WILDHABER Consulting

Stellungnahme

zur Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur (VZertES) und zu den technischen und administrativen Vorschriften des BAKOM

Wildhaber Consulting
Dr. Bruno Wildhaber, CISA/CISM
Zimikerried 15
CH-8603 Schwerzenbach
Tel +41 1 826 21 21
Fax +41 1 826 21 22
bruno@wildhaber.com
www.wildhaber.com

Generelles

Wildhaber Consulting (www.wildhaber.com) ist ein Beratungsunternehmen mit dem Schwerpunkt Recht und Technologie in E-Business Systemen. Dr. Bruno Wildhaber war eingeladener Experte bei der Entwicklung des ersten Deutschen Signaturgesetzes (1997) und als Partner von r3 Security Engineering Organisator einer der ersten kommerziellen PKI Konferenzen im Jahr 1996. Dr. Wildhaber war in mehreren internationalen PKI Forschungsprojekten tätig und hat verschiedene nationale und internationale PKI Systeme mitgestaltet, u.a eines der ersten produktiven Identrus Systeme, eines PKI Verbundes in der Finanzindustrie, dessen Anforderungen über das europäische Signaturgesetzniveau hinausgehen.

Zur Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur (VZertES) und zu den technischen und administrativen Vorschriften des BAKOM nehmen wir wie folgt Stellung:

Die Verordnung und die technischen Ausführungsvorschriften sind für die Umsetzung des Signaturgesetzes absolut zwingend. Es muss unbedingt darauf geachtet werden, dass dort wo technische Verfahren direkte und wertmässig hohe Auswirkungen auf Rechtsgeschäfte haben, möglichst genaue und präzise Vorgaben existieren. Im vorliegenden Entwurf fehlen diese auf der Verordnungsebene - hier besteht dringender Korrekturbedarf.

Mit der Anlehnung der Bestimmungen an die neue Norm der ETSI wird der richtige Weg beschritten. Auf eine Beurteilung der ETSI Normen wird aus diesem Grund verzichtet. Die Regelungen der Schweiz sollten sich deshalb auf wesentliche, CH spezifische Aspekte, beschränken.

Bedeutung für den elektronischen Geschäftsverkehr

Wir machen darauf aufmerksam, dass es nicht sinnvoll ist, Anforderungen an Zertifizierungsdiensteanbieter zu stellen, die über das europäische Niveau hinausgehen. Es sollte Ziel der Behörden sein, den elektronischen Geschäftsverkehr wenn möglich zu fördern. Aus diesem Grund ist eine Anerkennung von internationalen Anbietern ohne grossen bürokratischen Prüfverfahren unbedingt zu ermöglichen.

Struktur und Aufbau der Regelwerke

Es war in der verfügbaren Zeit nicht möglich, die Abstimmung der einzelnen Vorschriften untereinander auf Vollständigkeit bzw. Lücken zu prüfen. Wir haben den Eindruck, dass dies nochmals überprüft werden sollte, zumal sich der Handlungsbedarf zur Beschreibung von Details auch aus den umfangreichen ETSI Normen ergibt. Der mehrstufige Aufbau führt zwangsläufig zu grossem Interpretationsspielraum und teilweise auch zu Kreisverweisen, wie z.B. in 1.4 Punkt 4. Aus diesem Grund wird auf eine detaillierte inhaltliche Beurteilung der technischen und administrativen Vorschriften verzichtet.

Konkrete Vorgaben zu Sicherheitskomponenten

Es ist zwingend, kritische Komponenten direkt zu beschreiben, wie dies auf Verordnungsebene ansatzweise versucht wird (z.B. in Art. 12). Hier gibt es bei verschiedenen Punkten Handlungsbedarf (Beschreibung der Signaturkomponenten). Als derzeit international gültige Zertifizierungskriterien kommen dabei primär die Common Criteria und/oder ITSEC zum Zug. Als gutes Beispiel dient die Verordnung zum Deutschen Signaturgesetz, SigV vom 16.11. 2001 (Beilage). Wir empfehlen, eine äquivalente Regelung 1:1 zu übernehmen.

Auszug:

Sichere Signaturerstellungseinheiten müssen unabhängig vom Einsatz und der Anwendung nach den Sicherheitskriterien "Common Criteria for Technology Security Evaluation" (CC) [CC98] mit der Prüftiefe EAL 4 gegen ein hohes Angriffspotential und einer vollständigen Missbrauchsanalyse oder nach den "Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik" (ITSEC) [ITSEC91], [ITSEM94] mit der Prüftiefe E3 und in beiden Fällen mit der Mechanismenstärke "hoch" durch eine akkreditierte Prüfstelle geprüft und durch eine Bestätigungsstelle bestätigt werden.

Ohne diese Detaillierung ist es sowohl für Anbieter wie auch Anerkennungsstellen praktisch unmöglich, eine vernünftige Aussage zu den erforderlichen Sicherheitskomponenten zu machen.

Kommentare zur VZertES

Artikel	Anmerkung	Verbesserungsvorschlag
Art. 1	Die Schaffung von Anerkennungsstellen in einem so kleinen Markt scheint und unsinnig, da dies eine Kostenexplosion verursacht, zumal es sich jetzt um eine Norm handelt, die europäisch abgestützt ist. Das verhindert den Eintritt von Anbietern unnötig.	SAS anerkennt direkt, bzw. akzeptiert ausländische Anerkennungsstellen gemäss AkkBV; gestützt auf Zulassungen in Ländern, welche über eine, der CH vergleichbaren Signaturgesetzgebung, verfügen.
Art. 3 Abs. 1	Es fehlen ausreichend klare Anforderung an die Signaturerstellungseinheiten nach anerkannten Sicherheitskriterien (Common Criteria/ITSEC). Das gilt sowohl für Anbieter als auch Inhaber..	Angabe der notwendigen CC bzw. ITSEC Level gemäss Beispiel SigV (Deutschland)
Art. 3 Abs. 2	In den technischen Vorschriften fehlen die notwendigen Angaben, der Verweis auf ETSI genügt nicht	Eindeutige und klare Beschreibung der HEUTE zulässigen Geräte und Equipments mit Sicherheitsklassifikation (siehe SigV D). Regelmässige Anpassung entsprechend der technischen Entwicklung. Hier geht es u.a. um wesentliche Fragen der Haftung beim Inhaber und Anbieter.
Art. 5 Abs. 2	Die Frist von 6 Jahren erscheint eher lang	Reduktion auf 3 Jahre oder alternativ Re-Identifikation nach 6 Jahren

Artikel	Anmerkung	Verbesserungsvorschlag
Art. 6	Nicht nur die Aufbewahrung, sondern primär die Erstellung von Kopien muss verboten werden! Das ergibt sich auch aus den technischen Anforderungen in Art. 3	.... dürfen keine Kopien .... erstellen.
Art. 7	Man kann bei der Ungültigkeitserklärung keine hohen Identitätsnachweis verlangen. Zudem macht die Identifikation über einen möglicherweise kompromittierten Schlüssel keinen Sinn. Das ist ein Fehlkonzept, welches zwar aus Urzeiten der CPS Entwicklung stammt und sich offenbar widerspenstig hält, sich in der Praxis aber nicht bewährt hat (vgl. die Ausführungen zur Haftung!)	Eine Beschreibung der Berechtigungsprüfung ist nicht notwendig, deren Umfang muss dem Anbieter überlassen werden. Viel wichtiger ist eine Regelung, welche beschreibt, wer wie lange haftet, sollte ein Missbrauch geschehen. Man greife hier auf die Praxis der Banken beim Management von EC Karten zurück. Mitteilung über alle möglichen Kanäle -- Sofortige Sperrung – Aufzeichnung; Haftung des Schlüssel (Karten)inhabers bis zur Meldung.
Art. 12	Die Anforderungen sind ungenügend spezifiziert. Eine Passwortlänge von 4 Stellen galt bereits vor 10 Jahren als unsicher, heute müsste man fast von Klartext reden. Begrüsst wird die explizite Nennung von Biometrie als Alternativmittel für die Authentifikation.	Beibehalten der Regelung; aber ausführliche Beschreibung notwendig, basiert stark auf den technischen Anforderungen gemäss Art. 3. Bei Einsatz von Passworten sind die Minimalanforderungen: 6 Stellen; keine Wörter aus Wörterbüchern
Art. 13 Abs. 1	Diese Regelung ist nicht konform mit der Haftungsverteilung gemäss ZertES. Entweder ist hier keine Frist anzugeben oder die Anbieterin regelt das selbst. Auf jeden Fall muss der Inhaber aber sofort melden. **Bei Nichtmeldung trägt er das Haftungsrisiko.**	.... muss sie SOFORT ..... Klare Zuweisung des Haftungsrisikos,
Art. 13 Abs. 2	Hier müssen alle Fälle erwähnt werden,die einen Haftungsfall auslösen können, z.B. genügt der blosse Verdacht, dass der Schlüssel missbraucht wurde als ausreichender Grund für die Melde- bzw. Sperrpflicht.	Erweiterung der Gründe und klare Zuweisung des Haftungsrisikos

Kontakt: Bruno Wildhaber, bruno@wildhaber.com, Tel. 01 826 21 21

