

Swisscom AG, Group Legal Services, Alte Tiefenastrasse 6, 3050 Bern

Bundesamt für Kommunikation
Zukunftstrasse 44
2501 Biel

Datum 16. Juli 2004

Ihr Kontakt Kirsten Müller Kellenberger, +41-31-342 51 40

Thema

Stellungnahme der Swisscom AG zur Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur und Technische und administrative Vorschriften

Sehr geehrte Damen und Herren

Wir danken Ihnen für die Gelegenheit, zur genannten Vernehmlassungsvorlage Stellung nehmen zu können, und äussern uns gerne wie folgt:

1. Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur

Artikel 2 Anerkennungsvoraussetzungen

Die vorgesehenen Beträge zur Deckung der Haftung der Anbieterin von Zertifizierungsdiensten scheinen eher hoch angesetzt und könnten damit der Entwicklung des elektronischen Geschäftsverkehrs entgegen wirken. Wir sind daher der Ansicht, dass diese Summen auf ein angemessenes Mass herabzusetzen sind.

Artikel 5 Ausstellung qualifizierter Zertifikate

Absatz 2

Aus der Formulierung des letzten Teilsatzes „...dessen Zertifikat erneuert werden soll.“ lässt sich schliessen, dass ein neues Zertifikat sich auf den gleichen Signaturprüf Schlüssel bezieht, der bis anhin verwendet wurde. Es ist jedoch gängige Praxis, dass bei einer Erneuerung des Zertifikats - nach Ablauf seiner Gültigkeitsdauer - auch das Schlüsselpaar erneuert wird. Dies insbesondere, da die Gültigkeitsdauer per Definition diejenige Zeitperiode bezeichnet, während der mit genügender Gewissheit angenommen werden kann, dass aus dem Signaturprüf Schlüssel – und allenfalls aus den hergestellten Signaturen – der Signaturschlüssel nicht abgeleitet werden kann. Dies bedeutet, dass nach Ablauf der Gültigkeitsdauer diese Sicherheit nicht mehr besteht. Somit ist es im Hinblick auf das Rechtssicherheitsbedürfnis nicht sinnvoll, nach Ablauf der Gültigkeitsdauer ein neues Zertifikat für das gleiche Schlüsselpaar zu erstellen. Aus diesen Gründen schlagen wir folgende Formulierung vor:

„Beantragt eine vor weniger als sechs Jahren gemäss Absatz 1 identifizierte Person ein neues elektronisches Zertifikat, können die anerkannten Anbieterinnen von Zertifizierungsdiensten einen Antrag entgegennehmen, der mit einer elektronischen Signatur versehen ist, die anhand des alten Signaturschlüssels erzeugt wurde. Der Antrag hat vor Ablauf der Gültigkeitsdauer des Zertifikats zu erfolgen.“

Artikel 7 Ungültigerklärung qualifizierter Zertifikate

Verzeichnis für ungültig erklärte qualifizierte Zertifikate

Es fehlen Vorschriften im Zusammenhang mit der Führung von Verzeichnissen für ungültig erklärte Zertifikate. Hierzu gehören u.E. auch Bestimmungen innerhalb welcher Zeit (z.B. 12 Stunden) eine anerkannte Anbieterin die Verzeichnisse nachzuführen hat. Wünschenswert wäre demnach, eine Verpflichtung aufzunehmen, wonach die anerkannten Anbieterinnen die gemäss Absatz 2 aufgelisteten Anforderungen zweimal täglich in solchen Verzeichnissen nachzuführen haben.

Artikel 10 Einstellung der Tätigkeit

Es ist unklar, ob die Regelung beinhaltet, dass noch existierende anerkannte Anbieterinnen für Zertifizierungsdienste in jedem Fall verpflichtet wären, die umschriebenen Pflichten zu übernehmen und ob dies auch dann gelten würde, falls die anerkannte Anbieterin, welche ihrer Geschäftstätigkeit einstellt, in Konkurs fällt und die daraus entstehenden Kosten trotz bestehender Versicherung bzw. Garantie nicht mehr oder nicht mehr vollumfänglich übernehmen könnte (vgl. Art. 13 Zertes). Zudem wäre denkbar, dass die noch existierenden anerkannten Anbieterinnen für die Übernahme diese Pflichten über keine entsprechenden Ressourcen verfügen. Aus diesen Gründen vertreten wir die Ansicht, dass die noch existierenden anerkannten Anbieterinnen die Möglichkeit haben sollten, die Übernahme der erwähnten Pflichten abzulehnen.

Ferner beinhaltet der Artikel, dass die Anerkennungsstelle jederzeit – innert 30 Tagen – bereit sein muss, die erwähnten Pflichten zu übernehmen und dass sie dafür die entsprechenden technischen Gerätschaften bereithalten müsste. Ob diese Regelung letztendlich praktikabel ist, scheint eher unwahrscheinlich.

Artikel 11 Signaturschlüssel

Die Inhaberin oder der Inhaber des Signaturschlüssels, welcher in einer Smart Card oder Token gespeichert werden muss, darf diesen keiner anderen Person anvertrauen. Zudem soll der Signaturschlüssel, soweit zumutbar, auf sich getragen oder weggeschlossen werden.

Diese restriktive Handhabung verhindert de facto die verschlüsselte Speicherung des Signaturschlüssels auf einem Server im Internet sowie das dynamische Herunterladen, Entschlüsseln und den Einsatz des Signaturschlüssels auf diversen Endgeräten und stellt ein Hindernis für die zügige Entwicklung des elektronischen Geschäftsverkehrs dar. Der Vorteil einer solchen Vorgehensweise ist offensichtlich und liegt in der geographischen Mobilität sowie in der Flexibilität bezüglich des Einsatzes verschiedener Endgeräte. Zudem bestehen heute bereits ausreichende technische Möglichkeiten, eine entsprechende Verschlüsselung sicherzustellen. Wir schlagen deshalb vor, die Ausführungsbestimmungen dahingehend mit neuen Sicherheitsanforderungen anzupassen, dass eine solche Verwendung des Signaturschlüssels durch den Inhaber oder die Inhaberin ohne Übernahme von zusätzlichen Haftungsrisiken erfolgen kann.

Artikel 13 Meldung bei Verlust

Absatz 1

Die Relativierung der in Absatz 1 angesetzten Frist in einem separaten Absatz scheint uns unnötig kompliziert und könnte zur Verwirrung Anlass geben. Wir schlagen daher die folgende Formulierung vor:

„Hat die Inhaberin oder der Inhaber den eigenen Signaturschlüssel verloren oder ist dieser abhanden gekommen, muss sie oder er möglichst innerhalb von 24 Stunden ab Kenntnis des Verlustes die Ungültigerklärung des eigenen Zertifikats veranlassen.“

Absatz 3 wäre in diesem Fall zu streichen.

Absatz 2


















Der hier geregelte Sachverhalt lässt sich generell auf einen kompromittierten Schlüssel anwenden. Deshalb schlagen wir die folgende Formulierung vor:

„Das Gleiche gilt für Inhaberinnen oder Inhaber des Signaturschlüssels, die wissen oder den begründeten Verdacht haben, dass ein Dritter Kenntnis des Passworts erlangt hat oder dass der Signaturschlüssel kompromittiert wurde.“

2. Technische und administrative Vorschriften

Aktuelle Zertifizierungspraxis

Die Anforderungen basieren auf europäischen Standards, speziell den ETSI-Standards, oder auf RFCs. Dieser Ansatz ist prinzipiell zu begrüssen, da ein Schweizer Certification Service Provider (CSP) eine Kompatibilität auf der europäischen Ebene anstreben sollte. Gleichzeitig muss jedoch darauf hingewiesen werden, dass der Entwurf sich nur im geringen Masse an praktikable und kommerzielle Randbedingungen hält. So wird zum Beispiel in Deutschland von dem BSI eine Zertifizierung hauptsächlich nicht nach den ETSI-Standards sondern nach dem ITSEC-Standard durchgeführt (siehe zum Beispiel die Zertifizierung BSI-DSZ-ITSEC-0164-2002). Ferner berücksichtigt die Verordnung die Internationale Sicherheitsstandardisierung bzgl. der Common Criteria nicht, die heute massgeblich für viele Evaluationen und Zertifizierungen eingesetzt werden. Wie aus der folgenden Tabelle ersichtlich ist, wurden bereits einige PKIs zertifiziert, ohne dass hierfür die ETSI-Standards als Grundlage genommen wurden.

Produkt Name	Hersteller	Konformität	Datum	CC-Schema
Alacris OCSP Client Professional v4.0.0	Alacris Corporation	EAL 2	Jan 04	
Alacris OCSP Server Professional v3.0.0	Alacris Corporation	EAL 2	Feb 04	
Chrysalis-ITS Lunas@ CA3 V3.97, Software Versions 8.0.8.2.1	Chrysalis-ITS	EAL 4 Augmented ALC_FLR 2	Nov 02	
Entust/Authority from Entust/PKI 5.1	Entust Technologies, Inc.	EAL 3	Feb 01	 
Entust/RA from Entust/PKI 5.1	Entust Technologies, Inc.	EAL 3	Feb 01	 
IBM Directory Server 5.1	IBM Corporation	EAL 2	Aug 03	
Netscape Certificate Management System America Online, Inc. 6.1 Service Pack 1	America Online, Inc.	EAL 4 Augmented ALC_FLR 2	Mar 03	
Passport Certificate Product version 4.1.1	Diversinet	EAL 2 Augmented ADV_SPM 1	May 02	
RSA Keon CA System, V6.5	RSA Security	EAL 4 Augmented ALC_FLR 2	Dec 02	
SecureNet TrustedNet Connect, V 2.0	SecureNet Limited	EAL 4	May 03	 
TimeStamp Server Version: 2.0.2 Patch 1	Baltimore Technologies Pky Limited	EAL 3	May 03	 
UNCERT TimeStamp Server Version 2.0.2	Baltimore Technologies	EAL 3	May 03	 

Eine Verordnung, die fast ausschliesslich auf den ETSI-Standards basiert, würde daher International anerkannte Zertifizierungen ausschliessen und die kommerziellen Betreiber in der Schweiz dazu zwingen, eine erneute Zertifizierung durchzuführen. Ferner möchten wir darauf hinweisen, dass ETSI als Standardisierungsorganisation hauptsächlich Standards für Telekom-Anbieter definiert. Der Entwurf sollte sich aber mehr auf ein kommerzielles oder administratives IT-Umfeld als auf ein typisches Telekom-Umfeld beziehen, da dies den Gegebenheiten im Markt besser gerecht wird.

Spezifikation der Verfahren

Weder der Entwurf noch die referenzierten Textstellen der internationalen Normen spezifizieren die Vorgaben für Verfahren, Algorithmen oder Schlüsselstärke. Dies ermöglicht dem CSP Algorithmen und Schlüsselstärke selber zu definieren und im Laufe der Zeit der aktuellen Technik anzupassen. Dies hatten wir für problematisch, da ein Zertifikat mit einem hohen Modul für eine entsprechende Gültigkeitsperiode sicherlich eine andere Qualität besitzt als ein Zertifikat, dessen Generierung auf einem niedrigen Modul basiert. Zudem werden neueste Entwicklungen in der Sicherheitsbranche nicht berücksichtigt. Mit dem heutigen Entwurf ist es sogar möglich, Modulgrössen zu verwenden, die gebrochen werden können. Wir empfehlen daher, in einem Anhang zum Entwurf die Verfahren (RSA, El Gamal, Elliptische Kurven, NTRU)

und Modulgrössen näher zu spezifizieren und diese aufgrund der Entwicklungen immer wieder, wenn notwendig, im Anhang zu modifizieren. Konkret sollte pro in der Praxis gängigem Signaturalgorithmus eine minimale Schlüssellänge für die Schlüssel der Anbieterin sowie der Schlüsselhaber gefordert werden, z.B. für RSA jeweils mind. 1024 bit. Ausserdem sollte pro in der Praxis gängigem Signaturalgorithmus eine maximale Gültigkeitsdauer der Zertifikate gefordert werden, z.B. für RSA jeweils max. 5 Jahre.

Generierung der Zertifikate

Es ist zu begrüssen, dass der CPS das Schlüsselpaar für qualifizierte Zertifikate im Auftrag des Antragstellers selber in einer sicheren Umgebung generieren und danach das Schlüsselpaar auf eine Secure-creation device (SSCD) speichern kann. Dieses Vorgehen kann betriebliche Vorteile bieten. Es ermöglicht dem CPS die Mengen-Produktion von Zertifikaten. Im Weiteren ist ein Verfahren zur Erstellen der Zertifikate möglich, das keine Interaktion mit dem Endbenutzer erfordert. Zudem wird sichergestellt, dass die Zertifikate bzw. Schlüssel bei einer zentralisierten Lösung immer unter Einhaltung eines hohen Sicherheitsstandards abgespeichert werden, was bei lokalen Lösungen wie Chipkarten nicht immer der Fall ist.

Kapitel 6.2 ETSI Norm

In den Ausführungsvorschriften fehlt ein Verweis auf das Kapitel 6.2 der ETSI Norm [6]. Ein entsprechender Verweis sollte jedoch nach Möglichkeit eingefügt werden, da ansonsten die Bestimmungen lückenhaft sind. Ist dies nicht möglich, sollte in Ziffer 3.4.1 der Absatz 7.3.1 h) in der dort referenzierten Norm [6] gestrichen werden, da dieser sich auf das erwähnte Kapitel 6.2 in [6] bezieht.

Ziffer 3.2.1 b) Organisation

Es wäre begrüssenswert, festzuhalten, dass die Ergebnisse der internen Audits dem Tätigkeitsjournal beizufügen und entsprechend aufzubewahren sind.

Ziffer 3.2.2 Verwaltung der Politik

Im zweiten Absatz ist „Aussage der Zertifizierungspraxis (CPS)“ durch „Aussage über die Zertifizierungspraxis (CPS)“ zu ersetzen.

Ziffer 3.4.3.1 Felder des Zertifikats

Feld: „subjectAltName“: Das Attribut "subjectAltName" sollte gemäss dem RFC 3280 Kapitel 4.2.1.7 erstellt werden.

Feld: "issuerAltName": Es fehlt ein Feld, das den expliziten Text mit der Angabe enthält, dass die Anbieterin anerkannt ist. Nach Möglichkeit sollte ein solches Feld eingefügt werden, z.B. als Attribut "QCStatements". Zudem wäre es wünschenswert nicht die Abkürzungen EA und SAS zu verwenden, sondern diese Wörter voll aus zu schreiben.

Feld: "keyUsage": Hier wäre es sinnvoll, nicht nur Bit Nr. 1 zu setzen, sondern alle anderen auf Null zu setzen, mit Ausnahme derer, die nötig sind, damit mit dem Zertifikat auch ein Login bzw. eine Authentifikation durchgeführt werden kann (z.B. SSL Client Authentifikation oder Windows Logon). Ein qualifiziertes Zertifikat sollte auch für Logins benützt werden können.

Feld: "QCStatements / Wert der Transaktion": Wert: "Der Maximalwert der Transaktion sind in der...." Ist durch „Der Maximalwert der Transaktion ist in der...“ zu ersetzen.

Feld: "QCStatements / Präzisierung des Zertifikats": Der Wert wird nicht in Form des OID angegeben, sondern ergibt sich aus dem INTEGER und dem EXPONENT gemäss RFC. Deshalb sollte „... Kapitel 3.2.6, in Form eines Objektbezeichners...“ durch „... Kapitel 3.2.6, unter Verwendung eines Objektbezeichners...“ ersetzt werden.

3. **Generelle Bemerkungen.**

Wir messen der internationalen Verwendung elektronischer Signaturen und deren rechtlicher Anerkennung hohen Stellenwert bei, da dies der Entwicklung eines intensiveren elektronischen Handels über die Grenzen hinweg förderlich ist. Daher wäre es begrüssenswert, wenn der Bundesrat die internationale Verwendung und Anerkennung elektronischer Signaturen gemäss Art. 19 Zertes baldmöglichst anstrebt. Zudem erachten wir es als sinnvoll und richtig, sich stark an die europäischen Vorschriften anzulehnen.

Generell lässt sich sagen, dass die Verordnung recht knapp gehalten ist und damit dem Bundesamt ein grosser Spielraum überlassen wird. Unseres Erachtens wäre es begrüssenswert, weitere Angaben auf Verordnungsstufe zu regeln.

In der Vorlage werden praktisch keine Anforderungen an Registrierungsstellen gemacht. Wir schlagen daher vor, die Anforderungen bzw. Aufgaben der Registrierungsstellen gemäss Art. 8 Abs. 4 Zertes in der vorliegenden Vorlage auszuführen und zu präzisieren.

Wir danken Ihnen bestens für die Berücksichtigung unserer Anliegen und stehen für allfällige Rückfragen oder ergänzende Auskünfte gerne zur Verfügung.

Mit freundlichen Grüssen

Swisscom AG
Group Legal Services



Rolf Zaugg, Fürsprecher
Senior Counsel



Kirsten Müller Kellenberger, Fürsprecherin
Legal Counsel