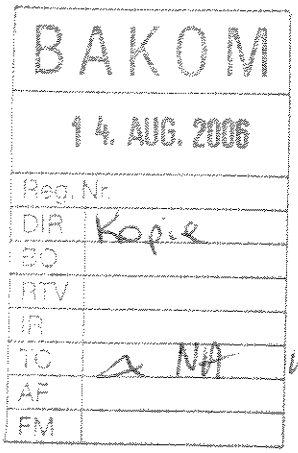

Bundesamt für Kommunikation
BAKOM
Herrn Martin Dumermuth, Direktor
Zukunftsstrasse 44
CH 2501 Biel

Bern, 11. August 2006

Anhörung der betroffenen Kreise zum Änderungsentwurf der TAV über Zertifizierungsdienste im Bereich der elektronischen Signatur (SR 943.032.1)

Sehr geehrter Herr Dr. Dumermuth

Wir bedanken uns für die Einladung zur Kommentierung des TAV-Änderungsentwurfes, der wir gerne nachkommen. Unsere Stellungnahme haben wir als betroffene Fachgruppe auf Wunsch des Vorstandes von eCH verfasst und mit diesem abgesprochen.

In der eCH-Fachgruppe Sicherheit bearbeiten wir aktuell eine Standardisierung der nicht-qualifizierten Zertifikate, die in Abstimmung mit den relevanten Marktteilnehmern kurz vor Eingabe in den eCH-Expertenausschuss ist und in den nächsten Wochen genehmigt werden sollte. Auch seitens des BAKOM erhielten wir in der Vernehmlassung wertvolle Hinweise, die in den Standard-Entwurf eingegangen sind.

In Kombination mit einer den aktuellen Markt- und Sicherheitsentwicklungen angepassten TAV werden wichtige Grundlagen zur Förderung elektronischer Geschäftsprozesse im eGovernment und der Wirtschaft geschaffen und verbessert.

Auf den nachfolgenden Seiten haben wir unsere Anmerkungen in der Reihenfolge der Gliederung zusammengetragen, die wir Ihnen als weitere Diskussionsgrundlage zur Verfügung stellen möchten.

Gern stehen wir Ihnen auch für die weitere Bearbeitung der TAV sowie angrenzender Dokumente unterstützend zur Verfügung.

Mit bestem Dank und freundlichen Grüssen

eCH-Fachgruppe Sicherheit

i.V. Werner

Gerold H. Werner
Leiter der eCH Fachgruppe Sicherheit
041 – 750 93 20
max.consult-ag@bluewin.ch

Adrian Müller
Mitglied der eCH Fachgruppe Sicherheit
078 729 78 37 044 217 40 50, 079 502 53 45
adrian@mueller-consulting.biz

Review-Protokoll

Dokument: ..... **Technische und Administrative Vorschriften über Zertifizierungsdienste im Bereich der elektronischen Signatur SR 943.032.1**

Version: ..... 3 vom 20.06.2006

Autor(en): ..... Eidgenössisches Departement für Umwelt, Verkehr und Kommunikation UVEK, Bundesamt für Kommunikation BAKOM

Review-Leitung: ..... Gerold H. Werner

Review-Protokoll: ..... v1.0 vom 04.08.2006

Nr.	Seite	Kapitel	Thema/Inhalt	Empfehlung / Aktion
1.	9	3.2 c	*„Die CSP muss jedes Jahr interne Audits …""* Betriebs- und Sicherheitskonzept der CSP sind gemäss dem vorliegenden Entwurf nicht Gegenstand der jährlichen Audits.	Prüfen, ob ggf. folgende Dokumente auch in das Audit einbezogen werden sollten: - Betriebskonzept (für die ZertES-relevanten Bereiche) - Sicherheitskonzept (dto.)
2.	9	3.2 d)	*„Die internen Audits müssen … und aufbewahrt werden"* Inhaltliche und grammatikalische Bezüglichkeit des Satzes sind nicht eindeutig. Gemeint ist eventuell (sinngemäss): (a) die Audits müssen Abweichungen und Änderungen von Technik / Organisation / Betriebspraxis gegenüber den aktuell geltenden Dokumenten (gem. 3.2.c) feststellen und dokumentieren. (b) alle Audit-Unterlagen sind zu archivieren über mindestens … Jahre (c) auf der Grundlage der Audit-Ergebnisse sowie nach Prüfung und Entscheidung der CSP sind entweder die Gegebenheiten der IST-Situation den genannten Dokumente anzupassen – oder umgekehrt. Aus der bisherigen Formulierung ergibt sich keine Verpflichtung, die erkannten Abweichungen oder Mängel überhaupt oder innerhalb bestimmter Frist zu beseitigen und die dafür erforderlichen Massnahmen ebenfalls zu dokumentieren und ggf. einer Prüfung zu unterziehen.	Da der links genannte Aspekte (a) ja substantieller Gegenstand von Audits sind und in den referenzierten ISO/IEC-Standard hinreichend abgedeckt sein sollte, bleiben wesentlich die Forderungen nach Archivierung und Umsetzung. Beispiel: d1) Alle Audit-Unterlagen sind für den Zeitraum von *n* Jahren zu archivieren. d2) Die Prüfungsergebnisse des Audits sind innert *n* Wochen umzusetzen, zu dokumentieren und in die betroffenen Dokumente einzuarbeiten.

Nr.	Seite	Kapitel	Thema/Inhalt	Empfehlung / Aktion
3.	9	3.2 e)	*„Die Politik und Praktiken der CSP … "* Nachdem bereits in den vorhergehenden Spiegelpunkten Detailaspekte angesprochen sind, wird hier nochmals auf übergeordnete ETSI Docs verwiesen. Als eine der Elementar-Anforderungen sollte der Punkt „e)" vielleicht als 3.2. a) an den Anfang platziert werden, so dass sich eine Gliederung der Punkte ergibt wie: - Grundlagen gem. ETSI TS 101 456 Kap. 7.4, 7.5 [jetzt: e) und a)] - Präzisierung der Referenzen [jetzt: b)] - Audit [jetzt: c) und d)] - Reparierte Ausrüstung [jetzt: f)] - Desaster Recovery Plan mit den Aspekten + Plan für Kontinuität … [jetzt: g)] + Prüfung und Aktualisierung des o.g. Plans [jetzt: h)] - Daten Recovery [jetzt: i)]	Reihenfolge von 3.2 e) prüfen und ggf. neu gliedern.
4.	10	3.2 h)	*„Die CSP muss … ihren Kontinuitätsplan entsprechend… nachführen"* Aus der vorliegenden Formulierung ergibt sich nur die Verpflichtung, den PLAN nachzuführen, nicht jedoch die korrespondierende technische und organisatorische Infrastruktur. Eine Frist ist ebenfalls nicht gesetzt.	Ergänzung der Formulierung etwa: *„Die CSP muss … ihren Kontinuitätsplan entsprechend … nachführen sowie dessen Implementierung sicherstellen."*
5.	11	3.3.3 a) Abs. 2 Punkt 5	*„… Die im Voraus festgelegte Anzahl darf nicht höher als vier sein;"* Analog zur Festlegung der Laufzeit eines Zertifikates könnte die Anzahl der zulässigen Fehlversuche ebenfalls der CSP überlassen werden, die ja letztlich auch die Haftung aus den entstehenden Risiken übernimmt.	Notwendigkeit der Festlegung prüfen.

Nr.	Seite	Kapitel	Thema/Inhalt	Empfehlung / Aktion
6.	12	3.3.3 d)	*„Wenn die Signaturerstellungseinheit in einer physisch gesicherten Umgebung betrieben wird …“* Dieser neu in die TAV aufgenommene Artikel adressiert offenbar die aus der Praxis und den Geschäftsmodellen der CSPs resultierende Forderung nach ZertES-konformer Massensignatur durch Server mit HSMs. Ziel scheint zu sein, eines der bislang grössten Hindernisse für einen wirtschaftlichen Betrieb der ZertES-konformen Infrastrukturen auszuräumen, indem qualifizierte Signaturen auch durch Server im Betrieb durch „bevollmächtigte Personen“ erstellt werden können. Im Ergebnis wird die qualifizierte Signatur im automatisierten Batch-Betrieb als Outsourcing-Leistung ermöglicht. Was betriebswirtschaftlich natürlich zu begrüssen ist, jedoch unseres Erachtens im Widerspruch steht zu den Bestimmungen des ZertES selbst, in dem die „ausschliessliche Verfügung“ des Signaturschlüssels durch den Zertifikatsinhaber selbst ja den wesentlichen Kern darstellt für die Gleichstellung einer qualifizierten Signatur mit der handschriftlichen Unterschrift gemäss OR Art. 14. Eine delegierte Zeichnungsberechtigung ist zwar in Recht und Praxis etabliert und alltägliche Praxis, wird in VZertES Art. 11 „Sicherheitsvorkehrungen“ Abs. 1 jedoch explizit ausgeschlossen: “Die Inhaberin oder der Inhaber eines qualifizierten Zertifikats darf die Signaturerstellungseinheit keiner anderen Person anvertrauen.“ In diesem Szenario ist auch die Prüfung der zu signierenden Inhalte durch den Zertifikatsinhaber zwar theoretisch nicht ausgeschlossen (indem diese Prüfung nicht verhindert werden darf; siehe 3.3.3 a) Abs. 2 Punkt 1), aber in der Praxis eher abwegig. Eine Anfechtung wegen praktisch fehlender Prüfmöglichkeit scheint daher doch recht erfolgversprechend. Vor diesem Hintergrund muss der gesamte Abs. d) quasi als „Hintertürchen“ zur Umgehung dieser grundlegenden Restriktion des (den TAV übergeordneten) ZertES interpretiert werden. Der rechtliche Bestand eines solchen „Work Around“ scheint uns fraglich, müsste jedoch durch juristisch qualifiziertere Instanzen geprüft werden.	Wir sehen folgende Alternativen: (a) Streichung des Abs. d), um die Konsistenz zum ZertES wieder herzustellen. (b) Ergänzung des ZertES um die Nutzung des Signaturschlüssels durch bevollmächtigte Personen oder Instanzen. Für diese Lösung sollte jedoch vorab die Kompatibilität zur EU-Richtlinie sowie der Signaturgesetze der EU-Staaten sowie anderer Wirtschaftspartnerländer geprüft und bewertet werden. Eine möglicherweise „schmerzfreiere“ und auch im Hinblick auf Haftungsfragen praxisnähere Lösung im Sinne automatisierter und durchgängiger Geschäftsprozesse auch durch Outsourcing-Dienstleister liesse sich evtl. erreichen, indem für Geschäftsprozesse, welche Massenverarbeitung bedingen (Beispiel: SHAB), keine qualifizierte Signatur gefordert wird, sondern eine solche mit vergleichbarem Sicherheitsniveau, aber eigenständigem Rechtsrahmen (z.B. gemäss Standard eCH-0048; z.Zt. in Verabschiedung).

Nr.	Seite	Kapitel	Thema/Inhalt	Empfehlung / Aktion
7.	14	3.4.2 c) Tab. Zeile 1	*„Objektbezeichner"* Da es sich bei dem gemeinten Wert nicht um eine OID handelt, wie der Name vermuten lässt, sondern um einen Hash des CA-Keys, sollte hier ein anderer Begriff gewählt werden.	Begriff eindeutig wählen; z.B. CA-Schlüssel-Identifikator oder ähnlich.
8.	14	3.4.2 c) Tab. Zeile 2	*„Geltungsbereich des Zertifikates"* Die Restriktion der keyUsage auf Bit 1 schränkt den Nutzwert des Zertifikates auf sehr wenige Anwendungsfälle ein – und macht es daher auch wirtschaftlich unattraktiv. In der Praxis werden durch diese Anforderung sinnvolle Signaturmöglichkeiten (z.B. Doc- und eMail-Signatur in Microsoft-Programmen) verhindert.	Restriktion der keyUsage prüfen und. ggf. erweitern auf weitere Signaturfunktionen. Insbesondere sollte die Zulassung von Bit 0 (digitalSignature) geprüft werden.
9.	15	3.4.2 c) Tab. Zeilen 7, 8, 9	*„qcStatements"* Wir möchten vorsorglich darauf hinweisen, dass als kritisch gesetzte qcStatements in den derzeit marktgängigen Office- und Businessanwendungen zu Fehlern bei der Signaturprüfung führen können, da die primär global ausgerichteten Anwendungen diese Parameter meist weder anzeigen noch auswerten – also eine derartige Signatur gemäss Spezifikation zurückweisen müssen. Auch für die Sorgfaltspflicht des Dritten ist eine „human readable" Anzeigemöglichkeit wesentliche Voraussetzung für eine auch juristisch tragfähige Abwicklung. Im Ergebnis wird also eine fehlerfreie Verarbeitung nur mit speziell ausgerichteten und ZertES-konformen Anwendungen erreichen können.	Setzen der qcStatements auf „Nicht Kritisch" Für Geschäftsprozesse, für die die korrekte Auswertung dieser Parameter essentiell ist, müsste die obligatorische Auswertung der qcStatements als Anforderung an die Applikation gestellt werden. Insbesondere die Angabe eines pauschalen Grenzwertes einer Transaktion (in welcher Währung/Einheit?) könnte in verschiedenen Appliktionen und Rollen des Zert-Inhabers zu Konflikten führen. Die mittelfristig beste Lösung ist unseres Erachtes, die Angaben in qcStatements auch in einer „human-readable" Form in die Erweiterung certificatePolicies zu schreiben.

Nr.	Seite	Kapitel	Thema/Inhalt	Empfehlung / Aktion
10.	15	3.4.3 c) Punkt 3	*Kritische Erweiterung für CSP Zertifikat „qcStatements"* Im Gegensatz zur Option, die qcStatements in den User-Zertifikaten auf kritisch zu setzen oder nicht, wird hier für das CSP-Zertifikat das critical-flag für diese Erweiterungen gefordert. Dies führt bei der Prüfung der Zertifikatskette zu den selben Problemen wie die kritisch gesetzte qcStatements im Benutzerzertifikat.	Weglassen der qcStatements in CA-Zertifikaten
11.	15	3.4.3 d)	*Nicht-kritische Erweiterungen des CSP-Zertifikates*	Es sollten zusätzlich folgende Erweiterungen aufgenommen werden: - subjectKeyIdentifier Die Erweiterungen crlDistributionPoint und authorityKeyIdentifier sollten für Root-Zertifikate nur optional sein.