keyon

Bundesamt für Kommunikation
Zukunftstrasse 44
2501 Biel

Rapperswil, 5. August 2006

Stellungnahme Änderungsentwurf SR 943.032.1

Sehr geehrte Damen und Herren

Mit diesem Schreiben nehmen wir Stellung zum Änderungsentwurf der technischen und administrativen Vorschriften über Zertifizierungsdienste im Bereich der elektronischen Signatur (SR 943.032.1). Wir wissen es sehr zu schätzen, dass wir zu einer Stellungnahme eingeladen wurden.

Kapitel 3.3.3 Bst. d

Wir begrüssen sehr, dass die Gegebenheiten am Markt hinsichtlich der Verfügbarkeit von zertifizierten HSM berücksichtigt werden. Die Verwendung von FIPS 140-2 Level 3 (oder höher) zertifizierten HSM sollte unbedingt ermöglicht werden.

Wir haben jedoch zur aktuellen Formulierung einige Vorbehalte, die untenstehend aufgeführt sind:

I. Alle unter Bst. d aufgeführten Massnahmen lassen vermuten, dass die FIPS 140-2 Level 3 Zertifizierung gegenüber der CC EAL4+ oder ITSEC E3 hoch Zertifizierung als minderwertiger betrachtet wird. Wenn diese Vermutung zutrifft, müssten demnach die Unterschiede der Anforderungen an die jeweiligen Zertifizierungen detailliert aufgeführt werden, bevor man entsprechende Massnahmen beschreiben kann, um einen äquivalenten Sicherheitslevel zu erreichen. Uns liegt keine solche Gegenüberstellung vor, daher können wir den Ursprung und die Absicht der Formulierungen nicht genau beurteilen.

II. Die Formulierung „Die CSP muss sicherstellen, dass die Signaturerstellungseinheit und der Server, auf dem sich die Signierapplikation befindet, …“, bezieht sich primär auf das Umfeld der SSCD (z.B. der Signaturserver oder die Signierapplikationen). Diese Anforderung soll sicherstellen, dass die SSCD nicht durch bösartige Software, welche auf einem Signierserver installiert wurde, missbraucht wird.

    Diese Anforderung ist jedoch vollständig unabhängig vom Zertifizierungsgrad der SSCD und sollte daher nicht spezifisch auf

keyon
Schönbodenstrasse 4
8640 Rapperswil
Switzerland
Tel +41 55 220 64 00
Fax +41 55 220 64 01
www.keyon.ch
info@keyon.ch

keyon

die FIPS Zertifizierung angewendet werden. Diese Anforderung sollte entweder unabhängig von der Zertifizierung gestellt oder umformuliert werden. Wir schlagen letzteres vor.

Der Einsatz von zertifizierten Signaturkomponenten oder zertifizierten Signaturbibliotheken, wie dies z.B. in Deutschland gefordert wird, ändert am Risiko eines Missbrauchs der SSCD durch Umsysteme nichts, solange die Lieferapplikationen der zu signierenden Daten nicht ebenfalls zertifiziert sind. Letzteres ist praxisfremd, nicht wirtschaftlich umsetzbar und am Markt nicht erhältlich. Auf eine allfällige Forderung zur zwingenden Verwendung von zertifizierten Signaturkomponenten oder zertifizierten Signaturbibliotheken sollte daher nicht eingegangen werden.

III. Der Betrieb der SSCD und der Signierapplikation gemäss ISO 27001 erachten wir als sinnvoll. Es sollten jedoch analoge Richtlinien erlaubt werden.

IV. Falls der physische Schutz der Signierschlüssel eines FIPS 140-2 Level 3 HSM nicht nachweislich schlechter ist als der physische Schutz der Signierschlüssel in einem CC EAL4+ oder ITSEC E3 hoch zertifizierten HSM, sollte auf die letzte Forderung hinsichtlich Zugangskontrolle zur SSCD und zur Signierapplikation verzichtet werden. Die Einrichtung eines solch physisch gesicherten Raumes inkl. den geforderten Kontrollen und Protokollen ist kostenintensiv und in der Praxis nur bei grossen Unternehmen umsetzbar.

Im Weiteren ist die Forderung, dass der Zugriff zur Signierapplikation kontrolliert und nachvollziehbar sein soll, unabhängig vom Zertifizierungsgrad der SSCD (siehe Punkt II.). Diese Anforderung sollte daher nicht spezifisch auf die FIPS Zertifizierung angewendet werden. Sie sollte entweder unabhängig von der Zertifizierung gestellt oder umformuliert werden. Wir schlagen letzteres vor.

Ein Outsourcing der SSCD und der Signierapplikation in ein Rechenzenter, welches die physischen und organisatorischen Voraussetzungen erfüllen würde, steht im Konflikt zu Art. 2 Bst. b Ziffer 3 ZertES und Art. 59 Bst. a OR und stellt demnach keine Alternative dar.

keyon

V. Alle Formulierungen verlangen, dass der CSP die Einhaltung der Anforderungen sicherstellt.

Art. 8 ZertES legt die Pflichten anerkannter Anbieterinnen von Zertifizierungsdiensten fest. Aus unserer Sicht liegt es nicht in der Verantwortung des CSP, wie die SSCD und die Signaturschlüssel betrieben resp. verwendet werden.

Art. 11 VZertES beschreibt die Sicherheitsvorkehrungen die im Zusammenhang mit der Verwendung der SSCD und den Signierschlüsseln getroffen werden müssen. Art. 11 VZertES erwähnt aber nur die Inhaberin oder den Inhaber eines qualifizierten Zertifikats und nicht den CSP. Die hier gemachten Formulierungen erweitern die Verantwortung der CSP und widersprechen den oben erwähnten Artikeln. Es liegt einzig und alleine in der Verantwortung der Inhaberin oder des Inhabers, wie die SSCD und die Signierschlüssel verwendet werden. Art. 2 Bst. b Ziffer 3 ZertES und Art. 59 Bst. a OR stützen diese Aussage.

Die Formulierungen sollten entsprechend angepasst werden. Eine Erweiterung der Verantwortung der CSP würde sich wahrscheinlich negativ auf die Kosten der Zertifikate und der damit verbundenen Services auswirken.

Kapitel 3.4.2 Bst. c

I. Es sollte eine Aussage gemacht werden, ob die Aufzählungen der X.509 V3 Erweiterungen abschliessend ist oder nicht. Wir empfehlen, dass weitere kritische oder nicht kritische Erweiterungen erlaubt sein sollen.

II. Die qcStatements dürfen nur als ganzes entweder kritisch oder nicht kritisch gesetzt werden. Eine Mischform ist nicht erlaubt. Die hier gemachte Formulierung lässt dies aber offen.

Wir würden uns freuen, wenn unsere Anmerkungen berücksichtigt würden. Bei Fragen stehe ich Ihnen gerne zur Verfügung.

Freundliche Grüsse

Rene Eberhard
CEO