AWK Group
Consulting and Engineering

BAKOM
Bundesamt für Kommunikation
Herr Peter Fischer
Zukunftsstrasse 44
Postfach
2501 Biel

16. Juli 2004 Ga

AWK Group
**Stellungnahme zur Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur und technische und administrative Vorschriften**

Sehr geehrter Herr Fischer

Für die Einladung zur Stellungnahme in obiger Angelegenheit danken wir Ihnen bestens.

Die AWK Group hat grosses Interesse an einer praxistauglichen und anwenderfreundlichen Verordnung für Zertifizierungsdienste. Unseres Erachten muss die Verordnung unbedingt die folgenden übergeordneten Anforderungen erfüllen:

- Sicherheit der Zertifikate gewährleisten
- Verbreitung von Zertifikaten nicht erschweren:
  - Zertifikatsbezug muss für Benutzer möglichst einfach möglich sein
  - Hürden für einen ZDA (Zertifizierungsdienst-Anbieter) dürfen nicht zu hoch angesetzt werden
  - Europäischen Anbietern darf der Markteintritt nicht unnötig erschwert werden (Anlehnung an europäisches Umfeld)

Die Stellungnahme im Anhang beinhaltet unter anderem auch unsere Erfahrungen aus verschiedenen Projekten, wie zum Beispiel:

- Konzipieren und Realisieren von *Public Key Infrastructure* (PKI) für Kantonsverwaltungen
- Studie für das Bundesamt für Justiz *„Braucht die Schweiz einen amtlichen digitalen Ausweis?"*
- Business-Plan für eine öffentliche PKI in der Schweiz (Auftraggeber war die IG tOP, ein Verein, bestehend aus interessierten Kreisen aus Verwaltung und Privatwirtschaft)

AWK Group · Leutschenbachstrasse 45 · Postfach · CH-8050 Zürich · Tel. +41 44 305 95 11 · Fax +41 44 305 95 19
info@awkgroup.com · www.awkgroup.com

Unsere Stellungnahme lassen wir Ihnen wunschgemäss auch elektronisch zugehen an die Adresse digsig@bakom.admin.ch und ermächtigen Sie ausdrücklich zur Publikation auf Ihrer Website.

Für allfällige Rückfragen stehen wir Ihnen jederzeit gern zur Verfügung:


| | | |
|---|---|---|
| Patrik Rüegge | Direktwahl 01 305 95 64 | patrik.rueegge@awkgroup.com |
| Peter Gabriel | Direktwahl 01 305 95 60 | peter.gabriel@awkgroup.com |


Mit freundlichen Grüssen
AWK Group

Peter Gabriel
Partner

Patrik Rüegge
Technologiemanager Sicherheit

# Stellungnahme der AWK Group zur Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur (VZertES)

*Allgemeine Bemerkungen*

Wir haben nur die VZertES geprüft. Auf eine Prüfung der technischen und administrativen Vorschriften haben wir verzichtet.

*Artikel 1*

Für den begrenzten Schweizer Markt muss unseres Erachtens nicht zwingend eine akkreditierte Anerkennungsstelle geschaffen werden. Hingegen ist es zwingend, die Kriterien für eine Anerkennung sowie das Vorgehen (z. B. in den technischen und administrativen Richtlinien) explizit für alle Bereiche (Gebäudeinfrastruktur, Hardware, Software, notwendige Zertifizierungen, Prozesse) aufzuführen. Entsprechend ist ein Verweis auf diese Ausführungen notwendig.

*Artikel 2, Absatz 1*

Der Versicherungsschutz pro Fall erscheint hoch. Ist dieser Betrag mit dem europäischen Umfeld abgestimmt?

*Artikel 7, Absatz 1*

Die Ungültigerklärung im Falle des Verlusts des Zertifikates ist nicht geregelt. Sinnvoll ist auch eine möglichst schnelle Meldung analog der Sperrung einer Kreditkarte im Verlustfall. Bewährt hat sich eine Helpdesk–Nummer mit 7 x 24 h Zugang. Die Haftungsansprüche beim Verlust des Zertifikats können dann ähnlich dem Bankenumfeld gestaltet werden.

*Artikel 10, Absatz 2*

Die Übernahme der Liste der geführten Zertifikate wird für einen anderen ZDA bzw. die Anerkennungsstelle mit Kosten verbunden sein. Es sollte definiert werden, wie die Entgeltung für diese Weiterführung zu handhaben ist (Rückstellungen beim ZDA, Versicherung für diesen Fall oder ähnliches).

Es fehlt die Definition der Pflicht zur Übernahme und Weiterführung / Publikation der fremden Liste für einen ZDA.

In diesem Zusammenhang: Was passiert, wenn die Stelle, welche einen ZDA zertifiziert hat, ihren Dienst einstellt? Muss sich der ZDA neu zertifizieren lassen? Eine entsprechende Regelung haben wir nicht gefunden.

*Artikel 11*

Die Pflichten des Inhabers eines Signaturschlüssels sind weitreichender als jene eines ec-Karten-Inhabers, die lediglich eine Trennung von PIN und Karte notwendig machen. Analoge Pflichten sollten hier definiert werden, entsprechend Artikel 12, Absatz 5.

Die Anforderungen an den Träger eines Signaturschlüssels sollten unseres Erachtens definiert werden (sind Soft-Zertifikate zugelassen bzw. ausgeschlossen?).

*Artikel 12, Absatz 1*

Ein Passwort sollte mindestens 6 Zeichen (alphanumerisch) umfassen. Ein Passwort aus 4 Zeichen bietet keinen adäquaten Schutz mehr.

*Artikel 13:*

Das Meldeverfahren sollte genauer definiert werden. Zudem fehlen Pflichten des ZDA, welche Infrastuktur er zu betreiben hat (Helpdesk) und welche Mittel zur Identifikation angewendet werden müssen (siehe auch Artikel 7).