SIK/CSI

Petersgraben 52 Postfach 4003 Basel Schweiz
Telefon: +41 (0)61 267 6065 Telefax: +41 (0)61 267 9860

E-Mail: Urs.Jermann@sik.admin.ch
Intranet: www.sik.admin.ch (IP:172.30.80.7)

Schweizerische Informatikkonferenz

Conférence suisse sur l'informatique

Conferenza svizzera sull'informatica

Bundesamt für Kommunikation
Zukunftstrasse 44
2501 Biel - Bienne

Basel, 19. Juli 2004

Stellungnahme der Schweizerischen Informatikkonferenz zur Konsultation der Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur und technische und administrative Vorschriften.

Sehr geehrte Damen und Herren

Die Schweizerische Informatikkonferenz (SIK) ist eine Organisation des Bundes, der Kantone, der Gemeinden und des Fürstentum Liechtenstein zur Förderung der Zusammenarbeit zwischen den Staatsebenen im ICT-Bereich.

Wir danken Ihnen für die Möglichkeit zur Stellungnahme. Gerne nehmen wir zu den Entwürfen der oben erwähnten Verordnung und Vorschriften wie folgt Stellung:

Allgemein:

- Wir sind mit den Entwürfen grundsätzlich einverstanden und begrüssen die Inkraftsetzung der Verordnung und der dazugehörigen Vorschriften.

- Wir unterstützen die Verweise auf die internationalen Standards in diesem Bereich. Es ist jedoch schwierig, eine mögliche gegenseitige Beeinflussung bei Erweiterungen resp. Anpassungen der einzelnen Standards zu erkennen. Eine Abhängigkeit zu diesen Normeninstitutionen scheint beim Einsatz der qualifizierten Signatur – so wie ihr Einsatz geplant ist – gegeben. Zusätzlich sollten die erwähnten Standards auf der BAKOM-Homepage veröffentlicht werden.

- Wir begrüssen, wenn der Bundesrat baldmöglichst klare Aussagen macht, ob der Bund gewillt ist, eigene Lösungen für den Bürger zu fördern (Ankündigung der elektronischen Identitätskarte, eID) oder voraussetzt, dass Unternehmen in der Schweiz diese Aufgabe wahrnehmen und voran treiben.

Verordnung:

- Artikel 1, Absatz 2

  Die Verordnung beauftragt die Schweizerische Akkreditierungsstelle (SAS) zusätzlich, die Aufgabe der Anerkennungsfunktion zu übernehmen, sofern keine akkreditierte Anerkennungsstelle vorhanden ist.

  Um eine Gewaltentrennung zu garantieren, sollte in diesem Falle ein anderes Organ oder Behörde als die SAS mit der Anerkennungsfunktion beauftragt werden.

- Artikel 2, Absatz 2

  Die Verordnung erlaubt einer Anbieterin von Zertifizierungsdiensten (CSP), die eine Anerkennung anstrebt, eine gleichwertige Finanzgarantie vorzulegen anstatt einer Versicherung von 10 Millionen Franken pro Versicherungsjahr abzuschliessen.

  Unsere Mitglieder unterstützen diese Möglichkeit mit Nachdruck. Die öffentlichen Körperschaften zeihen es in dieser Zeit der knappen Mittel vor, eine Garantie vorzulegen als eine Versicherung abzuschliessen.

- Artikel 7, Absatz 3

  Die anerkannten Anbieterinnen sind verpflichtet, Dritten mindestens bis zum Ablauf der Gültigkeit des Zertifikats den Online-Zugang zu den verlangten Informationen zu gewähren.

  Die Überprüfung des Zertifikats sollte auch nach Ablauf der Gültigkeit noch online möglich sein. Wir schlagen vor, dass die Informationen bis zum Ablauf + n Jahre online zur Verfügung gestellt werden müssen.

- Artikel 10, Absatz 1

  Die anerkannten Anbieterinnen von Zertifizierungsdiensten melden der SAS die Aufgabe ihrer Geschäftstätigkeit 30 Tage im Voraus.

  Wir bezweifeln, dass die Frist von 30 Tagen in der Praxis genügt, um den Transfer der Tätigkeiten zu einer anderen anerkannten Anbieterin zu gewährleisten.

- Artikel 12, Absatz 1

  Passwörter, die Zugang zum Signaturschlüssel verschaffen, müssen eine Länge von mindestens vier Zeichen aufweisen.

  Vier Zeichen sind für ein sicheres Passwort zu kurz. Wir schlagen eine Länge von mindestens sechs Zeichen (Zahlen und Buchstaben) vor.

Fragen und Bemerkungen zu den dazugehörigen Vorschriften

Durch eine Revokation kann ein Zertifikat vor Ablauf der Gültigkeitsdauer ausser Kraft gesetzt werden.

- Ist mit Kapitel 3.2.12. "Tätigkeitsjournal" und Kapitel 3.5 "Zeitstempel" sichergestellt, dass auch Tage oder Wochen im Nachhinein zweifelsfrei überprüft werden kann, ob eine Transaktion mit einem gültigen Zertifikat ausgeführt wurde?

- Sind CSP und e-Business Anwender zu einer Zusammenarbeit im Bereich der IT Sicherheit verpflichtet (z.B. im Bereich Nachvollziehbarkeit, Nicht-Abstreitbarkeit)?

- Es stellt sich die Frage, warum im Rahmen der ZertES beim Zertifikatsprofil gegenüber den geltenden Spezifikationen (ETSI-Standards) Besonderheiten eingeführt werden. Wie steht es somit mit der Interoperabilität (Kapitel 3.4.1 Format der Zertifikate)?

- Der Unterschied der Definition der "qualifizierten elektronischen Signatur" und der "fortgeschrittenen elektronischen Signatur" ist aus unserer Sicht zu wenig transparent erklärt.

Wegen der kurzen Zeit für die Stellungnahme hatte die Fachstelle der SIK nur die Möglichkeit eine Umfrage bei ihren Mitgliedern durch zu führen und deren Ergebnisse als Basis für die Stellungnahme zu verwenden. Auf eine nachträgliche Bereinigung durch den Vorstand und der Arbeitskonferenz mussten wir verzichten.

Wir sehen der Inkraftsetzung der Verordnung und der dazugehörigen Vorschriften mit Zuversicht entgegen und hoffen, Ihnen geholfen zu haben.

Mit freundlichen Grüssen

Schweizerische Informatikkonferenz

Felix Albrecht
Vorstandsmitglied

Urs Jermann
Fachstelle

cc:
- Vorstand der SIK
- Delegierte und Beobachter der SIK
- Lenkender Ausschuss "Telekommunikation"