

Stellungnahme zum BGES

Stellungnahme der Fachgruppe Security zum Entwurf des „Bundesgesetz über die elektronische Signatur (BGES) (Vernehmlassungsvorlage), Januar 2001)

27. März 2001.

Inhalt

1	Einleitung	2
2	Kommentare zum BGES	2
	2.1 Terminologie	2
	2.2 EU Kompatibilität	2
	2.3 Secure Signature Device	2
	2.4 Freiwillige Akkreditierung	3
	2.5 Obligationenrecht	3
3	Kommentare zum Begleitbericht	3
	3.1 Marktpositionierung	3
4	Detaillierte Kommentare	3
5	Fazit	8
6	Kontaktadressen	9
7	Referenzen	9

Abkürzungen

BAKOM	Bundesamt für Kommunikation
CSP	Certificate Service Provider
FGSec	Fachgruppe Security der SI
HCI	Human-Computer Interface
PKI	Public Key Infrastructure
SI	Schweizerische Informatiker Gesellschaft

Begriffe

englisch	Deutsch
*Advanced Electronic Signature	Fortgeschrittene elektronische Signatur
Certification-service-provider	Zertifizierungsdiensteanbieter
Distinguished Name	Eindeutiger Name
*Electronic Signature	elektronische Signatur
*Qualified Certificate	Qualifiziertes Zertifikat
Relying Party	Empfänger einer unterschriebene Meldung
*Secure signature creation device	Sichere Signaturerstellungseinheit
*Signatory	Unterzeichner
*Signature-creation device	Signaturerstellungseinheit
* gemäss [EU-RL]	

1 Einleitung

Die Fachgruppe Security (FGSec) ist eine weitgehend selbständige Sektion der schweizerischen Informatiker Gesellschaft. Sie wurde 1993 gegründet. Ihr Ziel ist die Förderung der Informationssicherheit in Gesellschaft, Öffentlichkeit und Wirtschaft. Weitere Informationen sind erhältlich unter <http://www.fgsec.ch>.

Die FGSec bildet regelmässig Arbeitsgruppen zu aktuellen Themen, welche sich mit der Erarbeitung des Stands der Entwicklung und dem Aufzeigen der Perspektiven von sicherheitsrelevanten Technologien und deren Anwendungen beschäftigen. Die Ergebnisse werden in der Regel in einer Fachtagung vorgestellt, z.B. zum Thema PKI am 28. März 2001 in Zürich.

Darüberhinaus nimmt die FGSec Stellung zu informationssicherheitsrelevanten Entwicklungen. Der vorliegende Kommentar zum Bundesgesetz über die elektronische Signatur (BGES) wurde von der Arbeitsgruppe PKI der FGSec entwickelt, die mehr als 20 Personen umfasst. Der erstellende Ausschuss setzte sich am 7. März 2001 zusammen aus Anthony Thorn (Leiter), Dr. Marcus Holthaus, Daniel Frei, Andreas Kohler und Fredy Schwyter. Alle Mitglieder der Arbeitsgruppe PKI sind Experten im Bereich Informationssicherheit und bearbeiten v.a. **technisch-organisatorische** Gegebenheiten.

Nachfolgende Kommentare werden getragen vom Ausschuss, von der AG PKI, sowie vom Vorstand der FGSec.

2 Kommentare zum BGES

2.1 Terminologie

Die Terminologie des BGES (Begriffe in Artikel 3) muss durch diejenige aus der EU-Direktive [EU-Dir] ersetzt werden. Dies hat eine Überarbeitung des gesamten Dokuments zu Folge.

Im Besonderen müssen die Begriffe „Qualifiziertes Zertifikat“ (Qualified Certificate), „Fortgeschrittene elektronische Signatur“ (Advanced Electronic Signature)“ und „Sichere Signaturerstellungseinheit“ (Secure signature creation device) verwendet werden. Ausserdem etabliert sich der Begriff „Qualified Certificate“ weltweit [RFC 3039] und nicht nur in Europa.

2.2 EU Kompatibilität

Die Kernaussage der EU Direktive nämlich die Äquivalenz einer Handunterschrift zu;

ein „fortgeschrittene elektronische Signatur“ basierend auf ein „Qualifiziertes Zertifikat“ welche mit einer „sichere Signaturerstellungseinheit“ fehlt im BGES.

2.3 Secure Signature Device

Das Problem eines korrumpierten Terminals wird im BGES ignoriert. Dieses Problem stellt (neben der Verständnisfrage bei den Nutzern) **das grösste Hindernis** einer verbreiteten Verwendung dar.

Der Begleitbericht impliziert in 23, bzw. 231, dass ein E-Mail-Client eine akzeptable sichere Signaturerstellungseinheit ist. Wir sind der Überzeugung, dass diese Annahme falsch ist und dass E-Mail-Clients ein hohes Gefährdungspotential aufweisen.

Die Qualität der Benutzerschnittstelle (Human-Computer-Interface HCI) der sicheren Signaturerstellungseinheit muss ebenfalls behandelt werden. Sie muss die unbeabsichtigte Unterzeichnung verhindern, da diese zu rechtlichen Verbindlichkeiten führt.

Wie empfehlen, dass das BAKOM eine Richtlinie herausgibt, wie ein Nutzer seinen privaten Schlüssel aufbewahren, verwenden und schützen muss.

Diese Richtlinie muss dem Nutzer durch den CSP übergeben und bestimmt, wie sicher die Signaturerstellungseinheit sein muss und wie er dies gewährleisten kann.

Es ist möglich und problematisch, dass diese Richtlinie während der Lebensdauer eines Zertifikates nachgeführt und überarbeitet werden muss.

2.4 Freiwillige Akkreditierung

Die Problematik eines unakkreditierten CSP, welcher qualifizierte Zertifikate ausstellt, muss ebenfalls noch behandelt werden.

2.5 Obligationenrecht

Die Formulierung von Artikel 15a OR (neu) impliziert, dass auch Zertifikate, welche nicht dem BGES entsprechen, eigenhändigen Unterschriften rechtlich gleichgestellt sind (auch Testzertifikate), wenn sie von einem akkreditierten CSP ausgestellt wurden.

3 Kommentare zum Begleitbericht

Der Inhalt des Begleitberichts deckt zum Teil Fragestellungen unterschiedlicher Tiefe in einer nicht nachvollziehbaren Form ab, und ist in der aktuellen Version nicht akzeptabel. Z.B. erklärt 142.2 exzellent und nachvollziehbar die Auswirkungen auf die *Willenserklärung* und *Haftung*. Die in 210.071 genannten Beispiele, "*Sein Leben zu riskieren*" und in 210.073 "*Stromunterbruch*", sind in der vorliegenden Art zu grob, decken die eigentlichen Problematiken nicht ab und diskreditieren den Rest des Dokuments.

Eine angemessene Behandlung des Problems der Unterwanderung eines Systems (Trojanische Pferde etc.) fehlt hingegen.

3.1 Marktpositionierung

Es ist bisher nicht klar, ob "BGES"-Unterschriften auf den High-End-Teil des Marktes abzielen – wo hohe Kosten vertretbar sind und die Zertifikate eher punktuell verwendet werden würden – oder ob sie den mittleren Bereich abdecken sollen, in welchem eine erschwingliche Lösung für einen grossen Marktanteil sorgen würde. Das BGES und der Begleitbericht implizieren hier unterschiedliche Zielsetzungen: Das BGES ignoriert das Problem der sicheren Signaturerstellungseinheit, und der Begleitbericht impliziert, dass ein E-Mail-Client für diesen Zweck akzeptabel ist.

Wir bitten zu beachten, dass in den vergangenen Monaten verschiedene Schwächen in E-Mail-Clients entdeckt und zum Teil von verbreiteten Schadprogrammen ausgenutzt wurden, welche die E-Mail-Clients zu Aktivitäten veranlassten, welche vom Benutzer nicht beabsichtigt waren.

4 Detaillierte Kommentare

Art.	BGES Text	Comment
1	" Gegenstand und Zweck 1 Dieses Gesetz regelt die Voraussetzungen, unter denen sich Anbieterinnen von Zertifizierungsdiensten anerkennen lassen können, und deren Rechte und Pflichten.	Es regelt auch die Verwendung der elektronischen Signatur, der Haftung der Nutzer und Zertifizierungsdienststellen (CSPs) usw.
	2 Es hat zum Zweck: a. b. durch die Gleichstellung der elektronischen Signatur mit der eigenhändigen Unterschrift (Art. 15a des Obligationenrechts 2) die rechtliche Anerkennung elektronischer Signaturen sicherzustellen;	"Gleichstellung" ist irreführend, denn es bestehen wesentliche Unterschiede. Im Besonderen hat die Beweislastumkehr zwar gleiche Rechte, aber viel mehr Pflichten zur Folge. Nur die Anerkennung ist gleichgestellt, nicht die Unterschrift.
2	3 Macht der Bundesrat von dieser Möglichkeit Gebrauch, so kann er unter Beachtung der Grundsätze dieses Gesetzes spezifische Ausführungsbestimmungen erlassen.	Die aktuellen Ausführungsbestimmungen (Entwurf) beziehen sich auf die Zertifizierungsdienstverordnung, und nicht auf das BGES.

Art.	BGES Text	Comment
3	Begriffe	<p>Es bestehen keine Referenzen der Beziehungen zu den EU-Begriffen der „Fortgeschrittene elektronische Signatur (Advanced Electronic Signature)“, „Qualifiziertes Zertifikat (Qualified Certificate)“, „und „Sichere Signaturerstellungseinheit (Secure Signature Creation Device) etc. Vgl. EU-Direktive Art. 2.</p> <p>Das „Sichere Signaturerstellungseinheit“ wird nicht erwähnt. Dies hat ernsthafte Konsequenzen. Vgl. unten.</p>
	a & b	<p>Der Begriff „digitale Signatur“ ist hier neu, stellt das zentrale Element dar, wird aber später nicht mehr verwendet! Der Begriff „elektronische Signatur“ stellt zwar notwendige, aber nicht hinreichende Voraussetzungen zur Verfügung; Der Titel „BGES“ müsste eigentlich „BGDS“ lauten. Die fortgeschrittene elektronische Signatur wird nicht genannt.</p>
	f. Zertifikat: elektronische Bescheinigung, welche die Zuordnung eines öffentlichen Prüfschlüssels zu einer natürlichen Person bestätigt und durch die digitale Signatur einer Anbieterin von Zertifizierungsdiensten authentifiziert wird;	<p>Das Zertifikat bindet den Schlüssel an den eindeutigen Namen (Distinguished Name) einer natürlichen Person, nicht an die Person selbst.</p>
	g. Anbieterin von Zertifizierungsdiensten Stelle, die im Rahmen einer elektronischen Umgebung Daten beglaubigt und zu diesem Zweck elektronische Zertifikate ausstellt.	<p>g. Das BGES behandelt nur die Beglaubigung von öffentlichen Schlüsseln, und nicht allgemein die „Daten-Beglaubigung“</p>
4		<p>Das Zertifikat sollte als „Qualified“ bezeichnet werden und die entsprechenden Eigenschaften aufweisen, da dies international verstanden wird, anstatt sich auf das BGES zu beziehen.</p>
	c. zuverlässige Informatiksysteme und -produkte verwenden;	<p>Nicht nur zuverlässig, sondern auch vertrauenswürdig. Im deutschen Sprachgebrauch wird i.d.R. von „verlässlichen und vertrauenswürdigen Informationssystemen“ gesprochen.</p>
	d. über ausreichende Finanzmittel und -garantien verfügen;	<p>Warum Finanzmittel UND -garantien? Theoretisch sollte eines von beiden genügen.</p>
	e. die notwendigen Versicherungen zur Deckung allfälliger Haftungsansprüche und der Kosten, welche aus den in Artikel 13 Absätze 2 und 3 vorgesehenen Mass-nahmen erwachsen könnten, abschliessen	<p>Es ist nicht klar, ob dies sowohl die Haftungsansprüche (Art 18) wie auch die osten einer Stilllegung (Art 13) betrifft. (e.g. sowie die Kosten...)</p> <p>Die übersteigt die Anforderungen der EU Direktive.</p>

Art.	BGES Text	Comment
	C & D	<p>Die Finanzmittel sollten ausreichen, damit der CSP arbeiten kann, ohne unangebrachte Rationalisierungen vornehmen zu müssen. Die Garantien und Versicherungen müssen ausreichen, um potentielle Haftung und Kosten der Stilllegung abdecken zu können. (Art 13).</p> <p>Es besteht ein prinzipielles Problem mit der "angemessenen Haftung" der Verwendung von Zertifikaten. Ein Zertifikat, welches auf unangemessenem Weg erlangt wurde, kann theoretisch tausendfach missbraucht werden, bevor es revoziert wird. Die Anzahl der Nutzungen liegt ausserhalb des Einflussbereichs des CSPs oder des rechtmässigen Nutzers; deshalb kann er nicht dafür haften und es kann nicht durch ihn versichert werden.</p>
8	<p>1 Jedes gestützt auf dieses Gesetz ausgestellte elektronische Zertifikat muss auf eine natürliche Person lauten und hat mindestens folgende Angaben zu enthalten:</p> <p>a.</p> <p>b. den Hinweis, dass es in Anwendung dieses Gesetzes und der entsprechenden Ausführungsvorschriften ausgestellt wurde;</p>	<p>Dies bedeutet, dass jedes Zertifikat auf das BGES verweist.</p> <p>Dies ist nicht kompatibel zur EU-Direktive, welche eine Referenz des "Qualifiziertes Zertifikat (Qualified Certificate)" verlangt.</p> <p>Es wäre angemessener, "Swiss qualified certificate issued by an accredited certificate service provider" als Referenz zu verwenden.</p>
	c. den Hinweis auf mögliche Nutzungsbeschränkungen;	Nutzungs- und/oder Haftungs- beschränkungen
	d. den Namen des Inhabers oder der Inhaberin des öffentlichen Prüfschlüssels;	Dies muss ein Distinguished name sein, d.h. er muss eindeutig sein.
10	<p>Informations- und Dokumentationspflicht</p> <p>1</p> <p>2 Sie müssen ihre Kunden und Kundinnen spätestens bei der Ausstellung der elektronischen Zertifikate auf die Folgen eines möglichen Missbrauchs oder Verlusts des privaten Signaturschlüssels aufmerksam machen. Sie müssen ihnen geeignete Massnahmen zur Geheimhaltung des privaten Signaturschlüssels vorschlagen.</p>	Dies kann nur umgesetzt werden, wenn das BAKOM einen Standard-Text für die CSPs entwirft, welche diese an ihre Kunden weitergeben können. Der Text wird, häufige Nachführungen aufgrund der fortschreitenden technologischen Entwicklung und der Bedrohung durch Unterwanderung verlangen.
11	3 Bestehen bezüglich der Gültigkeit des Zertifikats Zweifel, so kann dieses für die Dauer von maximal drei Tagen suspendiert werden. Nach Ablauf dieser Frist erklären die Anbieterinnen von Zertifizierungsdiensten die Zertifikate definitiv für ungültig oder erneut für gültig. Im ersten Fall wird die Ungültigerklärung im Zeitpunkt der Suspendierung des Zertifikats wirksam; im zweiten Fall hat die Suspendierung keine Wirkung auf die Gültigkeit des Zertifikats.	Es sollte klar geäussert werden, dass der Nutzer innert (z.B.) 3 Tagen reagieren muss, da ansonsten sein Zertifikat revoziert wird.

Art.	BGES Text	Comment
12	Verzeichnisse der elektronischen Zertifikate	Terminologie: Der Begriff „Verzeichnis“ kann als technischer Terminamentlich für X.500- oder LDAP-Verzeichnisse verstanden werden, oder einfach als indizierte Liste von Daten.
	1 Jede anerkannte Anbieterin von Zertifizierungsdiensten führt ein Verzeichnis der elektronischen Zertifikate, in das sich ihre Kunden und Kundinnen eintragen lassen können.	Dies ist ein Verzeichnis im technischen Sinne.
	2 Sie führt zudem ein Verzeichnis aller für ungültig erklärten oder suspendierten Zertifikate, auch wenn diese nicht im Verzeichnis nach Absatz 1 eingetragen worden sind.	Dies muss kein Verzeichnis im technischen Sinne sein. Ausserdem muss es kein Verzeichnis der Zertifikate sondern nur ein Verzeichnis der Seriennummern sein.
	3 Sie gewährleistet jederzeit den elektronischen Zugang zu den Verzeichnissen. Dafür darf neben den Kosten für die Nutzung der öffentlichen Fernmeldedienste kein weiteres Entgelt verlangt werden.	„den Verzeichnissen“ bezieht sich auf zwei unterschiedliche Objekte Der Begleitbericht ist in diesem Punkt auch verwirrend.
13	Einstellung der Geschäftstätigkeit 1 2 Stellen sie ihre Geschäftstätigkeit freiwillig ein, so sind sie verpflichtet, die von ihnen ausgestellten, noch gültigen elektronischen Zertifikate für ungültig zu erklären. Die Akkreditierungsstelle beauftragt eine andere anerkannte Anbieterin von Zertifizierungsdiensten, das Verzeichnis der für ungültig erklärten Zertifikate zu führen und die abgelaufenen oder für ungültig erklärten Zertifikate, das Tätigkeitsjournal sowie die entsprechenden Belege aufzubewahren.	Sind akkreditierte CSPs verpflichtet, die CRLs und Logs eines anderen CSPs zu führen, der seine Geschäftstätigkeit eingestellt hat? Wer entscheidet, zu welchem Preis dies zu geschehen hat?
	3 Fällt eine anerkannte Anbieterin von Zertifizierungsdiensten in Konkurs, so beauftragt die Akkreditierungsstelle eine andere anerkannte Anbieterin von Zertifizierungsdiensten, die von jener ausgestellten, noch gültigen elektronischen Zertifikate für ungültig zu erklären, das Verzeichnis der für ungültig erklärten Zertifikate zu führen und die abgelaufenen oder für ungültig erklärten Zertifikate, das Tätigkeitsjournal sowie die entsprechenden Belege aufzubewahren.	Dies stellt ein Problem dar, da ein X.509-Zertifikat den CRL-Issuer spezifiziert (optionales Attribut “CRL Distribution Point,” oder default Certificate Issuer). Es ist nicht offensichtlich, wie <i>die relying party</i> überzeugt werden kann, dass der neue CRL Ausgeber authoritative ist- im Besonderen wenn der Nachschlag in der CRLautomatisiert wurde. Eine Umleitung zum neuen Aussteller ist einfach, aber ändert die Ausstellerinformation nicht.
14	Datenschutz 1 Die anerkannten Anbieterinnen von Zertifizierungsdiensten dürfen diejenigen Personendaten erheben und weiterbearbeiten, die zur Erfüllung ihrer Aufgaben notwendig sind. 2 Im Übrigen gilt die Datenschutzgesetzgebung.	Es muss ein Basis festgelegt werden, um zu einer einheitlichen Bestimmung des eindeutige Namensgebung zu gelangen., z.B. <ul style="list-style-type: none"> • Name, Vorname, Stadt, Land, Geburtsdatum , E-Mail-Adresse • Name, Vorname, Land, AHV Nr. etc.

Art.	BGES Text	Comment
	<p>Verwendung privater Signaturschlüssel</p> <p>1</p> <p>2 Die Inhaber und Inhaberinnen privater Signaturschlüssel müssen diese so aufbewahren, dass eine Verwendung durch unbefugte Drittpersonen ausgeschlossen werden kann. Sie treffen hierzu alle nach den Umständen zumutbaren Vorkehrungen.</p>	<p>Wir empfehlen "mit hoher Wahrscheinlichkeit ausgeschlossen werden kann."</p> <p>Der Begriff „Ausgeschlossen“ ist nicht zufriedenstellend, und der Begleitbericht geht nicht in genügendem Masse auf die einzelnen Gefährdungen ein.</p> <p>Das Problem ist nicht, sein „Leben zu riskieren“, aber die Unterwanderung der Signaturgeräte durch Trojanische Pferde und andere Malware.</p> <p>Keine der momentan verbreiteten Plattformen, und keines der erschwinglichen Geräte, können momentan einer Unterwanderung widerstehen. Ein trojanisches Pferd könnte beispielsweise</p> <ul style="list-style-type: none"> • Eine Kopie des privaten Schlüssels, welche auf dem Harddisk des Nutzers gespeichert ist, zum Angreifer senden. • Den privaten Schlüssel verwenden, um ein anderes Dokument zu unterzeichnen, als der Nutzer legitimiert (gesehen) hat, auch wenn der Schlüssel auf einer Smartcard gespeichert ist. <p>Wir können die Grösse des aus dieser Unterwanderung entstehenden Schadens nicht abschätzen. Kreditkartenfirmen akzeptieren seit Jahren einen gewissen Prozentsatz betrügerischer Transaktionen als Teil ihrer Geschäftstätigkeit, ebenso wie ein Einzelhändler unerklärliche Bestandesrückgänge akzeptiert.</p> <p>Es könnte aber auch katastrophale Ausmasse annehmen, wenn beispielsweise ein verbreiteter E-Mail-Client als Sichere Signaturerstellungseinheit akzeptiert wird und eine Schad-Software dieses System gezielt und verbreitet attackiert.</p> <p>Es muss definiert werden, was "zumutbar" ist.</p>
17	<p>Haftung des Inhabers oder der Inhaberin des privaten Signaturschlüssels</p> <p>1 Die Person, die behauptet, ihr privater Signaturschlüssel sei ohne ihren Willen zum Einsatz gelangt, ist dafür beweispflichtig.</p>	<p>„<i>beweispflichtig</i>“ zu sein, ist kritisch. da eine Unterwanderungsgefahr auf jeder Plattform besteht. Es besteht niemals eine Gewähr für die Grundvoraussetzung „What You See Is What You Sign“</p>
	<p>3 Die Haftung entfällt, wenn der Inhaber oder die Inhaberin des privaten Signaturschlüssels die Vorkehrungen nach Artikel 16 Absatz 2 getroffen hat. Im Übrigen gelten die Bestimmungen des Obligationenrechts.</p>	<p>Art 16 definiert keine Vorkehrungen, sondern bezieht sich nur auf das „Zumutbare“.</p>
18		<p>Welche Haftung tragen die Anerkennungstellen?</p>

Art.	BGES Text	Comment
22	<p>1 Wer als Anbieterin von Zertifizierungsdiensten vorgibt, über die Anerkennung nach diesem Gesetz zu verfügen, oder wer Zertifikate nach diesem Gesetz ausstellt, ohne die Angaben nach Artikel 8 zu machen, wird auf Antrag mit Busse bis zu 100 000 Franken bestraft.</p>	<p>Die EU-Direktive erlaubt die Ausstellung qualifizierter Zertifikate auch ohne Akkreditierung. Es ist klar aus dem Begleitbericht, dass dies in der Schweiz nicht erlaubt sein wird. Dies geht aber nicht aus dem BGES-Text hervor. Ist dies EU-kompatibel? Was liegt in unserem Interesse?</p>
	<p>Obligationenrecht</p>	
	<p>Art 15a e. Elektronische Signatur Wird ein Vertrag durch elektronischen Datenaustausch abgeschlossen, so ist die elektronische Signatur der eigenhändigen Unterschrift nach Artikel 14 gleichgestellt, wenn sie auf dem Zertifikat einer anerkannten Anbieterin von Zertifizierungsdiensten im Sinne des Bundesgesetzes vom 10.10 über die elektronische Signatur beruht.</p>	<p>Die Begriffe „Digitale Signatur“ / „Elektronische Signatur“ werden inkonsistent verwendet. Die Anerkennung ist gleichgestellt, nicht die Unterschrift. Es wurde vergessen, dass eine „anerkannte Anbieterin von Zertifizierungsdiensten im Sinne des Bundesgesetzes“ auch andere Arten von Zertifikaten ausstellen kann, z.B. Test-Zertifikate. Diese sind nicht für eine Verwendung vorgesehen, welche eine Gleichstellung zur Handsignatur erlauben würde. Wir vermissen ein Äquivalent zur EU-Direktive bzgl.</p> <ul style="list-style-type: none"> • Fortgeschrittene elektronische Signatur (Advanced Electronic Signature) • Qualifiziertes Zertifikat (Qualified Certificate) • „Sichere Signaturerstellungseinheit“ (Secure Signature Creation Device) <p>Nicht nur der CSP, sondern auch Zertifikat, Signatur sowie sichere Signaturerstellungseinheit müssen dem BGES entsprechen.</p>
	<p>2. Bei Führung des Handelsregisters mit EDV 1 ... 2 Der Bundesrat bestimmt, ob und unter welchen Voraussetzungen die elektronische Einreichung von Anmeldungen und Belegen beim Handelsregister zulässig ist. Er kann den Kantonen die Ausstellung beglaubigter, elektronisch signierter Handelsregisterauszüge vorschreiben.</p>	<p>Die Begriffe „Digitale Signatur“ / „Elektronische Signatur“ werden inkonsistent verwendet.</p>

5 Fazit

Die Arbeitsgruppe PKI der FGSec sieht grundsätzliche technische Voraussetzungen nicht erfüllt, um eine Gleichstellung der Anerkennung elektronischer (digitaler) Signaturen mit handschriftlichen

Unterschriften zu erlauben. Insbesondere das Problem der Unterwanderung von Signaturgeräten ist heute nicht gelöst. E-Mail-Clients sind keine und "Sichere Signaturerstellungseinheiten".

Auch wird die in Teilen fehlende Kompatibilität zur EU-Direktive bemängelt. Es wird Frage gestellt, ob nicht eine weitgehende Kompatibilität angestrebt werden müsste.

Es bestehen weitere Schwächen und Inkonsistenzen, welche uns zur Ablehnung des Vorschlages und zur Forderung einer grundsätzlichen Diskussion und Überarbeitung veranlassen.

6 Kontaktadressen

Fachgruppe Security
Arbeitsgruppe Public Key
Infrastructure

Anthony Thorn
AT Systems & Services GmbH
Ringstrasse 5
6332 Hagendorn

Tel 041 783 10 40
Fax 041 783 10 44
anthony.thorn@atss.ch

Fachgruppe Security
Vorstand

Dr. Marcus Holthaus
IMSEC GmbH
Dersbachstrasse 312a
Hünenberg
6330 Cham

Tel 041 780 00 11
Fax 041 780 00 21
Marcus.Holthaus@imsec.ch

7 Referenzen

[EU-RL] RICHTLINIE 1999/93/EG DES EUROPÄISCHEN PARLAMENTS UND DES
RATES vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für
elektronische Signaturen

[RFC 3039] Internet X.509