werden soll, weil verschiedene renommierte SW Hersteller mit dem entsprechenden Vermerk „critical extension" nicht korrekt umgehen oder ihn nicht richtig auswerten können. Die Folge davon sind möglicherweise Fehlermeldungen oder inkorrektes Verhalten der SW.

Die richtige Auswertung der qualifizierten Zertifikate ist essenziell; insbesondere *im Hinblick auf die mögliche Haftung und etwelche Schadenersatzansprüchen*. Deswegen ist neben der richtigen Behandlung der kritischen Erweiterung auch notwendig, dass die Inhalte wie „der Grenzwert der Transaktion" dem Benutzer korrekt angezeigt werden können. *Eine SW für Unterschriftenprüfung, welche den Inhalt des qc-Statements korrekt anzeigt, kann den Vermerk der kritischen Erweiterungen sicherlich richtig be- und abhandeln.*

Zudem muss dem Benutzer klar ersichtlich gemacht werden, ob es sich um ein qualifiziertes Zertifikat einer nach ZertES anerkannten CA oder bloss um ein anderes Zertifikat einer nach ZertES anerkannten CA handelt.

Es gibt z.B. folgende Möglichkeit, wie das Problem umgangen werden kann, dass eine E-Mail SW die Verifikation der qualifizierten Signatur nicht richtig abhandelt:

- Relevantes Dokument qualifiziert signieren und in einer authentisierten E-Mail zustellen
- Den privaten Schlüssel passend zu einem nicht qualifizierten Zertifikat verwenden, damit die Authentisierung der besagten E-Mail geschützt wird.

[1] Online Identifizierung meint hier: Das Zertifikat kann allein anhand des Inhalts eindeutig dem Inhaber zugeordnet werden, ohne dass zusätzliche Personendaten oder andere Informationen von der CA benötigt werden.

Daniel Muster
Hochschule für Technik Zürich
anwendungsorientierte Forschung und Entwicklung
Technoparkstrasse 1
CH-8005 Zürich

Hochschule für Technik Zürich
Lagerstrasse 45 - Postfach 1568
CH-8021 Zürich
Tel.: +41 (0)43 268 25 22, Fax: +41 (0)43 268 25 30

Qualifizierte Zertifikate sollten bekanntlich wegen der Sicherheit im klassischen Client Server Umfeld zur Authentisierung **nicht** eingesetzt werden, weil normalerweise in diesem Kontext nicht klar ersichtlich ist, was bei der Authentisierung unterschrieben worden ist. Deshalb müssen dort andere (nicht qualifizierte) Zertifikate für die Authentisierung eingesetzt werden. Also wird der Benutzer folglich meist mehrere Zertifikate (z.B. 1 für rechtsverbindliche Signatur, 1 für die Authentisierung, 1 für die Verschlüsselung) besitzen.

Aus den soeben genannten Gründen, sollte die TAV in den Feldern qc-Statements nicht geändert werden. Für weitere Argumente s. RFC 3739, Kapitel 4 „Security Considerations".

Kapitel 3.5 Datierungssysteme

Obwohl in ETSI TS 101 861 erwähnt, könnte man explizit vermerken, dass das TSP Protokoll, definiert in RFC 3161, eingehalten werden sollte und mindestens über http realisiert werden muss.

Referenzen

ETSI TS 102 176-1 V1.2.1 (2005-07), Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms.

IETF RFC 3739 Internet X.509 Public Key Infrastructure: Qualified Certificates Profile.

IETF RFC 3161 Internet X.509 Public Key Infrastructure: Time-Stamp Protocol (TSP)

ZertES, Bundesgesetz vom 19. Dezember 2003 über Zertifizierungsdienste im Bereich der elektronischen Signatur (SR 943.03)

TAV, Technische und administrative Vorschriften, Zertifizierungsdienste im Bereich der elektronischen Signatur, SR 943.032.1, Ausgabe 2

DSG, Bundesgesetz vom 19. Juni 1992 über den Datenschutz

VDSG, Verordnung vom 14. Juni 1993 zum Bundesgesetz über den Datenschutz

Muster Daniel, Digitale Unterschriften und PKI, 3. Auflage 2006,
ISBN 3-9522387-3-2