WORM -Archivierung versus Digitale Signaturen / PKI

In der Schweiz wurde die elektronische Signatur durch das „Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur“(vom 19.12.2003) sowie durch die „Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur (ZertDV vom 12. April 2000) geregelt.

Auch das Obligationenrecht sieht in Art. 14, Abs. 2 bis bzw. Art. 59a eine Gleichstellung von digitalen Zertifikaten (ZertES-konforme elektronische Signatur) und der handschriftlichen Unterschrift im Bereich gesetzlicher Formvorschriften vor. Dabei wird eine Haftung des Inhabers des Signierschlüssels für den sorgfältigen Umgang mit dem Schlüssel (*PKI-Schlüssel*) vorausgesetzt. In diesem Zusammenhang spielen die Kurzbezeichnungen *ZertES*, *VZertES* und die entsprechende OR-Gesetzesartikel eine wichtige Rolle, die per 1. Januar 2005 in der Schweiz in Kraft gesetzt wurden.

Gegenüber der *EU-Signaturrichtlinie* liegen hier aber wesentlicher Unterschiede zur Regelung darin, dass für eine Rechtswirkung der erwähnten obligationenrechtlichen Normen jeweils die *Anerkennung* (EU-Terminologie: *Akkreditierung*) des jeweiligen Zertifizierungsdienstes durch eine *Anerkennungsstelle* vorausgesetzt wird. In der Schweiz braucht es also die gesetzeskonforme elektronische Signatur eines *anerkannten* Zertifizierungsdienstes, während in der EU nur eine gesetzeskonforme Signatur vorausgesetzt wird und die Akkreditierung damit freiwillig bleibt.
Die Anerkennung bzw. Akkreditierung ist eine Bestätigung dafür, dass der *Zertifizierungsdienst* die Anforderungen des Gesetzes erfüllt.

Die *Schweizerische Akkreditierungsstelle (SAS)* publiziert eine Liste der anerkannten Zertifizierungsdienste, welche derzeit die folgenden Firmen umfasst (Stand: Juli 2007):

- Swisscom Solutions, QuoVadis Trustlink Schweiz,
- SwissSign AG der Schweizerischen Post
- Bundesamt für Informatik und Telekommunikation (BIT)

Diese Firmen oder staatlichen Stellen sind anerkannte Anbieter von Zertifizierungsdiensten in der Schweiz. PKI-basierte Zertifikatsschlüssel, die von diesen Stellen signiert wurden, gelten entsprechend auch als digitale Unterschrift bei der Archivierung von e-Maildaten und signierten Dateispeichern.

Im Gegensatz dazu wird die WORM-Disk [i] in den meisten Ländern als „zertifizierter Datenspeicher für die Langzeitarchivierung“ und als „revisionssicherer elektronischer Datenspeicher“ eingesetzt und gerichtlich anerkannt. Das Verfahren zur Aufzeichnung von Daten auf diesem Speichermedium ist weltweit rechtlich abgesegnet und entspricht den gängigen Vorschriften.
Die von neuen von HP entwickelten WORM UDO-Disk erreichen derzeit Speicherkapazitäten von rund 30 GB, sind günstig in der Anschaffung (ca. CHF 90.- pro Stück) und können in sogenannten UDO-Jukeboxen mit Kapazitäten bis ca. 10 Terrabyte betrieben und verwaltet werden.
Die dabei verwendeten Aufzeichnungsverfahren entsprechen weitgehend den WORM-Standards, es gibt aber auch sogenannte wiederbeschreibbare Versionen (RW-Disks).

Die Hauptunterschiede dieser beiden Verfahren bestehen darin, dass PKIs für alle e-Mailbedürfnisse eingesetzt werden können:

- für digitale Signaturen
- zur Verschlüsselung von Mails und Beilagen
- zum Aufbau von VPN-Verbindungen zur Firma
- zur zertifizierten Archivierung von Maildaten

PKI-basierte Zertifikate werden als in den operativen Businessprozessen eingesetzt. Der Benützer kann sie aktiv einsetzen, sie im täglichen Anwendungsbereich und für verschiedene Aufgabenstellungen einsetzen.
Die betrieblichen Rahmenbedingungen für die IT-Abteilung sind etwas aufwendiger, weil die dazu notwendigen Infrastruktursysteme betrieben werden müssen (siehe Darstellung 6-2 im Kapitel 6, „Sicherheit“).

WORM-Disks sind hingegen ausschliesslich eine technische Angelegenheit der IT-Abteilung. Hier handelt es sich um komplette, mit Hardware-Systemen integrierte Lösungen zur Datenarchivierung. Der Benützer wird selten oder gar nie mit diesen Mitteln zu tun haben.

Tatsache ist aber, dass das eine oder das andere Verfahren bei der e-Mailarchivierung zum Einsatz gelangen sollte, damit die geforderte rechtssichere Archivierung technisch und operativ korrekt erfolgt. Es können selbstverständlich auch beide Verfahren in Kombination eingesetzt werden. Damit wäre dann die „erhöhte Sicherheitsstufe“ erreicht, bei der aber, auch aus IT-betrieblicher Sicht, die komplexesten Aufwendungen und Implementierungsvarianten zum Einsatz kommen.

[i] WORM = **W**rite **O**nce **R**ead **M**any. WORM-Datenträger können nur einmal beschrieben werden, sind dann aber beliebig oft lesbar. Ein WORM-Laufwerk besitzt zwei verschiedene Laserstrahlen. Einen zum Lesen der Datenträger und einen intensiveren zum Schreiben der Daten.
WORM-Datenträger sind mit einer kristallinen oder polykristallinen Beschichtung überzogen. Wenn der Schreibstrahl auf die Oberfläche trifft, wird die Beschichtung geschmolzen oder verdampft. Die geschmolzenen Stellen kühlen sehr schnell ab, wodurch sich die Atome der Beschichtung nicht in ihrer ursprünglichen Struktur anordnen. Sie besitzen deshalb ein anderes Reflexionsvermögen als die Oberfläche. Beim Lesen des Datenträgers tastet der schwächere Laser die Oberfläche ab. Ein Sensor nimmt die reflektierten Strahlen auf und wandelt sie in Bit-Werte um.
Die Langzeitarchivierung und die Haltbarkeit der Daten werden dabei auf bis zu 40 Jahre garantiert. Damit weisen sie eine bedeutend längere Lebensdauer als magnetische Speichermedien auf.
WORM-Disks haben in der Regel eine Speicherkapazität von 3.5 - 25 GByte pro Seite der Disk, wobei die mittlere Zugriffszeit mit ca. 35-50 ms via SCSI-Schnittstelle eher als langsam bezeichnet werden muss. Die Datenübertragungsrate ist (im Vergleich zu anderen modernen Speichermedien) mit 2.1 – 5.6 MByte/s eher gering. Oft werden moderne Laufwerke dieser Art als UDO-Laufwerke bezeichnet.

Dieses Speichermedium und die dabei eingesetzten Standards werden demnächst durch die *Holographic Versatile Disc* (HVD) abgelöst (siehe oben), welche bedeutend leistungsfähiger ist und sich preislich nur wenig von einer WORM-Disk unterscheidet. Die rechtlich anerkannte Beweispflicht der Unveränderbarkeit von gespeicherten Daten auf dieser Disk, ist derzeit in Bearbeitung.