Aktuelle Standards von Verschlüsselungstechnologien & Verzeichnisdienste

Sicherheitstechnische Standards und ihre Einsatzverfahren / Beurteilung beim Einsatz mit e-Mail:

Verschlüsselungsverfahren	Status	Empfehlung
Single DES Algorithmus	Unsicher, gilt als „geknackt“	Sollte raschmöglichst mit höherwertigem Standard ersetzt werden, weit verbreitet
Triple-DES / 3-DES Algorithmus	Noch sicher, gilt als „noch nicht geknackt“	Kann für gewisse Einsätze im e-Mailumfeld nicht verwendet werden
AES Verschlüsselung	Neuer Standard, gilt als „sehr sicher“ weil öffentlich, nicht US-kontrolliert	Dieser Standard ist anzustreben, wird aber noch nicht von allen Herstellern eingesetzt/unterstützt
MD5 Hashwerte	Gilt teilweise als sicher, ist aber „knackbar“ [i]	Genügt für „kurzlebige“ Verschlüsselungsverfahren, nicht für Langzeitarchivierung geeignet, kann mit e-Mails verwendet werden
SHA-1 Hashwerte	Gilt als sicher	Wurde durch die amerikanische NSA entwickelt, kann im Zusammenhang mit e-Mails verwendet werden
X.509 nach PKCS-Standards	Gilt als sicher, international standardisierte Verfahren, hohe Akzeptanz in Sicherheitskreisen	Vermutlich beste Verschlüsselungsstufe, in Kombination mit AES und SHA-1, meist aufwendig in der Implementierung, benötigt zusätzliche Systeme, geeignet für VPN-Tunnels
SSL/TLS Verfahren	Gilt als sicher, weit verbreitet, gilt als international standardisiertes Verfahren	Gutes Standardverfahren für sichere Datenverbindungen via Internet, geeignet für sichere Web-Mailverbindungen, nur bedingt geeignet für VPN-Tunnels

Tabelle 1: Sicherheitsstandards und ihre Einsatzmöglichkeiten

Verschlüsselungsverfahren können den e-Mailverkehr, die Archivierung und die Verwaltung von Informationen und Daten, speziell bezüglich der rechtlichen Vorgaben, entscheidend verbessern. Heute sollten deshalb im Zusammenspiel zwischen e-Mailarchivierung, Compliance-Richtlinien und Sicherheit, in der Datenkommunikation verschiedene der oben genannten Sicherheitsstandards in beliebiger Kombination eingesetzt werden können.

Typische Verschlüsselungsverfahren vergleichend dargestellt:

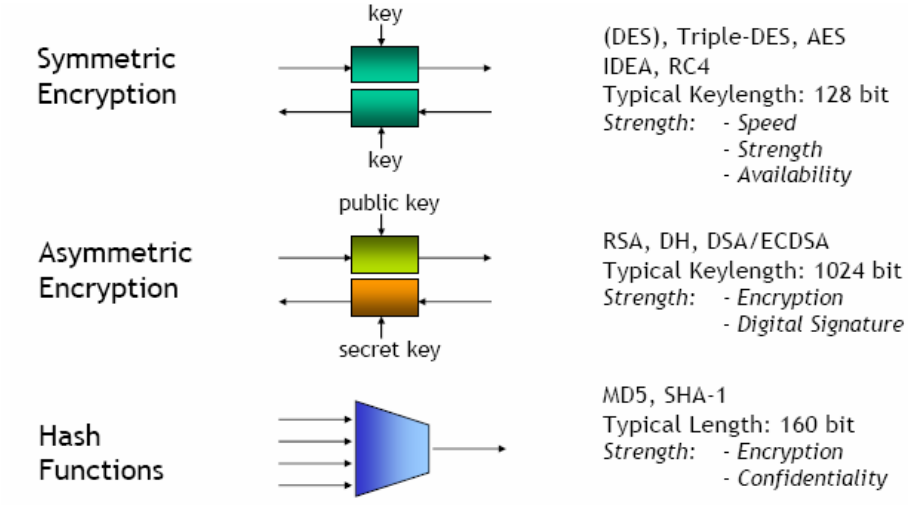

Abbildung -1 : Verschiedene kryptografische Verschlüsselungsmethoden

Grundlagen zum Einsatz von PKI-basierten Zertifikaten

Zertifikatsdienste benötigen nun eben diese Service-Funktionen, damit die entscheidenden Elemente von PKI-Zertifikaten (wie sie zur e-Mailverschlüssung häufig eingesetzt werden) optimiert zum Einsatz gelangen können. Anforderungen an Zertifikate sind dabei (siehe auch Kap. 15, e-Mailstandards):

Sicherheitsanforderung	**Technische/operationelle Massnahme**
Unveränderbarkeit / Fälschungssicher	durch Verschlüsselung
Transparenz und Rückverfolgbarkeit der e-Mailkommunikation	mit Authentifizierung
Eindeutige Identifikation	Identifikation Sender/Empfänger über digitale Unterschrift
In elektronischer/digitaler Form reproduzierbar/ herstellbar	digitale Signatur / digitales Archiv
Versand/Empfang nicht abstreitbar	Nachvollziehbar / unveränderbar archiviert

Ein Windows Domain-Controller kann nun durch die bereits im Betriebssystem und dem ADS integrierten Dienste der „Certificate Authority“ leicht erweitert werden. So kann mit geringem Aufwand und mit relativ einfachen Mitteln für jeden Benützer das notwendige Zertifikat erstellt werden, wie es zum Versand und zur Verschlüsselung von e-Mails verwendet wird.

Eine typische PKI-Umgebung funktioniert ungefähr so, wie in der untenstehenden Abbildung dargestellt (in diesem Fall auf der Basis von Smart-Cards mit Crypto-Chip als Datenträger für die PKI-Zertifikate) .

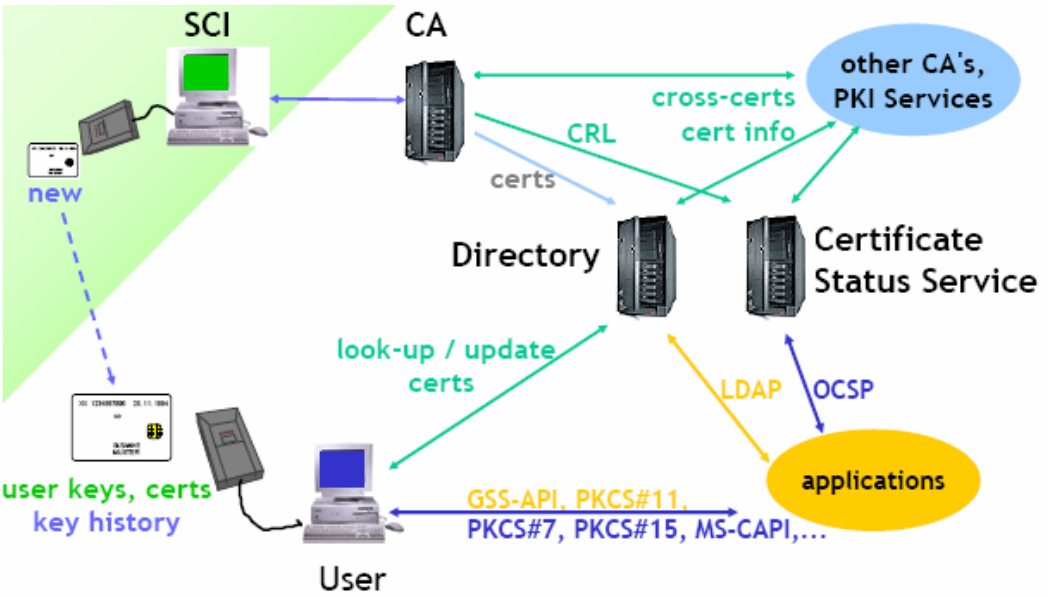

Abbildung 2 : ICT-Infrastruktur und notwendige Systeme für den Einsatz von PKI-basierten Chipkarten

Abkürzungen:

SCI	Smart-Card Interface System zur Erstellung von PKI-Chipkarten
CA	Certificate Authority
CRL	Certificate revokation list zur Sperrung von ungültigen oder verfallen Zertifikaten
LDAP	Light-weight Directory Access Protocol als Verzeichnisdienst und zur Login-Kontrolle von Benützern sowie für die e-Mailadressierung
OCSP	Online Certificate Status Protocol für die sofortige Prüfung eines präsentierten Zertifikates
PKCS	Public Key Cryptography Standards [ii] für den Einsatz von PKI-Zertifikaten im Zusammenhang mit den zu kontrollierenden Applikationen-Loginprozessen

Ein weiterer Baustein des aktiven e-Mail-Managements und der Datenarchivierung bilden in diesem Zusammenhang der Einsatz von verschlüsselten Mailarchiven. Eine falsche Handhabung kann hier verheerende Folgen haben oder limitierte Möglichkeiten für den operativen Einsatz darstellen. Daneben gilt es die Vorschriften des Datenschutzes einzuhalten.

Die zentrale Frage der Schlüsselverwaltung und deren Handhabung müssen eindeutig nach Vorgaben der Geschäftsleitung geklärt und durch konkrete Vorgaben formuliert werden.

- Sollen PKIs zusammen mit den Mailboxen auch über längere Perioden gespeichert werden oder werden alle Mails ohne PKI-Verschlüsselung archiviert?
- Wie muss die Verwaltung und der Einsatz von „ungültigen Zertifikaten“ erfolgen (z.B. von Mitarbeitern, die das Unternehmen verlassen haben, in eine andere Verantwortungsstufe gewechselt haben oder den PKI-Schlüssel verloren haben)?
- Welche Technologie soll für den Einsatz von Zertifikaten zum Einsatz gelangen (Chip-Karten, USB-Dongle, biometrischer Leser, etc.)

In der Schweiz wurde die elektronische Signatur durch das „Bundesgesetz über Zertifizierungs-dienste 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 [iii] 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 Kosten für diese Medien sind relativ gering. Weitere Details zu Backup-/Archiv-Medien sind in den e-Beilagen enthalten.

Die Hauptunterschiede dieser beiden Verfahren bestehen darin, dass PKIs auch für alle anderen 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 also in mehreren operativen Businessprozessen eingesetzt. Der Benützer kann sie somit aktiv im täglichen Anwendungsbereich und für verschiedene Aufgabenstellungen einsetzen. Die betrieblichen Rahmenbedingungen für die IT-Abteilung sind dadurch jedoch etwas aufwendiger, weil die dazu auch die notwendigen Infrastruktursysteme betrieben werden müssen (siehe Darstellung im Kapitel „Sicherheit“).

Verzeichnisdienste und deren Eigenschaften (Directory Services)

Hier eine etwas umfassendere Betrachtung von zusätzlichen IT-Diensten, die in einer modernen Informatikumgebung mit berücksichtigt werden müssen:

- Identitiy Management / Identity Access Management
- Directory Services / Active Directory (ADS) / LDAP / Meta-Directories
- Access / Security Group Policies

Diese Aufgaben werden heute mehrheitlich durch zentral administrierte und verwaltete Lösungen zur Verfügung gestellt, sogenannte „Directory Services“ [iv]. Die am meisten verbreitere und bei KMUs häufig zentral eingesetzte Lösung ist der Microsoft Active Directory Service (ADS) welcher sich im Microsoft-Umfeld seit Windows 2000 zum Standard durchgesetzt hat. Daneben sind die heute aus dem Linux-Umfeld bekannten Dienste des „Light Weight Directory Protocols (LDAP)“ weit verbreitet und weitgehend als „Standard-Dienst“ zu bezeichnen. ADS und LDAP können sehr gut zusammenarbeiten und stellen eine koordinierte Verwaltung von Benützern, Objekten und Diensten in einem Netzwerk sicher.

Glossarium und Quellenhinweise für weitere Informationen

Unter den hier aufgeführten Quellen und Internet Links finden Sie weitere Erklärungen und Darstellungen zu den hier behandelten Begriffen und technischen Standards.

Teilweise wird auch auf Unterlagen von nicht direkt öffentlich zugänglichen Quellen verwiesen. Der Autor hilft auf Anfrage weiter und gibt Auskünfte zu den verwendeten Unterlagen.

---

[i] Der Sicherheitsexperte Bruce Schneier diskutierte in seinem Blog die Unsicherheitsfaktoren von MD5
http://www.schneier.com/blog/archives/2005/03/more_hash_funct.html

[ii] PKCS-Standards für den Einsatz mit PKI-Zertifikaten
http://www.rsa.com/rsalabs/node.asp?id=2124

[iii] 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.

[iv] *Directory Services* sind Dienste, die Benützer, Objekte und Rechte zentral in einer Domäne verwalten und anderen Diensten/Servern die entsprechenden Informationen, Zugriffsrechte oder Zertifikate zur Identifikation und Zugriffsberechtigung zur Verfügung stellen.
Beispiele: Microsoft Active Directory Services; OpenLDAP Services.
Eine weiterentwickelte Form dieser Dienste sind die sogenannten *Meta-Directories*, die für mehrere unterschiedliche Applikationsumfelder und Betriebssysteme grenzüberschreitend Identität und Autorisierung übernehmen können und als zentrale Verwaltungsinstanz in einem Netzwerk dienen.
http://www.techweb.com/encyclopedia/defineterm.jhtml?term=directoryservice
http://www.goldmann.de/grundlagen-meta-directory_tipp_66.html