ID Cyber-Identity AG
Technoparkstrasse 1
8005 Zürich

14. Mai 2012

Herrn
Urs Paul Holenstein
Bundesamt für Justiz
Bundesrain 20
CH-3003 Bern

Betrifft: Neufassung des Bundesgesetze über die elektronische Signatur, ZertES

Sehr geehrter Herr Holenstein,

Zur Neufassung des Bundesgesetzes über die elektronische Signatur, ZertES nehmen wir wie folgt Stellung:

1. Das bestehende Bundesgesetz über die elektronische Signatur (ZertES) vom 19.12.2003 definiert die qualifizierte elektronische Signatur im Sinne einer eigenhändigen Unterschrift gemäss OR 14 Abs. 2bis. Es definiert die dazu notwendigen qualifizierten Zertifikate und regelt die zu erfüllenden Voraussetzungen für die Anerkennung von Zertifizierungsdienstanbieterinnen, welche qualifizierte Zertifikate ausstellen.
   Der Fokus des bestehenden ZertES ist somit ausgerichtet auf eine ganz bestimmte Anwendung von digitalen Zertifikaten, nämlich die elektronische Unterschrift, gleichgestellt der eigenhändigen Unterschrift gemäss OR 14, wenn eine solche überhaupt erforderlich ist.

2. Dieser Fokus ist zu eng und wird den vielfältigen Anwendungen von digitalen Zertifikaten wie z.B. Massensignatur von elektronischen Dokumenten, Code Signatur und Authentisierung eines Partners im elektronischen Geschäftsverkehr nicht gerecht.

   Zurecht geht deshalb die Neufassung des ZertES davon aus, dass in der Praxis den jeweiligen Anwendungen entsprechend verschiedene Zertifikatsklassen eingesetzt werden. Im neuen Gesetz werden deshalb zwei Zertifikatsklassen gesetzlich geregelt, nämlich:
   a) Das qualifizierte Zertifikat wie bisher für die qualifizierte Signatur äquivalent zur persönlichen eigenhändigen Unterschrift gemäss OR 14;
   b) Das geregelte Zertifikat, offen für vielfältige heutige und künftige Anwendungen im automatischen oder Personen-gebundenen elektronischen Verkehr, sowohl für elektronische Signatur als auch für Authentisierung von Geschäftspartnern.

   Mit den entsprechenden Regelungen der Haftung wird die nötige Rechtssicherheit bei der Ausstellung und Verwendung dieser beiden Zertifikate geschaffen.

3. Damit folgt der Gesetzgeber nunmehr dem Standard „**eCH-0048 PKI-Zertifikatsklassen“ (2006; rev. 2012)** des Vereins eCH für eGovernment Standards. Zweck des Standards ist (Zitat):
   Wesentliche Grundlage zur Realisierung verbindlicher und vertrauenswürdiger eGovern-

ment Geschäftsprozesse ist die verlässliche Identifikation der beteiligten Partner. Als internationaler Standard hat sich in diesem Kontext der Einsatz von elektronischen Signaturen mittels X.509 Zertifikaten etabliert. Diesem technischen Standard ist zusätzlich ein organisatorisches und juristisches Regelwerk an die Seite zu stellen, damit die eindeutige Zuordnung von Dokumenten, Willenserklärungen, etc. zu ihren Urhebern in Form digitaler Signaturen sichergestellt werden kann und mit den von allen Beteiligten gewünschten Rechtsfolgen verbunden ist.
Das Einsatzgebiet von X.509 Zertifikaten ist nicht nur auf die Signatur von elektronischen Dokumenten beschränkt. Es umfasst weiterhin die Authentifizierung, Code-Signaturen, Verschlüsselung und weitere. Der vorliegende eCH-Standard ***adressiert sämtliche Einsatzbereiche.***

Das notwendige **Know-How für die Neufassung der Verordnung** und der **Technischen und Administrativen** Vorschriften ist bei eCH vorhanden und kann in Anspruch genommen werden.

4. **Hervorzuheben** ist im Entwurf der Neufassung (Art. 7 und Art. 13):
   a) Das geregelte Zertifikat kann auf natürliche Personen UND auf UID-Einheiten (juristische Personen, Personengesellschaften, einfache Gesellschaften, etc. gem. UIDG vom 18.6.2010, welche mit einer Unternehmens-Identifikationsnummer UID identifiziert sind) ausgestellt werden.
   b) Das geregelte Zertifikat *kann* zudem enthalten: „*spezifische Attribute der Inhaberin oder des Inhabers des zugehörigen geheimen kryptografischen Schlüssels, beispielsweise berufliche Qualifikationen;*“ sowie bei natürlichen Personen den Hinweis, „*dass sie zur Vertretung einer bestimmten Person oder UID-Einheit berechtigt ist;*“
   c) Zeitstempeldienst durch anerkannte Anbieterinnen Zertifizierungsdiensten.

   Damit kann **die heute notwendige Infrastruktur zum Gebrauch dieser Zertifikate** wie Nachweis von Berufsausweisen und Vertretungsbefugnissen **stark vereinfacht werden.** Ein qualifizierter Zeitstempel gem. c) kann insbesondere die Beweiskraft der qualifizierten Signatur im Verkehr mit Behörden und Gerichten erhöhen.

5. Hinweis zur Neuformulierung von OR Art. 59a (implizite Beweislastumkehr):
   Im erläuternden Bericht wird bezüglich Haftung nach OR 59a ausgeführt: „*Art. 59a Haftung für Signaturschlüssel: Die bisherige Haftung des Schlüsselinhabers für qualifizierte Zertifikate soll auch auf geregelte Zertifikate ausgedehnt werden, weil diese Haftung eine der essentiellen Grundlagen für die Akzeptanz beim Dritten ist; ohne diese Haftung wäre das geregelte Zertifikat in den Augen dessen, der sich darauf verlassen soll, wenig wert.* ***Allerdings soll die Haftung auf Signatur-Anwendungen beschränkt sein und für Authentisierung oder weitere Anwendungen nicht gelten****. Aus diesem Grund wird hier (in OR Art. 59a neu) der Begriff «Signaturschlüssel» NICHT durch den generellen Begriff «kryptografischer Schlüssel» ersetzt.*“

   Die Neufassung von OR Art. 59a, Abs. 1 im Entwurf lautet aber:
   „*Der Inhaber eines* ***geheimen kryptografischen Schlüssels (anstelle des Begriffs Signaturschlüssel in OR Art. 59a alt)*** *haftet Drittpersonen für Schäden, die diese erleiden, weil sie sich auf ein gültiges geregeltes Zertifikat einer anerkannten Anbieterin von Zertifizierungsdiensten im Sinne des Bundesgesetzes vom … über die elektronische*

Signatur verlassen haben."
Diese widersprüchliche Formulierung im Entwurf von OR Art. 59a lässt vermuten, dass für Authentisierung die gleiche Haftungsregelung (d.h. implizite Beweislastumkehr) wie für Signatur gilt.
Dieser Widerspruch sollte beseitigt werden! Wir sind der Meinung, dass die Aussage im erläuternden Bericht im Gesetz klar zum Ausdruck kommt, wonach die Haftung im Sinne einer Beweislastumkehr auf Signatur-Anwendungen beschränkt ist.

6. Schlussfolgerungen

a) Das geregelte Zertifikat kann sowohl für Authentisierung als auch für Signatur verwendet werden.
Die **Signatur entspricht aber nicht einer eigenhändigen Unterschrift** gemäss OR 14 durch eine natürliche Person. Dafür ist nach wie vor ein qualifiziertes Zertifikat zu verwenden. Bei der Verwendung eines geregelten Zertifikates für Signierung durch eine natürliche Person besteht bezüglich **Haftung** gemäss OR 59 a (neu) aber **kein Unterschied** zu einem qualifizierten Zertifikat.
Die in Punkt 5 angesprochene verschiedene Haftung für Authentisierung und Signatur legt deshalb nahe, dass es möglich sein sollte, ein **Zertifikat NUR für Authentisierung** lösen zu können und für Signierung im Sinne von OR 14 Abs. 2bis ein qualifiziertes Zertifikat zu lösen. Im Abschnitt 1.2 des erläuternden Berichtes „Ziele der Revision" wird diese Ansicht gestützt durch (Zitat) „*In der Praxis wird das Vertrauen zwischen Partnern im elektronischen Verkehr in der Mehrzahl der Fälle nicht durch eine signierte Meldung, sondern durch die Authentisierung an einem Online-Dienst hergestellt.*"

b) Die **Haftungs-Regelung für geregelte Zertifikate**, wonach bei geregelten Zertifikaten nur bei Signatur und nicht bei Authentisierung die implizite Beweislastumkehr von OR 59 a (neu) gilt, **ist missverständlich** (unklar, schwer zu verstehen). Diese Regelung wird im erläuternden Bericht durch die Aussage zu OR 59a (neu) erörtert, wonach diese Haftung eine essentielle Grundlage für die Akzeptanz von geregelten Zertifikaten bei Dritten sei. Wir bezweifeln diese Aussage aber.
Das Problem kann gelöst werden, indem die bestehende Formulierung von OR 59a beibehalten wird, d.h. dass **diese Haftungsregelung nur für qualifizierte Zertifikate** gilt. Ohne implizite Beweislastumkehr wird die geregelte elektronische Signatur gemäss Neufassung Art. 2.c zu dem, was eine Unterschrift im **normalen Geschäftsverkehr** ist.

c) Die Referenzierung der UID-Einheit im geregelten Zertifikat gemäss UIDG vom 18.6.2010 ist ein starker „Added Value" für ein geregeltes Zertifikat. Es ist aber notwendig, dass dies in einer Weise geschieht, welche die **Interoperabilität mit bestehenden Identifikator-Systemen zur Identifikation von Zertifikatshaltern** gewährleistet. Dies können etwa private Schemen sein, die im automatisierten B2B-Verkehr genutzt werden (z.B. **GS1 GLN** od. **D&B D-U-N-S**). Zu beachten ist auch, dass auch Privatpersonen UID-Einheiten sein können und somit eine UID besitzen. Hier muss eine klare Unterscheidung zu Nummerierungs-Systemen für Privatpersonen (z.B. **SuisseID-Nr**.) möglich sein.
Die neue Verordnung und die Technischen Administrativen Vorschriften müssen deshalb verlangen:

Die zugehörige Identifikationsnummern (UID) müssen gemäss bestehenden internationalen Normen referenziert werden, sodass sie auch international automatisch ausgelesen und verwendet werden können; in Art. 20 des neuen ZertES sind die gesetzlichen Grundlagen gegeben. Beim Comité Européen de Normalisation (CEN) sind die notwendigen Standards vorhanden.

d) Begrüssenswert ist die Möglichkeit, ein geregeltes Zertifikat auf irgendeine UID-Einheit ausstellen zu können. Dadurch kann auch eine einfache Gesellschaft (keine juristische Person), welche Mehrwertsteuer-pflichtig ist, ein geregeltes Zertifikat erhalten. Damit ist auch ein Problem der **Mehrwertsteuer-Verwaltung** gelöst und es **braucht kein spezielles Zertifikat**.

Mit freundlichen Grüssen

Adrian Müller
Otto Müller
14. Mai 2012