Peter Stadlin
Aabachstrasse 4
CH-6300 Zug
Tel: 041-710 65 81
Mobil: 076-398 11 66

Bundesamt für Kommunikation BAKOM
Postfach
Zukunftstrasse 44
CH- 2501 Biel

6300 Zug, den 11. August 2006

-

Betrifft: Stellungnahme zu Änderungsentwurf der technischen und administrativen Vorschriften SR 943.032.1

Sehr geehrter Herr Jenny

vielen Dank für die Einladung zur Stellungnahme bezüglich dem Änderungsentwurf der technischen und administrativen Vorschriften SR 943.032.1.

Ich bin mit dem Änderungsentwurf einverstanden bis auf folgende 3 Präzisierungen:

2. System für die Anerkennung der CSP

-> im Diagramm "Anerkennungsstelle (CB)" nach "ZertES-Anerkennungsstelle (CB)" umbenennen.

3.3.3 d) Sichere Signaturerstellungseinheiten Absatz 3

Ändern zu:

- Die CSP muss sicherstellen, dass die Signaturerstellungseinheit von der Inhaberin oder vom Inhaber des qualifizierten Zertifikats und unterstützend von entsprechend bevollmächtigten Personen betreiben wird. Das Verfahren der Schlüsselerzeugung muss mit der Spezifikation ETSI TS 101 456 [6], Kapitel 7.2.1 a) Certification authority key generation, konform sein.

Begründung:
Sichere Signaturerstellungseinheiten nach FIPS 140-2 Level 3 (oder höher) verwenden meist Dual Control Verfahren, welche mindestens 2 Personen benötigen. Ein exklusiv-oder Formulierung bezüglich genau einer Person würde ein solches Verfahren nicht ermöglichen.

3.3.3 d) Sichere Signaturerstellungseinheiten Absatz 4

Ändern zu:

- Die CSP muss sicherstellen, dass der Betrieb der Signaturerstellungseinheit unter Umsetzung solcher Kontrollen erfolgt, welche auf der Grundlage des Protection Profile für SSCD Typ3 gemäss dem Dokument CWA 14169:2004 beruhen, diese Anforderungen aber ergänzend zu FIPS 140-2 Level 3 (oder höher) mittels relevanten Regelungen und Massnahmen gemäss der Norm ISO/IEC 27001 Anhang A auf Grund einer dokumentierten Risikoanalyse inkl. Statement of Applicability äquivalent substituieren.

Begründung:
Die Sicherheitsanforderungen sollen nicht schwächer als unter 3.3.3 b) definiert sein. Als Grundlage zur Risikoanalyse und den daraus folgenden Regelungen und Massnahmen soll das Protection Profile (Sicherheitsanforderungsprofil) CWA 14169:2004 [SSCD Typ3] verwendet werden.

ich hoffe, Ihnen mit meinen Ergänzungen einen konstruktiven Beitrag geleistet zu haben und verbleibe,

Mit freundlichen Grüssen

Peter Stadlin