

Stellungnahme zum Entwurf für eine Verordnung über eine Public Key Infrastruktur in der Schweiz

Stellungnahme von Dr. Bruno Wildhaber, Wildhaber Consulting, Zimikerried 15, 8603 Schwerzenbach, Tel. +41 1826 21 21, www.wildhaber.com
bw@wildhaber.com

Gleichzeitig Stellungnahme der Information Systems Audit and Control Association Switzerland Chapter (ISACA).

Thema 1: Wünschbarkeit einer obligatorischen Root

Die obligatorische Root Instanz macht dann Sinn, wenn man die ursprünglich vorgesehene Hierarchie gemäss Standardisierungsvorschlägen (X.500) realisieren oder vergleichbaren Beispielen (wie in Deutschland) folgen will. Die Vor- und Nachteile müssen an dieser Stelle nicht umfänglich aufgezeigt werden. Gegen eine mehrstufige Hierarchie spricht in jedem Fall das sich aufbauende Schadenspotential. Je länger die Zertifizierungskette, desto grösser der potentielle Schaden bei Ausfall einer Top Instanz. Will man diesen Weg gehen, bedeutet dies, dass die Anforderungen an die Root sehr hoch gesteckt werden müssen. Die Ca's müssten hohe Anforderungen erfüllen. Die notwendigen Fallback Szenarien müssen gestaltet und umgesetzt werden. Dieses System mag dann sinnvoll sein, wenn man die Digitale Signatur als tatsächliches Surrogat für die eigenhändige Unterschrift einsetzen kann. Da dies in der Schweiz nicht geplant ist, bzw. nur die freie Beweiswürdigung gilt, ist von einer Reglementierung der Zertifizierungsinstanzen grundsätzlich abzusehen, da der Nutzen für die Benutzer fehlt. Die Beweiskraft der Digitalen Signatur wird mit dem geplanten System nicht gewährleistet. Schon aus diesem Grund muss die Reglementierung auf einem minimalen Mass gehalten werden. Die vorgeschlagene Verordnung entspricht damit nicht der EU Direktive zur Digitalen Signatur welche fordert, dass die Mitgliedstaaten dafür zu sorgen haben, dass die Digitale Signatur der eigenhändigen gleichgestellt wird.

Zusammengefasst ergibt sich:

- a) hierarchische Systeme werden sich nicht oder nur vereinzelt durchsetzen (Haftungsproblematik),
- b) die obligatorische Root kann nicht für die rechtliche Beweiskraft der Digitalen Signatur garantieren,
- c) der Nutzen für den Anwender und die Betreiber von PKI's ist nicht gegeben.

In diesem Sinn ist auf die Einrichtung einer obligatorischen Root zu verzichten.

Thema 2: Rolle des BAKOM

Auch wenn keine obligatorische Root geschaffen werden muss, kann das BAKOM die Rolle des Wegbereiters wahrnehmen und Certification Bodies bezeichnen, welche die CA Anbieter auf ihre Konformität mit internationalen Standards überprüfen. Dies vor allem im Zusammenhang mit der Cross Certification im öff.-rechtlichen Bereich. Insofern ist die vom BAKOM vorgeschlagene Struktur sinnvoll und zu übernehmen.

Solange die gesetzliche Anerkennung der digitalen Signatur fehlt, können die Anforderungskataloge auf den gängigen Vorschriften der Fachorganisationen im Bereich Informationssicherheit basieren. Im privaten Umfeld werden sich die Best Practices oder Vorgaben der jeweiligen Organisationen durchsetzen. In jedem Fall ist nach der Zulassung eine regelmässige Kontrolle der PKI Parteien (CA, RA, DIR, Time Stamping) vorzusehen, idealerweise durch spezialisierte Experten (Informatik Revisoren oder Sicherheitsexperten).

Fazit:

Die Verordnung sollte sich gegenwärtig nur auf den öff.-rechtlichen Bereich beschränken da die Inkraftsetzung nur eine Belastung der Wirtschaft ohne einen ausreichenden Nutzen darstellt.