Signaturgesetz mit L(T)ücken

Das Bundesgesetz über die elektronische Signatur weist problematische Lücken auf. Dadurch werden Anwendungen erheblich eingeschränkt und die Umsetzung des Gesetzes erschwert.

Am 19. Dezember 2003 wurde das Bundesgesetz über die elektronische Signatur (ZertES) verabschiedet, wann es in Kraft treten wird, ist noch offen. Das Gesetz soll sichere Dienste der elektronischen Zertifizierung fördern und die Verwendung qualifizierter Signaturen begünstigen (Art. 1). Die Absicht ist nobel, doch bleiben beim Einsatz von elektronischen Signaturen im E-Business und E-Government weiterhin Stolpersteine vorhanden, denn folgende Punkte sind für die Förderung der elektronischen Signaturen kontraproduktiv:

- Qualifizierte Zertifikate sind nur für natürliche Personen möglich.
- Nicht standardisierte Autorisierungsinformationen müssen ins Zertifikat aufgenommen werden.
- Etwelche Identitätskennungen im Zertifikat, wie die E-Mail-Adresse, sind vielleicht nicht zwingend zu überprüfen.
- Die Abfrage der Revokationsliste kann kostenpflichtig gestaltet werden.
- Die Angaben bezüglich der Revokationszeit eines Zertifikats sind unpräzise.
- Der Betrieb eines Verzeichnisdienstes ist nicht obligatorisch.
- Einige wesentliche Punkte sind im Gesetz noch gar nicht geregelt.

Qualifizierte Zertifikate nur für natürliche Personen

Damit die elektronische Signatur in Zukunft die entsprechende Rechtswirkung gemäss Obligationenrecht entfaltet, muss sie mittels eines öffentlichen Schlüssels in einem qualifizierten Zertifikat verifiziert werden können. Die Anforderungen an ein qualifiziertes Zertifikat sind in Art. 7 festgelegt. Unter anderem darf ein qualifiziertes Zertifikat nur für eine natürliche Person ausgestellt werden; insbesondere nicht für einen Server oder eine juristische Person. Damit werden E-Business mit elektronischen Signaturen wie das Internetbanking oder E-Government-Anwendungen durch dieses Gesetz nicht geregelt. Dies ist ein Manko. Vielleicht wollte der Gesetzgeber erreichen, dass Rechtsgeschäfte mit Automaten unterbunden werden. Doch bereits heute kann man beispielsweise Fahrkarten, Esswaren oder Geld beim Automaten beziehen.

Diese Bestimmung hat noch einen weiteren Haken: Um die Echtheit der Zertifikate zu prüfen, ist der öffentliche Schlüssel der Zertifizierungsstelle (CA, engl. Certification Authority) erforderlich. Deswegen wird ein Zertifikat mit dem öffentlichen Schlüssel der CA ausgestellt und den Benutzern mitgegeben (siehe Abbildung S. 44).

Doch die CA wird im Normalfall wohl durch eine juristische Person (Aktiengesellschaft) verkörpert. Hielte man sich also an den Wortlaut des Gesetzes, dann könnten mit den bisher bekannten Verfahren gar keine Zertifikate gesetzeskonform auf deren Echtheit geprüft werden.

Autorisierungsinformationen im Zertifikat

Die Autorisierungsinformationen im qualifizierten Zertifikat (Art. 7 Abs. 2 lit. c) sind einerseits nicht konform zu den technischen Standards. Deswegen müssen Anpassungen bei der Auswertung und der Darstellung der Zertifikate bei den Sicherheitsapplikationen vorgenommen werden. Anderseits bringt die Information, wie der maximale Wert pro Transaktion, nicht mehr Sicherheit. Die maximale Anzahl Transaktionen pro Tag kann nämlich nicht beschränkt werden. Somit können Tausende von Transaktionen gestartet werden; der maximale Wert pro Transaktion ist zwar beschränkt, doch der daraus resultierende maximale Schaden nicht.

Identitätskennung eventuell nicht zu prüfen

Art. 8 Abs. 1 schreibt vor, dass sonstige Angaben zur Person von der zuständigen Stelle zu bestätigen sind. Präziser wäre, vorzuschreiben, dass insbesondere alle ins Zertifikat aufgenommenen Identitätskennungen wie etwa die E-Mail-Adresse zu prüfen sind. Erfolgt dies nicht, kann die Authentisierung umgangen werden.

Unverzügliche Revokation

Die Ungültigkeitserklärung eines Zertifikats wird als Revokation bezeichnet. Die Revokation eines Zertifikats hat gemäss Gesetz unverzüglich zu erfolgen (Art. 10 Abs. 1). Heisst dies nun, innerhalb von 10 Minuten nach Eingang des Antrages zur Revokation? Muss ein Betrieb mit einer Verfügbarkeit von 365x24 Stunden pro Jahr angeboten werden? All diese wirtschaftlich wichtigen Fragen bleiben mit der Formulierung «unverzüglich» unbestimmt.

Abfrage der Revokationsliste kostenpflichtig?

Die für ungültig erklärten Zertifikate werden in einer sogenannten Revokationsliste aufgeführt. Diese Liste muss allgemein zugänglich publiziert werden. Damit die Gültigkeit eines Zertifikats geprüft werden kann, muss die Sicherheitsapplikation anhand dieser Liste unter anderem prüfen, ob das Zertifikat nicht revoziert worden ist. Wird die Abfrage dieser Liste für Private kostenpflichtig gestaltet (implizit aus Art. 11 Abs. 3), so werden die Sicherheitsapplikationen mit grosser Wahrscheinlichkeit so konfiguriert, dass die Anzahl Anfragen nach einer aktuellen Liste minimiert wird, um Kosten zu reduzieren.

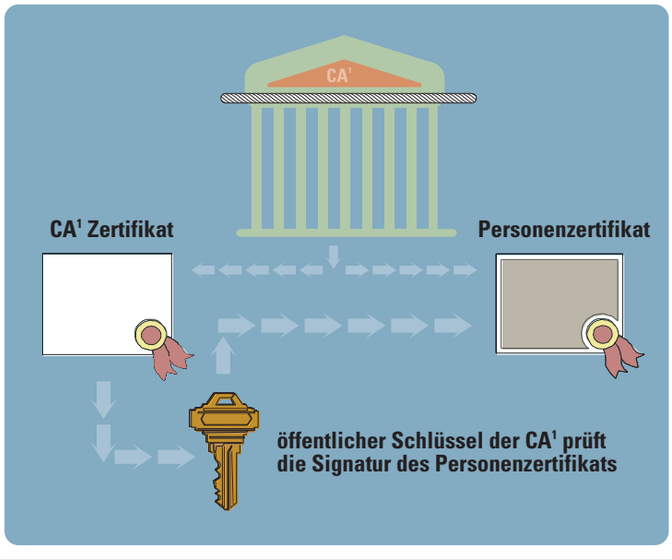
Erfolgt nun die Publikation der aktuellen Liste zum Beispiel um 14 Uhr, frägt aber die Sicherheitsapplikation die Liste erst um 20 Uhr ab, dann bleibt aus Sicht der Sicherheitsapplikation ein um 14 Uhr für ungültig erklärtes Zertifikat bis 20 Uhr gültig. Somit kann von 14 bis 20 Uhr weiterhin auf Basis dieses Zertifikats Missbrauch betrieben werden, obwohl die Revokation grundsätzlich unverzüglich erfolgt ist (siehe Abbildung S. 45).

Zudem ist nicht geklärt, wer für einen allfälligen Missbrauch in der erwähnten Zeitspanne haftet.

Verzeichnisdienst nicht obligatorisch

Ein Verzeichnisdienst ist eine Datenbank, welche die qualifizierten Zertifikate publiziert. Deren Publikation erfolgt nur auf Verlangen des Inhabers (Art. 11 Abs. 2). Das Führen eines solchen Verzeichnisdienstes ist also fakultativ (Art. 11 Abs. 2). Wird ein Verzeichnisdienst nicht geführt, dann wird aber die vertrauliche E-Mail-Kommunikation unter Umständen erschwert. Man mag einwenden, dass das Gesetz nicht für die vertrauliche Kommunikation gedacht ist, doch gibt es Bereiche, wo neben der authentisierten zusätzlich die vertrauliche

Der Zertifikatverifizierungsprozess



1) CA = Zertifizierungsstelle (Certification Authority)

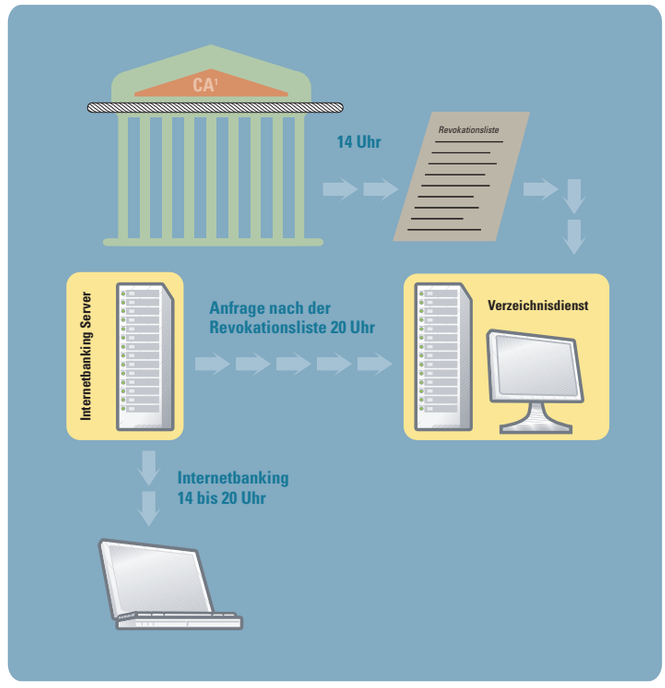
Kommunikation erforderlich ist, wie beispielsweise beim E-Mail-Austausch zwischen Kunde und Bank, Arzt oder Anwalt, oder beim E-Mail-Verkehr zwischen Behörde und Privaten, insbesondere zwischen Justiz und Anwälten.

Wesentliche Punkte nicht geregelt

Unter anderem vier Punkte bleiben zudem im Gesetz weiterhin unklar:

- Die Aufbewahrung und Verifikation digitaler Unterschriften nach Ablauf oder Ungültigkeitserklärung des Zertifikats: Wie werden die elektronischen Signaturen geprüft, wenn das entsprechende Zertifikat für ungültig erklärt worden ist, und welche Gültigkeit weist die Signatur nach der Ungültigkeitserklärung des Zertifikats auf?
- Angenommen, der private Schlüssel der CA, welcher für die Herstellung der Zertifikate verwendet wird, ist bekannt. Dann müssen sämtliche Zertifikate für ungültig erklärt werden, weil die Echtheit der Zertifikate und somit auch die Herkunft der elektronischen Signatur nicht mehr geprüft werden kann. Was ist in diesem Fall von Seiten der CA zu unternehmen, und wer trägt die daraus entstehenden Kosten?

Beispiel einer Zertifikatsrevokations-Zeitlücke



1) CA = Zertifizierungsstelle (Certification Authority)

- Muss die CA Rückstellungen vornehmen und diese speziell ausweisen, damit sie bei Einstellung der Geschäftstätigkeit infolge Konkurses den allfälligen Verpflichtungen aus Art. 13 Abs. 2 nachkommen kann?
- In Art. 6 Abs. 3 werden die Anforderungen an die Sicherheitsapplikation bei der Prüfung der Zertifikate und der Signaturen festgelegt. Angenommen, die Sicherheitsapplikation erfüllt diese Bedingungen nicht und es entsteht ein Schaden. Wer trägt primär die Haftung dafür, der Benutzer, der Software-Hersteller oder der Verkäufer der Applikation?

Fazit

Zertifikatsdienste als Basis für die authentisierte, vertrauliche und geschützte Kommunikation mit sensitiven Daten machen durchaus Sinn. Damit dies schnell und benutzerfreundlich abgewickelt werden kann, muss aber der Betrieb eines Verzeichnisdienstes obligatorisch und die Abfrage der Revokationsliste kostenlos sein. Sämtliche ins Zertifikat aufgenommenen Identitätskennungen sind auf Richtigkeit zu prüfen.

Zertifikatsdienste für den Abschluss von langfristig gültigen Rechtsgeschäften wie ein Häuserkauf oder das Verfassen eines Testamentes machen wegen der fehlenden Anforderungen bezüglich nachhaltiger Prüfung von elektronischen Signaturen zudem wenig Sinn.

Autor: Daniel Muster, dipl. Physiker Universität Bern, NDS ETH Zürich, Autor des Buches «Digitale Unterschriften und PKI»