santésuisse
Die Schweizer Krankenversicherer
Römerstrasse 20, Postfach
CH-4502 Solothurn
Tel. 032 625 41 41
Fax 032 625 41 51
mail@santesuisse.ch
www.santesuisse.ch

Bundesamt für Kommunikation
Zukunftstrasse 44
2501 Biel

Für Rückfragen:
Dr. Judith Petermann Büttler
Direktwahl: 032 625 42 68
E-Mail: judith.petermann@santesuisse.ch

Solothurn, 16. Juli 2004

Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur und Technische und administrative Vorschriften.

Sehr geehrte Damen und Herren

Wir danken Ihnen, dass Sie uns die Gelegenheit gegeben haben, zu den oben erwähnten Vorlagen Stellung zu nehmen.

Zur **Verordnung** haben wir folgende Bemerkungen:

Art. 6
Dieser Artikel fordert lediglich, dass die anerkannten Anbieterinnen von Zertifizierungsdienstleistungen keine Kopien der Signaturschlüssel aufbewahren dürfen. Wir empfehlen eine schärfere Formulierung, die sicherstellt, dass der Signaturschlüssel so erzeugt wird, dass das Erstellen einer Kopie nicht möglich ist. Dies scheint aus folgenden Gründen unproblematisch:

1) Die Prüfung der Signatur ist auch nach dem Verlust des Signaturschlüssels mit Hilfe des Zertifikates nach wie vor möglich. Gemachte Signaturen sind weiterhin gültig.
2) Ein Signaturschlüssel kann auf den gleichen Namen durch einen erneuten Registrationsprozess ausgestellt werden. Die daraus entstehenden Aufwände sind vergleichbar mit denen, die sich aus dem Verlust eines Passes ergeben.
3) Ein CSP, der Schlüssel für Kunden generiert, kann dies tun, wenn er nachweisen kann, dass der Produktionsprozess die Erstellung von Kopien verhindert.

Art. 7
Die gewählte Formulierung ist unglücklich, weil der Grund für die Ungültigkeitserklärung der Schlüsselverlust sein kann. In diesem Fall ist eine elektronische Übermittlung nicht möglich. Die Ungültigerklärung auf brieflichem Weg sollte deshalb im Artikel erwähnt und der elektronischen Übermittlung gleichgestellt werden.

Art. 8 Abs. 1
Das Führen eines Verzeichnisdienstes ist optional. Die Revokationslisten (CRL) hingegen muss zwingend online zur Verfügung gestellt werden. Ohne diese Information kann nicht überprüft werden, ob ein qualifiziertes Zertifikat im aktuellen Moment gültig ist oder nicht. Diese Aussage in Art 8 Abs. 1 ist problematisch, weil CRL typischerweise als Teil des Verzeichnisdienstes angeboten werden. Zudem ist der CRL Distribution Point ein Attribut im

Zertifikat (siehe Kapitel 3.4.3.1 der Technische und administrative Vorschriften über Zertifizierungsdienste im Bereich der e-lektronischen Signatur.)

Art. 8 Abs. 2
Die Aufbewahrungsfrist von elf Jahren nach Ablauf der Gültigkeit der Zertifikate ist unnötig lange. Im Sinne einer Harmonisierung der Ablauffristen ist zehn Jahre nach Ablauf der Gültigkeit genügend.

Art. 9
Hier sollte die Formulierung „mindestens zehn Jahre“ lauten. Informationen zur Registrierung von Individuen können unter Umständen bis zu 17 Jahren aufbewahrt werden müssen. Diese Zahl setzt sich wie folgt zusammen: Erstregistration bis Ausstellung letztes Zertifikat = 6 Jahre, Gültigkeit des Zertifikates = 1 Jahr, Aufbewahrung zur Dokumentation gemäss Art. 8 Abs. 2 = 10 Jahre.

Art. 13
Die Forderung, eine Ungültigkeitserklärung innert 24 Stunden auszulösen, erfordert zwingend eine Methode für eine telefonische Ungültigkeitserklärung. Dies ist ein Widerspruch zu Art. 7. Eine Alternative zur gemachten Forderung wäre, eine telefonische Suspendierung zu akzeptieren. Die Identifikation des Berechtigten kann auf der Basis von Daten erfolgen, die während der Registration gesammelt wurden. Eine Suspendierung kann während 30 Tagen rückgängig gemacht werden. Danach gilt das Zertifikat als ungültig erklärt und es muss eine neue Registration erfolgen.

Fehlende Bestimmungen:
Wir erachten es als sinnvoll, die maximale Lebensdauer von persönlichen Zertifikaten auf 13 Monate festzulegen. Damit würde dann auch die maximale Aufbewahrungsdauer für die Dokumentation definiert. Die Zahl 13 Monate resultiert aus dem Bedürfnis, Zertifikate so auszustellen, dass die Gültigkeit per sofort beginnt, der Ablauf aber Ende Monat ausgestellt wird.

Anmerkungen zu "Technische und administrative Vorschriften über Zertifizierungsdienste im Bereich der e-lektronischen Signatur"

Seite 6: Verwaltung des Zertifikatstatus: Hier sollte die Abkürzung OCSP in Klammern aufgeführt werden.

Freundliche Grüsse

santésuisse

Stv. Direktor	Stv. Direktor
Hans Christen	Stefan Kaufmann