SwissBanking

Herr
Peter **Fischer**
Stellvertretender Direktor
Bundesamt für Kommunikation
Zukunftsstrasse 44
P.O. Box
2501 **Biel**

Basel, 12. Juli 2004
MTI/A.61.7

**Entwurf der Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur (VZertES) / Vernehmlassungsverfahren**

Sehr geehrter Herr Fischer

Mit Schreiben vom 1. Juni 2004 haben Sie den Entwurf der Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur (VZertES) den interessierten Kreisen zur Vernehmlassung unterbreitet. Für die Gelegenheit, hierzu aus der Sicht der Finanzwirtschaft Stellung zu nehmen, danken wir Ihnen.

Als besonders wichtig erachten wir die Bestimmungen, die das Sicherheitsumfeld beim Schlüsselinhaber beschreiben.

Unsere Hauptanliegen sind, kurz gefasst, folgende:

- **In den vorgelegten Dokumenten sind das Speicherungsmedium des Signaturschlüssels sowie die Umgebung, in der die Signatur erstellt wird (Hardware/Smart Card vs. Software) nirgends geregelt. Davon ausgehend, dass der Schlüsselinhaber in der Regel keine Wahlmöglichkeit besitzt (technisch bedingt) bzw. besitzen darf, womit die Verantwortung dafür zwangsläufig beim Anbieter von Zertifizierungsdiensten liegt, ist in der Verordnung bzw. den technischen und administrativen Vorschriften eine entsprechende Regelung einzufügen.**

- **Die Verordnung sollte zusätzlich festhalten, dass der Inhaber des Signaturschlüssels die für ihn zumutbaren Vorkehrungen zu treffen hat, um den Signaturschlüssel möglichst geheim zu halten. Ebenso muss er verpflichtet sein, diejenige Sorgfalt walten zu lassen bzw. Vorkehrungen zu treffen, die ihm der Anbieter von Zertifizierungsdiensten überbindet.**

- **Die vorgesehene Passwortlänge ist zu kurz. In der Praxis der Finanzbranche wird regelmässig eine Länge von 6-8 Stellen (Tendenz steigend) verlangt. Für eine ausreichende Passwortlänge und eine angemessene Passwortwahl**

• Schweizerische Bankiervereinigung
Association suisse des banquiers
Associazione Svizzera dei Banchieri
Swiss Bankers Association

Aeschenplatz 7
Postfach 4182
CH-4002 Basel

T +41 61 295 93 93
F +41 61 272 53 82
office@sba.ch
www.swissbanking.org

**müsste die Verordnung auf entsprechende Detailspezifikationen durch das BAKOM verweisen.**

- **Der Passwortschutz ist derart auszugestalten, dass bei mehrmaliger Falscheingabe (3-6 mal) der Zugang zur Signierfunktion (und damit auch zum Signaturschlüssel) sich automatisch und endgültig sperrt.**

Wir haben unsere Stellungnahme nachfolgend wie folgt strukturiert:



## I. Grundsätzliche Bemerkungen zur Verordnung

- In den vorgelegten Dokumenten sind das Speicherungsmedium des Signaturschlüssels sowie das Sicherheitsumfeld beim Schlüsselinhaber, in dem die Signatur erstellt wird (Hardware/Smart Card vs. Software) nirgends geregelt. Idealerweise werden deshalb Hard Tokens (Smart Cards) als Signaturerstellungseinheit vorausgesetzt, welche (i) den privaten Schlüssel nie gegenüber der Signaturanwendungsumgebung exponieren, (ii) für jede einzelne Verwendung der Signierfunktion eine auf Passwort oder Biometriedaten basierende Freischaltung erfordern (mit beschränkter Anzahl Freischaltfehlversuchen) und (iii) die missbräuchliche Verwendung des Passwortes, der Biometriedaten und der Signierfunktion zum Unterschreiben einer gefälschten Meldung durch die Identifizierung einer ausreichend sicheren Anwendungsumgebung sicherstellen. Davon ausgehend, dass der Schlüsselinhaber in der Regel keine Wahlmöglichkeit besitzt (technisch bedingt) bzw. besitzen darf, womit die Verantwortung dafür zwangsläufig beim Anbieter von Zertifizierungsdiensten liegt, ist in der Verordnung bzw. den technischen und administrativen Vorschriften eine entsprechende Regelung einzufügen (siehe hierzu das Bundesgesetz über die elektronische Signatur, ZertES Art. 6). Ohne eine klare Beschreibung dieser Komponente wird die Lösung bei den potenziellen Schlüsselinhabern sowie in der Wirtschaft keine Akzeptanz finden, denn diese müssten letztendlich ein Risiko tragen, das sie selber nicht wirklich einschätzen könnten.

  Nämliches gilt wohl auch für die Frage, ob die Signierfunktion durch ein entsprechendes Passwort geschützt ist oder nicht. Dies scheint in den vorliegenden Entwürfen auch nirgends explizit vorgesehen zu sein; vielmehr taucht plötzlich der Umgang mit Passwörtern in Art. 12 der VZertES auf, ohne den Hinweis freilich, dass die Signierfunktion immer durch ein geeignetes Passwort geschützt sein müsse.

  Der Passwortschutz wäre derart auszugestalten, dass bei mehrmaliger Falscheingabe (3-6 mal) der Zugang zur Signierfunktion (und damit auch zum Signatur-

schlüssel) sich automatisch und endgültig sperrt. Zertifikate, die nicht auch diesen Anforderungen genügen, werden auf dem Markt bzw.in der Praxis kaum Chancen auf Akzeptanz haben.

Sodann erachten wir es aufgrund von Art. 6 Abs. 2 lit. a des Bundesgesetzes über die elektronische Signatur (ZertES) als unumgänglich, zwischen Signaturschlüssel und Signierfunktion zu differenzieren.

- Die Aufteilung der Sicherheitsthemen auf mehrere Dokumentebenen: ZertES, VZertES, BAKOM Vorschriften und ETSI Standards, erachten wir als zu unübersichtlich.

- Die Anlehnung an die entsprechenden ETSI Standards begrüssen wir sehr. Dabei setzen wir voraus, dass die referenzierten ETSI Standards vom BAKOM sorgfältig auf Widersprüche zur CH-Gesetzgebung geprüft wurden. Eine solche Prüfung ist unserem Verständnis nach nicht Bestandteil dieser Vernehmlassung. Aus diesem Grund beschränkt sich unsere Stellungnahme auf die beiden Dokumente VZertES und BAKOM Vorschriften, ohne detaillierte Prüfung der ETSI Standard Inhalte.

## II. Bemerkungen zu den einzelnen Bestimmungen der Verordnung

### *2. Abschnitt, Art. 1 Abs. 1*

Die Aussage über genügende Schlüssellänge und anerkannte Algorithmen ist ohne eine detailliertere Spezifikation ungenügend (siehe: Draft ETSI TS 102 XXX V.0.0.1, Electronic Signatures and Infrastructures [ESI]; Algorithms and parameters for Electronic Signatures).

### *4. Abschnitt, Art. 5 Abs. 2*

Bei Zertifikaten mit spezifischen Attributen (die sich kurzfristig ändern mögen) ist eine Prüfung dieser Attribute bei jeder Zertifikatsausstellung erforderlich.

### *4. Abschnitt, Art .7 Abs. 1*

Diese Bestimmung betrachten wir als fragwürdig, wenn sie abschliessend bzw. zwingend gemeint ist. Denn beim Verlust des Schlüssels bzw. vergessenem Passwort könnte dann nicht mehr signiert und auch nicht mehr gesperrt werden. Allenfalls sollte man dies ergänzen durch folgende Präzisierung:

> *"Sperrungen können auch bei entsprechender Legitimierung via Pass oder ID bei der entsprechenden Registrierungsstelle ausgelöst werden."*

***5. Abschnitt, Art. 11***

Die Aussagen sind stark von der Signaturerstellungseinheit und der Signaturanwendungsumgebung abhängig. Unter idealen Voraussetzungen wären durch den Inhaber primär das Hard Token und das Passwort zu schützen (Art 11). Für eine ausreichende Passwortlänge und eine angemessene Passwortwahl müsste die Verordnung, wie im 2. Abschnitt, auf entsprechende Detailspezifikationen durch das BAKOM verweisen.

Hier sollte zusätzlich festgehalten werden, dass der Inhaber des Signaturschlüssels diesen nicht nur wegzuschliessen (und zwar *sicher*), sondern auch die für ihn zumutbaren Vorkehrungen zu treffen hat, um den Signaturschlüssel möglichst *geheim zu halten*. Ebenso muss er verpflichtet sein, diejenige Sorgfalt walten zu lassen bzw. *Vorkehrungen zu treffen, die ihm der Anbieter* von Zertifizierungsdiensten *überbindet*.

**Art. 11 könnte somit wie folgt lauten:**
(Mit Grossbuchstaben werden die neuen Textstellen gekennzeichnet.)

> *"(1) DER ZUGRIFF AUF DIE SIGNIERFUNKTION MUSS DURCH EIN GEEIGNETES PASSWORT GESCHÜTZT SEIN.*
>
> *(2) Die Inhaberin oder der Inhaber des Signaturschlüssels darf diesen keiner anderen Person anvertrauen.*
>
> *(3) DIE INHABERIN ODER DER INHABER HAT ALLE NACH DEN UMSTÄNDEN ZUMUTBAREN VORKEHRUNGEN ZU TREFFEN, UM DEN MISSBRAUCH DES SIGNATURSCHLÜSSELS ZU VERHINDERN. Sie oder er muss den Signaturschlüssel, soweit zumutbar, auf sich tragen oder diesen SICHER wegschliessen.*
>
> *(4) DIE VOM ANBIETER VON ZERTIFIZIERUGSDIENSTEN ÜBERBUNDENEN SORGFALTSPFLICHTEN UND VERHALTENSWEISEN IM UMGANG MIT DEM SIGNATURSCHLÜSSEL UND DEM PASSWORT SIND VON DER INHABERIN ODER DEM INHABER EINZUHALTEN."*

***5. Abschnitt, Art. 12***

Abs. 1: Die vorgesehene Passwortlänge ist zu kurz. In der Praxis der Finanzbranche wird regelmässig eine Länge von 6-8 Stellen (Tendenz steigend) verlangt. Dabei ist auf deutsche Urteile zu verweisen, wo festgehalten wurde, laut Gutachten sei ein 4-stelliger Code knackbar. Zudem muss unseres Erachtens klargestellt werden, dass das Passwort aus *verschiedenen* Zeichen zu bestehen hat (Zahlen, Buchstaben oder Sonderzeichen). Ebenso erforderlich ist eine Einschränkung der Freischaltfehlversuche.

Abs. 2: Was ist unter "persönlichen Daten" zu verstehen? Diese Daten dürfen unseres Erachtens auch nicht aus dem Kreise von Bekannten und Verwandten stammen. Sowohl das eine wie das andere sollte mindestens in den Erläuterungen präzisiert wer-

den, verbunden mit dem Hinweis, dass es sich beim Passwort auch *nicht* um eine *leicht ermittelbare* Zahlen-/ Buchstabenkombination oder um Wörter aus dem Lexikon handeln darf.

Abs. 3: Hier würden wir von "SEPARATEM Verschluss" sprechen und auf Abs. 5 verweisen.

Abs. 5: Hier würden wir von "*getrennt voneinander und SICHER aufzubewahren*" sprechen.

Ergänzende Regelung:
Weiss oder vermutet der Inhaber, dass das Passwort einem Dritten bekannt geworden ist, hat er dieses *umgehend zu ändern*.

**Art. 12 könnte somit wie folgt lauten:**
(Mit Grossbuchstaben werden die neuen Textstellen gekennzeichnet.)

> *"(1) Passwörter, die DEN ZUGRIFF AUF DIE SIGNIERFUNKTION ERMÖGLICHEN, müssen eine Länge von mindesten 6-8 VERSCHIEDENEN Zeichen (Zahlen, Buchstaben ODER SONDERZEICHEN) aufweisen.*
>
> *(2) Das Passwort darf NICHT AUS EINER LEICHT ERMITTELBAREN ZAHLEN-/BUCHSTABENKOMBINATION BESTEHEN UND sich INSBESONDERE nicht auf Daten AUS DEM PERSOENLICHEN UMFELD der Inhaberin oder des Inhabers des Signaturschlüssels beziehen.*
>
> *(3) Zeichnet die Inhaberin oder der Inhaber das Passwort auf, so muss sie oder er auch diese Aufzeichnung unter SEPARATEM Verschluss halten (Abs. 5).*
>
> *(4) Auf einen Passwortschutz kann verzichtet werden, wenn geeignete biometrische Verfahren garantieren, dass DIE SIGNIERFUNKTION nur von der Inhaberin oder vom Inhaber verwendet wird.*
>
> *(5) Der Signaturschlüssel und die Passwörter sind getrennt voneinander SICHER aufzubewahren.*
>
> *(6) WEISS ODER VERMUTET DIE INHABERIN ODER DER INHABER, DASS DAS PASSWORT EINEM DRITTEN BEKANNT GEWORDEN IST, HAT ER DIESES UMGEHEND ZU ÄNDERN."*

***5. Abschnitt, Art. 13***

Abs. 1: Nicht nur der Verlust oder das Abhandenkommen, sondern auch der Fall, dass der Inhaber des Signaturschlüssels weiss oder den dringenden Verdacht hat, dass ein *Dritter Kenntnis* vom Signaturschlüssel erhalten hat, muss den Inhaber zur Meldung

bzw. Sperre zwingen. 24 Stunden dürften zu lange sein; muss nicht *umgehend* gehandelt werden?

Müsste nicht auch festgehalten werden, dass der Inhaber bis zum Zeitpunkt der Meldung, zuzüglich Bearbeitungszeit, für den allfälligen missbräuchlichen Einsatz des Signaturschlüssels die Verantwortung bzw. Folgen trägt?

Abs. 2: Ob hier eine Meldung, ja sogar eine Sperre, erforderlich ist oder ein Passwortwechsel genügt, ist wohl abhängig vom technischen Umfeld des Signaturschlüssels (siehe einleitende Vorbemerkung). Entsprechend wäre der vorliegende Abs. 2 ersatzlos zu streichen oder zu belassen, je nachdem, ob in technischer Hinsicht die besagte Korrektur in der VZertES gemacht wird oder nicht. Sollte die zwingend erforderliche Korrektur technischer Natur nicht erfolgen, so müsste dieser Abs. 2 bestehen bleiben, ohne dass aber der neu eingefügte Abs. 6 in Art. 12 (Passwortwechsel) sich damit erübrigte - denn jener führt je nach Sachlage mindestens zu einer gewissen Risikominimierung für die Übergangszeit bis zur Sperre des Signaturschlüssels.

Abs. 3: Ist wohl ersatzlos zu streichen.

**Art. 13 könnte somit wie folgt lauten:**
(Mit Grossbuchstaben werden die neuen Textstellen gekennzeichnet.)

> *"(1) WEISS ODER VERMUTET DIE INHABERIN ODER DER INHABER, DASS SEIN EIGENER SIGNATURSCHLÜSSEL EINEM DRITTEN IN BESITZ GELANGT IST ODER dass sie oder er diesen verloren hat, muss sie oder er DAS ZERTIFIKAT UMGEHEND UNGÜLTIG ERKLÄREN lassen.*
>
> SOLANGE KEINE MELDUNG ERFOLGT IST UND DIE LÖSCHUNG DES ZERTIFIKATS IM RAHMEN DES ÜBLICHEN GESCHÄFTSGANGES NICHT ERFOLGEN KONNTE, TRÄGT DIE INHABERIN ODER DER INHABER DIE VERANTWORTUNG FÜR DEN MISSBRÄUCHLICHEN EINSATZ DES ZERTIFIKATS.
>
> (2) ... (ev.) ..... ."

## III. Technische und Administrative Vorschriften

### *1.4 Qualifizierte elektronische Signaturen, Punkt 3*

Die Bedeutung von "Mittel, welche er unter seiner alleinigen Kontrolle halten kann", muss ausformuliert werden.

***1.4 Qualifizierte elektronische Signaturen, Punkt 4***

Der Verweis auf ZertES ist durch einen zusätzlichen direkten Verweis zu ergänzen. ZertES verweist nämlich auf VZertES, welche wiederum unter Art. 3 Abs. 2 auf die BAKOM Vorschriften verweist.

***1.4 Registrierung***

Ein “Aktivierungscode zur Aktivierung der Nutzung“ kann nicht nur nebenbei in einer Definition erwähnt werden, wie das hier offenbar der Fall ist.

***1.4 Sichere Signaturerstellungseinheit***

Der Verweis auf ZertES ist durch einen zusätzlichen direkten Verweis zu ergänzen. ZertES verweist nämlich auf VZertES, welche wiederum unter Art.3 Abs.2 auf die BAKOM Vorschriften verweist.

***3.3.8 a) & b)***

Für die Generierung des Schlüssels sind Algorithmen gemäss einer detaillierten Spezifikation (siehe: Draft ETSI TS 102 XXX V.0.0.1, Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Electronic Signatures) zwingend erforderlich.

***3.3.9***

Die sichere Signaturerstellungseinheit ist durch Artikel 6 Absatz 2 der ZertES (Mindestanforderungen) unzureichend spezifiziert. Signaturschlüssel- und Passwortanforderung gemäss Art. 11 & 12 der VZertES liefern beispielsweise weitere Spezifikationen. Art.6, Abs.1 und 2 c) erfordern zudem eine zusätzliche Regelung auch für die Signaturanwendungsumgebung.

Besten Dank für Ihre wohlwollende Prüfung unserer Anliegen. Für weitere Auskünfte stehen wir Ihnen sehr gerne zur Verfügung.

Mit freundlichen Grüssen
Schweizerische Bankiervereinigung

M. Tissot Dr C. Winzeler