Vernehmlassungantwort

zum Entwurf des

Bundesgesetzes über die elektronische Signatur (BGES)

der

Swiss Internet User Group (SIUG)

http://www.siug.ch/

Mitte April 2001

Art. 1

Wir begrüssen den Zweck des Artikels, die elektronische Signatur gesetzlich zu regeln und somit einer weiteren Verbreitung zuzuführen.

Art. 4 Abs. 1

Es ist wie vorgeschlagen äusserst wichtig, dass die Anbieterinnen von Zertifizierungsdiensten "zuverlässige Informatiksysteme und -produkte verwenden". Allerdings stellt sich hier die Frage, ob der Begriff "zuverlässig" nicht klar definiert werden sollte. Die immer wiederkehrenden Pressemeldungen über Computerviren und -würmer (z.B. ILOVEYOU-Virus) und die damit verbundenen Schäden an Computern tragen in der Bevölkerung kaum zu einem Gefühl des Vertrauens in die Informationstechnologien bei.

Gerade bei der heute am weitesten verbreitete Klasse von Microsoft Windows Betriebssystemen sind erhebliche Sicherheitslücken bekannt, sodass die verlangte Zuverlässigkeit kaum erfüllet wird. Zudem zeichnet sich gerade diese Klasse von Betriebssystemen (aber nicht nur diese) durch ihren nicht verfügbaren Quellcode aus, was auch im Hinblick auf die Generierung kryptographischer Schlüssel (siehe unten) problematisch ist. Falls die Schlüssel nämlich von den Zertifizierungsstellen selbst erstellt werden (was unserer Ansicht nach nicht zweckmässig ist, siehe unten), so kann nicht sichergestellt werden, was mit den neu erstellten Schlüsseln genau passiert. Dies wäre aber für sichere Schlüssel unbedingt notwendig.

Art. 7 Abs. 1

Es sollte hier festgehalten werden, dass kryptografische Schlüssel nur dann sicher sind, wenn sie durch den zugehörigen Besitzer selbst erzeugt wurden. Würden die Anbieterinnen von Zertifizierungsdiensten die Schlüssel zuerst selbst generieren und anschliessend gleich zertifizieren, so müssten die Schlüsselbesitzer den Schlüsselerzeugern und deren kompletten Softwaresystemen dahingehend vertrauen, dass die privaten Schlüssel nicht vor der Herausgabe in ein zusätzliches Archiv kopiert würden. Um ein grösstmögliches Vertrauen in persönliche, rechtsgültige elektronische Unterschriften zu gewährleisten, müssten die Schlüssel zwingend durch die Inhaber selber generiert werden können. Würden die erzeugten privaten Schlüssel vor der Herausgabe noch kopiert, wäre elektronische Unterschriftenfälschung ein leichtes. Dies wäre insbesondere deshalb problematisch, weil in Art. 17 die Beweispflicht für einen Schlüsselmissbrauch beim Schlüsselinhaber liegt. Wohl wird das Kopieren der privaten Schlüssel durch die Anbieterinnen von Zertifizierungsdiensten in Art. 16 verboten. Dennoch kann das in elektronischen Datenverarbeitungsanlagen leicht unbemerkt geschehen. Nur wenn die Schlüssel von den Besitzern selbst erzeugt werden, kann dieses Risiko zuverlässig umgangen werden.

Art. 11 Abs. 2

Die Ungültigkeitserklärung eines elektronischen Zertifikats muss unbedingt auch auf die selbe Art und Weise erfolgen können wie die ursprüngliche Ausstellung des elektronischen Zertifikats und nicht nur mittels einer elektronischen Unterschrift. Ansonsten könnte es passieren, dass ein (möglicherweise unwissentlich) gestohlener privater Schlüssel nicht mehr für ungültig erklärt werden könnte.

Zur Erklärung mag folgendes konstruiertes Beispiel dienen: Ein Signaturschlüsselinhaber hat seinen privaten Signaturschlüssel auf seinem Computer im Arbeitszimmer und zudem auf einer Backup-CD im Elternschlafzimmer gespeichert. Während der Ferienabwesenheit der Familie brennt das Haus und mit ihm alle Kopien des privaten Schlüssels nieder. Im Nachhinein könnte aber nicht sicher garantiert werden, dass der Schlüssel nicht vor dem Abbrennen des Hauses noch durch einen Einbrecher gestohlen wurde. Somit müsste der Signaturschlüssel unverzüglich für ungültig erklärt werden, was aber mangels Kopie zur digitalen Unterzeichnung der Ungültigkeitserklärung nicht mehr möglich wäre.

Eine Streichung des zweiten Satzes von Abs. 2 könnte das Problem lösen.

Art. 14

Hier sollte explizit festgehalten werden, dass die Weitergabe der Daten nicht erlaubt ist. Die Weitergabe der E-Mail-Adresse kann für den Schlüsselinhaber beispielsweise sehr unangenehme Folgen haben (Überhäufung mit unverlangter elektronischer Werbung (Spam)).

Art. 16 Abs. 1

Das Verbot des Kopierens privater Signaturschlüssel ist zwar an sich gut, reicht aber nicht aus (siehe oben, Kommentare zu Art. 7 Abs. 1).

Art. 16 Abs. 2

Angesichts der bekannten Mängel einiger kommerziell erfolgreicher Betriebssysteme müsste spezifiziert werden, was unter der Formulierung "nach den Umständen zumutbare Vorkehrungen" genau zu verstehen ist. Schliesslich besticht auch hier das eindeutig am meisten verbreitete Anwender-Betriebssystem Windows nicht durch eine gute Sicherheit, zumal für den durchschnittlichen Anwender die sichere Konfiguration irgend eines beliebigen Betriebssystems keine leichte (zumutbare?) Aufgabe ist.

Art. 17

Es ist problematisch, dem Schlüsselinhaber alle Folgen einer ungültigen (d.h. ohne seinen Willen erfolgten) Unterschrift aufzulasten. Dies inbesondere auch deshalb, weil sich der elektronische Diebstahl eines privaten Schlüssels durch eine Privatperson nur schwer belegen lässt (siehe auch Kommentare zu Art. 4 und Art. 16). Es ist sicher richtig, die Anwender von Signaturschlüsseln zu einem sehr vorsichtigen Umgang mit ihren privaten Schlüsseln anzuhalten. In diesem Sinne sind die zumutbaren Vorkehrungen von Art. 16 genauer zu spezifizieren. Dies allein kann aber nicht genügen: Vertrauen in die Sicherheit der elektronischen Signatur kann nur hergestellt werden, wenn auf einer Selbsterzeugung der privaten Schlüssel durch die Schlüsselinhaber bestanden wird.

Swiss Internet User Group (SIUG)
Zürich, den 20. April 2001