KPMG

Bundesamt für Kommunikation
Herr Christian Jenny
Zukunftstrasse 44
Postfach
2501 Biel

Kontakt: Reto P. Gurbenmann
Tel.: 044 249 25 39

Zürich, 18. August 2006

Änderungsentwurf der technischen und administrativen Vorschriften über Zertifizierungsdienste im Bereich der elektronischen Signatur (SR 943.032.1): Anhörung der betroffenen Kreise

Sehr geehrte Damen und Herren

Wir beziehen uns auf Ihr Schreiben vom 23. Juni 2006, mit dem Sie uns freundlicherweise zur oben genannten Stellungnahme eingeladen haben, sowie auf unser E-Mail vom 9. August 2006. Gerne beantworten wir Ihre Anfrage, ohne jedoch den Anspruch auf Vollständigkeit erheben zu können.

1 Sichere Signaturerstellungseinheiten, Massensignaturen (Ziff. 3.3.3 lit. d TAV ZertES)

Wir unterstützen die Erweiterung der TAV um die Möglichkeit eines Einsatzes einer sicheren, nach FIBS 140-2 Stufe 3 oder höher zertifizierten Signaturerstellungseinheit, um die Generierung von Signaturen im grossen Massstab zu ermöglichen.

Wir erlauben uns dennoch, folgende Punkte anzuführen:

- U.E. sind sowohl Ziff. 3.3.3 lit. a als auch Ziff. 3.3.3 lit. c auf die in lit. b und d geregelten Fälle anwendbar, wobei lit. b und d alternativ zur Anwendung kommen. Diese Systematik erscheint uns im vorliegenden Entwurf nicht ohne weiteres erkennbar zu sein.

- Gemäss Art. 6 Abs. 2 lit. c ZertES obliegt es dem rechtmässigen Inhaber, die Signaturschlüssel vor missbräuchlicher Verwendung verlässlich zu schützen. Voraussetzung dafür ist, dass die Signaturerstellungseinheiten dafür Gewähr leisten (Einleitungssatz Art. 6 Abs. 2 ZertES). Demgegenüber verlangt Ziff. 3.3.3 lit. d TAV

ZertEs neu, dass die CSP selbst die dort genannten Anforderungen sicherstellt. Damit ist u.E. nicht klar, ob und inwieweit die in Art. 6 Abs. 2 lit. c ZertES geregelte Verantwortung der Zertifikatsinhaber für den Schutz vor missbräuchlicher Verwendung der Signaturschlüssel auf der Grundlage von Ziff. 3.3.3 lit. d zumindest teilweise auf die CSP übertragen wird.

Wir würden demnach die Regelung von Ziff. 3.3.3 lit. d TAV ZertES in Ziff. 3.3.3 lit. b TAV ZertES unter Berücksichtigung der oben genannten Bedenken empfehlen. Eine mögliche Neuformulierung von Ziff. 3.3.3 lit. b TAV ZertES könnte demnach wie folgt lauten:

Die Zertifizierung der sicheren Signaturerstellungseinheiten muss für alle oben stehenden Anforderungen erhältlich sein und

i) entweder die Prüfstufe EAL 4 der Norm ISO/IEC 15408:1999 [11] umfassen, erhöht um die Versicherungselemente AVA_MSU.3 (vulnerability assessment, analysis and testing of insecure states) und AVA_VLA.4 (vulnerability assessment, highly resistant),

ii) oder die Prüfstufe E3 hoch des Dokuments ITSEC [14] umfassen,

iii) oder die Prüfstufe FIBS 140-2 level 3 oder höher umfassen; zusätzlich müssen folgende Anforderungen erfüllt sein:

- *Die sichere Signaturerstellungseinheit muss in einer, aufgrund einer Risikoanalyse ausgewählten physisch gesicherten Umgebung, betrieben werden.*
- *Die Signaturerstellungseinheit und der Server, auf dem sich die Signierapplikation befindet, müssen von anderen, nicht mit der Signaturerstellung zusammenhängenden Komponenten logisch getrennt sein.*
- *Die Signaturerstellungseinheit muss von der Inhaberin oder vom Inhaber des qualifizierten Zertifikates oder von einer bevollmächtigten Person betrieben werden.*
- *Der Betrieb der Signaturerstellungseinheit muss unter Umsetzung der Kontrollen erfolgen, die in Anhang A der Norm ISO/IEC 27001 genannt und auf Grund der Risikoanalyse als notwendig betrachtet werden.*
- *Der Zutritt zur physischen gesicherten Umgebung sowie der Zugriff zur Signaturerstellungseinheit muss protokolliert werden.*

2 Datierungssystem - Zeitstempel (Ziff. 3.5 TAV ZertES)

In der ZertES wird nicht der Begriff „Datierungssystem“, sondern „Zeitstempel“ verwendet. Wir schlagen vor, die TAV ZertES dementsprechend zu ändern.

***

Wir danken Ihnen bestens für die Gelegenheit, uns zum Entwurf der technischen und administrativen Vorschriften über Zertifizierungsdienste im Bereich der elektronischen Signatur (SR 943.032.1) äussern zu dürfen. Für Ihre Rückfragen stehen wir Ihnen selbstverständlich gerne zur Verfügung.

Mit freundlichen Grüssen

KPMG Klynveld Peat Marwick Goerdeler SA

Alain Beuchat
Partner

Reto Grubenmann
Senior Manager