Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für
Umwelt, Verkehr, Energie und Kommunikation UVEK

Bundesamt für Kommunikation BAKOM
Abteilung Fernmeldedienste

20.06.2006

Revision der Technischen und administrativen Vorschriften über die Zertifizierungsdienste im Bereich der elektronischen Signatur

Erläuternder Bericht

Die Erfahrungen mit den ersten Anerkennungsverfahren haben gezeigt, dass eine Anpassung oder Präzisierung bestimmter Abschnitte der Technischen und administrativen Vorschriften (TAV) über die Zertifizierungsdienste im Bereich der elektronischen Signatur nötig ist.
Dieses Dokument erläutert die wichtigsten Neuerungen.

Kapitel 1.2: Verweis auf die Spezifikation ETSI TS 101 456
Von nun an wird auf die neue Version der Spezifikation ETSI 101 456, die im Januar 2006 publiziert wurde, verwiesen.
Diese Anpassung hat nur einen geringen Einfluss auf die Anforderungen, die den Anbieterinnen von Zertifizierungsdiensten (CSP) auferlegt werden, da nur Kapitel 7.2.5 angepasst wurde. Demnach kann der Schlüssel der CSP, der für die Generierung von qualifizierten Zertifikaten verwendet wird, auch für das Signieren anderer Arten von Zertifikaten sowie von Informationen über widerrufene Zertifikate (z.B. Liste der für ungültig erklärten Zertifikate) verwendet werden.

Kapitel 1.2: Verweis auf die Spezifikation ETSI TS 101 861
Im Januar 2006 wurde auch von der Spezifikation ETSI TS 101 861 eine neue Version publiziert. Sie weist ebenfalls Anpassungen auf, deren Auswirkungen für die CSP vernachlässigbar sind.

Kapitel 3.2 Buchstaben b und c: Grundsätze für den Betrieb des Datierungssystems
Einige Grundsätze für den Betrieb des Datierungssystems werden hinzugefügt, da Art. 12 ZertES die Bereitstellung eines Zeitstempels vorschreibt.

Kapitel 3.2 Buchstabe c: interne Audits
Zur Präzisierung der Bedeutung des Ausdrucks «interne Audits» wird auf die Norm ISO/IEC 27001 verwiesen.

Kapitel 3.2 Buchstabe f: Prüfung reparierter Ausrüstungen
Die Verpflichtung, jede einzelne Ausrüstung vor ihrer Wiederinbetriebnahme zu prüfen, ist angesichts der Anzahl Ausrüstungen der CSP offensichtlich unverhältnismässig. Deshalb wird präzisiert, dass die Prüfung nur die Wiederinbetriebnahme derjenigen Ausrüstungen betrifft, die gemäss Risikoanalyse für die Sicherheit kritisch sind.
Um die Sicherheit der Ausrüstungen sicherzustellen, wird die Beteiligung von zwei Vertrauens-angestellten nicht nur bei der Wiederinbetriebnahme, sondern auch bei der Konfigurierung der reparierten Komponenten verlangt.

Kapitel 3.2 Buchstabe i: Aktualisierung der Informationen, welche die Wiederaufnahme der Tätigkeiten nach einem Schadensfall ermöglichen
Es wird präzisiert, dass es die aktuellen Informationen sind, die gespeichert werden müssen, damit alle auf den Systemen vorgenommenen Anpassungen, die Auswirkungen auf die Sicherheit haben könnten, berücksichtigt werden.

Kapitel 3.3.3: Einheit für Signaturerstellung im grossen Massstab
Es besteht ein echter Bedarf an im grossen Massstab generierten Signaturen, um die Integrität und Authentizität von Dokumenten zu gewährleisten. Die Verordnung über das Schweizerische Handelsamtsblatt (Verordnung SHAB, SR 221.415) sieht zum Beispiel in Artikel 8 Absatz 2 vor, dass die Signatur der Daten des SHAB auf einem qualifizierten Zertifikat einer anerkannten Anbieterin von Zertifizierungsdiensten im Sinne des ZertES beruhen muss.
Gleichzeitig haben am Markt eher Einheiten in Form von Chipkarten als Einheiten zur Signaturerstellung im grossen Massstab (*Hardware Security Module, HSM*) die Produktzertifizierung gemäss ISO/IEC 15408 (*common criteria*) oder ITSEC (wie in den TAV vorgeschrieben) erlangt. HSM waren dagegen am Markt mit einer Zertifizierung gemäss FIPS-140-2 erhältlich.
Somit sind die TAV anzupassen, damit die Implementierung solcher Lösungen nicht behindert wird. Zur Sicherstellung des Betriebs in einer physisch gesicherten Umgebung sowie der Personalsicherheit des Personals bei der Verwendung von Einheiten des Typs HSM wurde vorgeschlagen, auf die

entsprechenden Kapitel der Spezifikation ETSI TS 101 456 zu verweisen. Diese Spezifikation betrifft aber vor allem die Sicherheit der Infrastruktur der CSP und ist folglich nicht für HSM geeignet, da diese innerhalb der Infrastruktur der Zertifikatsinhaber betrieben werden und die neue Bestimmung diesen Fall abdecken soll. Deshalb wird stattdessen auf die Norm ISO/IEC 27001 verwiesen, welche offen lässt, für welche Organisation sie gilt. Die Wahl der Norm ISO/IEC 27001 ist sicher von Vorteil für diejenigen Zertifikatsinhaber, die bereits ein auf dieser Norm basierendes Sicherheitsmanagement-system umgesetzt haben.
Die neuen Anforderungen in den TAV lassen einen gewissen Spielraum bei der Wahl der geeigneten Sicherheitsmassnahmen auf Grund der Risikoanalyse, was bestimmt sinnvoll ist angesichts der Vielfalt an Varianten, die umgesetzt werden.
Gemäss den neuen Anforderungen muss die CSP sicherstellen, dass der Zertifikatsinhaber beim Betrieb solcher Signaturerstellungseinheiten Massnahmen ergreift, die den Vorschriften in Kapitel 3.3.3 Buchstabe a der TAV entsprechen. Dies ist umso mehr gerechtfertigt, als die CSP die Signaturerstellung im grossen Massstab mit Sicherheit verwirklichen wird.

Kapitel 3.4.1 Buchstabe b: Präzisierung der Informationen, die zu aktualisieren sind
Eine Präzisierung der Informationen, die zu aktualisieren sind, wird in der deutschen Fassung angebracht.

Kapitel 3.4.2 Buchstabe c: Bezeichnung der Erweiterung «qcStatements»
In der Praxis hat sich gezeigt, dass gängige Applikationen bei der Bearbeitung der Erweiterung «qcStatements», die im Zertifikat als kritisch bezeichnet ist, Fehler generieren.
Die Entscheidung, diese Erweiterung als kritisch oder nicht kritisch zu bezeichnen, wird deshalb der CSP überlassen, um solche Fehler zu vermeiden. Die Konformität mit Kapitel 3.2.6 des Dokuments RFC 3739, das keine besondere Bezeichnung verlangt, ist dennoch gewährleistet.

Kapitel 3.5: Inhalt des Datierungszertifikats
Es wurde vorgeschlagen, den Inhalt des Datierungszertifikats in den TAV im Detail anzugeben.
Die TAV sollen aber nicht strengere Regelungen enthalten, als sie im Rechtrahmen und in den genannten Dokumenten vorgesehen sind. Folglich nennen sie nur eine Anforderung des Dokuments RFC 3161. Letzteres Dokument wird in den TAV nicht mehr erwähnt, da es bezüglich des Datierungszertifikats auf das Dokument RFC 2459 verweist, das inzwischen durch das Dokument RFC 3280 ersetzt wurde.