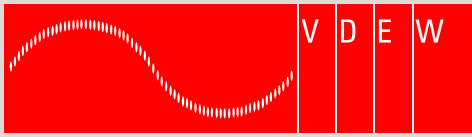
VDEW

MATERIALIEN

M-08/2005

Unternehmensübergreifende PKI-Topologien, PKI-Dienste und Einsatzrahmenbedingungen



Verband der
Elektrizitätswirtschaft e.V.

Unternehmensübergreifende PKI-Topologie, PKI-Dienste und Einsatzrahmenbedingungen

Anforderungen und Empfehlungen aus Sicht der deutschen Elektrizitätswirtschaft

Oktober 2005

Beate Becker, Telefon: 030/726147-209, Mail: beate_becker@vdew.net

Ergänzend zu den Gesetzen und Rechtsvorschriften für den Einsatz der elektronischen Signatur und der Verschlüsselung haben die Verbände eine gemeinsame Erklärung zu „Sicherheitsrahmenbedingungen für den elektronischen Geschäftsverkehr im deutschen Strommarkt" abgegeben. Diese stellt die Basis für die Bildung einer Vertrauensinfrastruktur der Marktteilnehmer beim elektronischen Datenaustausch dar und zeigt Maßnahmen zur Sicherheit auf. Dadurch wird das Sicherheitsniveau auf der technischen und organisatorischen Ebene nachhaltig gehoben.

Das vorliegende Dokument soll die zwingenden technischen und organisatorischen Maßnahmen prinzipiell beschreiben, die aus Sicherheitsgesichtspunkten heraus zur Teilnahme am Verfahren zum sicheren elektronischen Datenaustausch nötig sind. Die Komplexität der dabei entstehenden oder wenigstens denkbaren Topologie orientiert sich an einem Szenario.

Zwingende technische Maßnahmen stellen die Orientierung am Standard ISIS-MTT dar. Entscheidend ist natürlich auch die Veröffentlichung der Zertifikate. Für die Verschlüsselung wird vor dem Versand der öffentliche Schlüssel des Kommunikationspartners benötigt; für die Signaturvalidierung wird nach dem Versand der öffentliche Schlüssel benötigt. ISIS-MTT schreibt für beide Methoden getrennte Schlüsselpaare vor.

Ziel dieses Dokumentes ist es, das Anforderungsverständnis zu unterstützen und zu einem sicheren, interoperablen, normgerechten und nicht zuletzt wirtschaftlichen Datenaustausch zu führen.

Im letzten Kapitel werden die rechtlichen, technischen und organisatorischen Anforderungen an die wichtigsten Stützprozesse aufgezeigt.

VDEW

Verband der
Elektrizitätswirtschaft e.V.

Unternehmensübergreifende

PKI-Topologien, PKI-Dienste

und Einsatzrahmenbedingungen

Anforderungen und Empfehlungen aus Sicht der deutschen Elektrizitätswirtschaft

VDEW-Projektgruppe „Sicherheit beim elektronischen Datenaustausch“

Version: 1.0

STAND: 31. OKTOBER 2005

INHALT

1 Verbandspolitische Vorgehensweise zum Aufbau von Sicherheitsrahmenbedingungen

Die VDEW-Projektgruppe „Sicherheit beim elektronischen Datenaustausch“ hat zur Gewährleistung einer sicheren Kommunikation zwischen den Marktteilnehmern in der deutschen Elektrizitätswirtschaft eine gemeinsame Erklärung zu "Sicherheitsrahmenbedingungen für den elektronischen Geschäftsverkehr im deutschen Strommarkt“ zwischen den beteiligten Verbänden angeregt. Die Erklärung wird von folgenden Verbänden getragen:

- Bundesverband der Deutschen Industrie e. V. - BDI, Berlin
- VIK Verband der Industriellen Energie- und Kraftwirtschaft e. V., Essen
- Verband der Elektrizitätswirtschaft - VDEW - e.V., Berlin
- Verband der Netzbetreiber - VDN - e.V. beim VDEW, Berlin
- Verband der Verbundunternehmen und Regionalen Energieversorger in Deutschland - VRE - e. V., Berlin
- Verband kommunaler Unternehmen - VKU - e.V., Köln

Diese Erklärung bildet die gemeinsame Basis, damit die Sicherheitsbelange im Geschäftsverkehr in der Branche angemessen berücksichtigt werden. Die Erklärung auf der verbandspolitischen Ebene wird durch entsprechende Dokumente im organisatorischen und technischen Umfeld ergänzt und ausgestaltet. Diese Dokumente werden vom VDEW erarbeitet und veröffentlicht.

Allgemein definiert haben die organisatorischen Teile den Anspruch, ein einheitliches organisatorisches Sicherheitsniveau bei der Verschlüsselung und Signatur von unternehmensübergreifenden Transaktionen zwischen den Marktteilnehmern zu gewährleisten.

Ebenso allgemein definiert sollen die technischen Teile der Dokumente auch beim Einsatz unterschiedlicher Produkte oder Dienstleistungen die Interoperabilität auf der technischen Ebene sicherstellen.

Die politischen, organisatorischen und technischen Aussagen in der gemeinsamen Erklärung und seinen Folgedokumenten haben Empfehlungscharakter und sollen in der Solidargemeinschaft der Marktteilnehmer eine verlässliche Vertrauensinfrastruktur ermöglichen.

Die Maßnahmen sollen als Leitlinie bei der Umsetzung im eigenen Unternehmen und der nachfolgenden Anwendung an den Marktschnittstellen dienen. Allerdings sollen gegenüber den Verbandsempfehlungen geänderte Vorgehensweisen begründbar sein und das allgemeine Sicherheitsniveau nicht beeinträchtigen.

Die Marktteilnehmer sollten aus wirtschaftlichen Gründen daran interessiert sein, dass die Vertrauensinfrastruktur nicht ausgehöhlt wird. Nur dadurch ist die sichere elektronische Abwicklung der Geschäfte mittelfristig gewährleistet und kann so ausgebaut werden, dass auch weitere Automatisierungsschritte beherrschbar bleiben.

2 Elektronischer Geschäftsverkehr in der Verbandsarbeit

Der VDEW empfiehlt seinen Mitgliedsunternehmen die Anwendung von Electronic Data Interchange (EDI)-Verfahren mit den in der Projektgruppe „Marktschnittstellen“ erarbeiteten und verbandsweit empfohlenen Nachrichtenformaten, die im UN/EDIFACT- und XML-Standard zur Verfügung stehen und unter www.strom.de veröffentlicht sind. Weil dabei im Strommarkt die bisher übliche Schriftform durch eine elektronische Form ersetzt wird, sollte zwischen den Kommunikationspartnern ein EDI-Rahmenvertrag abgeschlossen werden. Ein solcher Vertrag ist auf EU-Ebene definiert worden und liegt in seiner ersten Fassung bereits seit 1994 in deutscher Übersetzung vor. Er legt in europaweit standardisierter Form die rechtlichen Bedingungen und Vorschriften fest, denen die Parteien bei der Abwicklung von Transaktionen mit Hilfe des elektronischen Datenaustausches unterliegen.

Mittlerweile werden zum Datenaustausch zunehmend keine Festverbindungen oder X.400-Verbindungen genutzt, sondern es wird z. B. per E-Mail über preiswertere Internetverbindungen kommuniziert. Die zunehmend bessere Dienstgüte rechtfertigt diese Vorgehensweise, allerdings müssen bei der Kommunikation über ein offenes Netz entsprechende Vertraulichkeits-, Integritäts- und Authentizitätsanforderungen berücksichtigt werden.

In einem EDI-Vertrag zwischen Marktpartnern sollten diese Anforderungen abgedeckt werden können, ohne dass jeweils bilaterale Absprachen getroffen werden müssen.

Die VDEW-Projektgruppe „Sicherheit beim elektronischen Datenaustausch“ hat zum Einsatz von elektronischer Signatur zur Gewährleistung von Datenintegrität und Absenderauthentizität und zum Einsatz von starker Verschlüsselung zur Gewährleistung von Vertraulichkeit beim elektronischen Datenaustausch Dokumente erarbeitet, die dazu geeignet sind, als technische und organisatorische Referenzdokumente für den Bereich Datensicherheit zu dienen und damit einen EDI-Vertrag zu ergänzen. Auf Verbandsebene haben sie empfehlenden Charakter. Erst in einem bilateralen oder multilateralen Vertrag werden sie rechtlich bindend, wenn alle Vertragspartner sie als Vertragsgrundlage akzeptieren. Ebenso wie die empfohlenen EDI-Marktschnittstellen, die Interoperabilität auf Anwendungsebene gewährleisten, gewährleisten sie Interoperabilität und vergleichbares Niveau auf der Sicherheitsebene.

Die politischen, organisatorischen und technischen Aussagen haben Empfehlungscharakter und sollen in der Solidargemeinschaft der Marktteilnehmer eine gemeinsam genutzte Vertrauensinfrastruktur ermöglichen.

Mit dem Zweiten deutschen Signaturgesetz von 2001 und Folgegesetzen entstanden erweiterte gesetzliche Möglichkeiten, die elektronische Form im Geschäftsverkehr einsetzen zu können. Dabei hat der Gesetzgeber die „Gesetzlich elektronische Form“, also im weitesten Sinn das Urkundenwesen, im Formanpassungsgesetz, im Verwaltungsverfahrensrecht und für die elektronische Rechnung als formgebundene Urkunde im Umsatzsteuerrecht geregelt.

Geschäftliche Transaktionen fallen rechtlich unter die formfreien Vereinbarungen. Das Projekt VEDIS, Verbindlichkeit und Sicherheit im Electronic Data Interchange, möchte Empfehlungen aussprechen, wie die „vereinbarte elektronische Form“ im liberalisierten Strommarkt ohne aufwendige neue Absprachen verbindlich gewährleistet werden kann.

Neben Verschlüsselung sollen elektronische Signaturen eingesetzt werden, die eine Identifizierung des Unterzeichners sowie die Erkennung nachträglicher Veränderungen der Daten ermöglicht und ausschließlich dem Unterzeichner zugeordnet sind. Dies leisten fortgeschrittene Signaturen.

Die explizite Aufführung der qualifizierten elektronischen Signatur in den Dokumenten ist nicht notwendig, da diese sowieso die gesetzliche Schriftform und damit auch die freiwillige Schriftform erfüllt.

Die entstehenden Infrastrukturen sollen aber offen für weitere Einsatzfälle und Anwendungen sein, die über die Kommunikation zwischen den Marktteilnehmern hinausgehen.

Aus diesem Grund hat sich VEDIS, unabhängig von der Durchsetzbarkeit, nicht für eine brancheninterne und hierarchische Lösung entschieden. Der liberalisierte Markt und seine Kommunikationsanforderungen zwischen den Marktteilnehmern lieferte den Anstoß für die Verbandsarbeit. Abzusichernde Geschäftsbeziehungen erstrecken sich aber auf viele weitere elektronische Kommunikationsbeziehungen zu Kunden, Partnern, Zulieferern, Dienstleistern und zunehmend auch auf elektronische Behördenkontakte.

Das vorliegende Dokument soll Anforderungen, Auswirkungen und Lösungsansätze aufzeigen und Empfehlungen aussprechen.

3 Anforderungen und ihre topologischen Auswirkungen

3.1 PKI-Grundprinzipien und resultierende Anforderungen im eigenen Haus des Marktteilnehmers

Bevor ein unternehmensübergreifender Einsatz angestrebt werden kann, sind zunächst die unternehmensinternen Voraussetzungen zu schaffen. Es geht bekanntlich um die Tatsache, dass in Zukunft zur Absicherung des Datenaustauschs kryptographische Schlüssel verwendet werden sollen. Diese Schlüssel werden paarweise eingesetzt. Ein Schlüsselpaar ist mathematisch untrennbar miteinander verbunden: ein Schlüssel ist geheim zu halten, der andere Schlüssel ist öffentlich, z. B. wie eine Telefonnummer öffentlich sein kann. Die eindeutige Zuordnung zwischen öffentlichem Schlüssel (und damit Schlüsselpaar) und Person wird durch ein Zertifikat bescheinigt. Den organisatorischen Teil dieses Prozesses, nämlich die Identitätsüberprüfung der Person, wird Registrierung genannt. Den technischen Teil, nämlich die Bescheinigung einer vertrauenswürdigen Instanz - des Trustcenters - dass Schlüssel, technische Angaben und Personenangaben zusammengehören, heißt Zertifizierung.

Mit den Schlüsselpaaren werden die beiden grundsätzlichen Operationen einer Public Key Infrastruktur, nämlich Verschlüsselung von Daten und elektronische Signatur, getätigt.

Die Signatur hat dabei mehr Funktionen, als lediglich Ersatz der handschriftlichen Unterschrift zu sein. Vortäuschen falscher Identität, Manipulation am Dokument, Vortäuschen falscher Quelle, Fälschen des Transaktionsnachweises oder Fälschen des Zeitpunkts werden gleichermaßen damit ausgeschlossen.

Prinzip der Verschlüsselung:

Mit dem öffentlichen Schlüssel des Empfängers kann der Absender z. B. eine E-Mail verschlüsseln, die nur der Empfänger mit seinem geheimen (privaten) Schlüssel entschlüsseln kann. Daraus resultiert die „topologische“ Anforderung, dass der öffentliche Schlüssel des Adressaten beschafft werden muss.

Elektronische Signatur:

Umgekehrt kann mit dem privaten Schlüssel des Absenders ein Text verschlüsselt werden, der unzweifelhaft mit dem öffentlichen Schlüssel dem Absender zugeordnet werden kann. Allerdings wird heute immer ein eindeutiges, kurzes Abbild des Textes mit dem privaten Schlüssel verschlüsselt. Das Abbild wird mit einer sogenannten Hashfunktion erzeugt. Dieses Abbild wird deshalb als Hashwert bezeichnet. Der verschlüsselte Hashwert heißt elektronische Signatur und wird parallel zu den Daten mitgeliefert, unabhängig davon, ob auch noch Datenverschlüsselung angewendet wird oder nicht.

Es ist in höchstem Maß unwahrscheinlich, dass zwei Dokumente/Datensätze über eine Hashfunktion zum gleichen Hashwert führen. Deshalb kann der Empfänger den Hashwert

des Dokumentes selbst bilden, um ihn mit dem aus der Signatur gewonnenen Hashwert zu vergleichen. Sind beide gleich und wurde die Gültigkeit des eingesetzten Schlüssels überprüft, ist sicher gestellt, dass Echtheit der Herkunft und Unversehrtheit des Inhaltes gewährleistet sind. Die Gültigkeitsprüfung heißt Validierung. Sie stellt die „topologische“ Anforderung beim Einsatz elektronischer Signaturen dar.

Anforderungen im eigenen Haus:

Die interne Infrastruktur besteht nun darin, Schlüsselmaterial zu beschaffen und sich das rechtmäßige Eigentum in Form von Zertifikaten bescheinigen zu lassen. Weiterhin muss die Schlüsselaufbewahrung und kryptographische Verarbeitung durch Software und/oder Hardwarekomponenten gewährleistet werden.

Die erste Frage lautet oft „Make or Buy“. Hier wird häufig der Zwischenweg gewählt, dass die Registrierung der Mitarbeiter im eigenen Haus erfolgt, während die Generierung des Schlüsselmaterials und ihre Zuordnung zu Personenkennzeichen (Zertifizierung) an einen Zertifizierungsdiensteanbieter delegiert werden.

Die zweite Frage wird oft lauten: Gatewaylösung oder arbeitsplatzbezogene Lösung. Gatewaylösungen, die oft als virtuelle Poststellen bezeichnet werden, lassen einen organisatorisch einfachen Einstieg in PKI-Funktionen zu. Damit wird vor allem die unsichere Kommunikationsstrecke zwischen zwei Firmen/Instanzen, etwa über das Internet, abgesichert (Seite-zu-Seite). Arbeitsplatzbezogene Lösungen sind dagegen eine Ende-zu-Ende-Absicherung über die gesamte Kommunikationsstrecke zwischen zwei Punkten. Beide Ansätze lassen sich aber auch bedarfsorientiert kombinieren.

VEDIS empfiehlt dringend, kurzfristig wenigstens nicht über das Internet zwischen zwei Firmen ungesichert zu kommunizieren.

VEDIS hat als Interoperabilitätskriterium die Norm ISIS-MTT gewählt und der Einfachheit halber im Dokument „Technische PKI-Interoperabilität“ sogar dort etwas abgeschwächt, wo noch technische Probleme bei Produkten auftauchen können (z. B. Unterstützung deutscher Umlaute). Die zu beschaffende Software muss konform zu diesen Minimalanforderungen sein, was in den weitaus meisten Fällen der Fall sein wird.

Die VEDIS-Empfehlungen stellen dabei jedem Anwender frei, ob das geheime Schlüsselmaterial auf einer SmartCard aufbewahrt und dort auch die kryptographischen Berechnungen zur Verschlüsselung und Signatur durchgeführt werden, oder ob eine organisatorisch sichere Lösung mit Hilfe von Software gewählt wird.

Für einige Einsatzfälle, die im Allgemeinen nur bestimmte Arbeitsplätze betreffen werden, verlangt der Gesetzgeber zwingend SmartCards als sichere Schlüsselaufbewahrungs- bzw. Signaturerstellungseinheit. Dies betrifft Rechnungen, Emissionszertifikatehandel und formgebundene Verträge, die sogenannte qualifizierte Signaturen erfordern. Weiterhin betrifft es etwa die Steuerdatenübermittlung, wo die entsprechende Verordnung zwar sogenannte fortgeschrittene Signaturen zulässt, aber weitere Vorgaben, wie SmartCard-Einsatz, an die Rahmenbedingungen macht.

3.2 Konkrete Anwendungsfälle im unternehmensübergreifenden Einsatz

- **Zur Verschlüsselung für einen externen Kommunikationspartner müssen unternehmensfremde Zertifikate (die den öffentlichen Schlüssel enthalten) beschafft werden.**

  Es gibt zunächst die Anforderung, das fremde Zertifikat zu finden.

  Lösungswege:

  1) Direktbeschaffung vom Kommunikationspartner, möglichst über einen vertrauenswürdigen Weg (signiert), händischer Import in den sogenannten Zertifikatsspeicher der eingesetzten Software.

  2) Beschaffung über das Unternehmen des Kommunikationspartners:
  Hinweis auf der Homepage des Unternehmens, Ansprechpartner im Haus, externer Zertifizierungsdienstleister oder Link auf extern zugängliches Directory (LDAP (Lightweight Directory Access Protokoll) und/oder HTTP vollqualifizierte Abfrage über E-Mail-Adresse)

  3) Beschaffung über Serviceprovider:
  European Bridge-CA des TeleTrusT e.V., private Serviceprovider

  4) Neue Norm:
  Nutzung des Domain Name Service (DNS) zur Nutzung der LDAP-Server-Suche.

- **Eigenes Zertifikat veröffentlichen**

  1) Generelle Hinweise: Verzeichnishinweise sollten immer über die eigene Homepage gefunden werden können (Vorschlag www.evu.de/pki). Dies gilt sowohl für das eigene Stammzertifikat (Root-CA) zur manuellen Überprüfungsmöglichkeit über den Fingerabdruck als auch für Hinweise auf den Ort des Verzeichnisses von User-Zertifikaten (z. B. Link auf Verzeichnis des Zertifizierungsdiensteanbieters ZDA). Üblicherweise befinden sich an dieser Stelle auch Hinweise auf die verwendeten Sicherheits-Regeln (Policy). Detaillierte Rahmenanforderungen dazu, aus Sicht der gemeinschaftlichen Sicherheitsanforderungen, werden in den VEDIS-Dokumenten „Sicherheitspolitik (PKI-Policy)“, „Umgang mit Schlüsselmaterial“ und „PKI-Zertifizierungspolitik des VDEW (CP, Certificate Policy)“ gegeben.

  2) User-Zertifikate: Voraussetzung für die Kommunikation ist die Kenntnis der Identität des konkreten Kommunikationspartners in Form seiner E-Mail-Adresse (natürliche Person oder Instanz, z. B. mscons@evu.de). Ein öffentlicher Schlüssel muss zur Verschlüsselung und zur Signaturüberprüfung elektronisch beschaffbar sein. Eine automatisierte Beschaffung ist anzustreben. Dabei sollte die E-Mail-Adresse, aufgrund der weltweiten Eindeutigkeit, zentrales Suchkriterium sein. Automatisierte Beschaffung ist über folgende Wege empfehlenswert: Das Verzeichnis der eigenen öffentlichen Schlüssel muss über LDAP oder über http abrufbar sein. Dies ist z. B. über eine LDAP-Proxy-Funktionalität möglich. Zertifizierungsdiensteanbieter (ZDA)

müssen im Rahmen des Service Level Agreements (SLA) zur Veröffentlichung des Verzeichnisses verpflichtet werden.

- **Umgang mit Sperrlisten (CRL, Certificate Revocation List)**
  1. Laut CPS sollen CRL tagesaktuell sein.
  2. Die CRL liegen z. B. unter ldap://ldap.evu.de oder http://www.evu.de/pki/crl
  3. Das Zertifikatsfeld CRL-Distribution Point (CDP) sollte eine URL auf diesen Ort enthalten (siehe VEDIS-Dokument „Technische PKI-Interoperabilität“).
  4. Zwischenspeicherung der CRL bis zu einem Tag kann Transaktionskosten reduzieren.

- **Weitere Infrastrukturmaßnahmen für unternehmensübergreifende sichere Kommunikation**

  Authentifizierung

  Marktbeobachter rechnen damit, dass technisch standardisierte Webservices zunehmend in unternehmensübergreifenden Portallösungen zum Einsatz kommen werden. Die sichere Authentisierung der Benutzer und die damit verbundene Zugangsberechtigung zu verteilten Funktionen und Ressourcen muss dabei gewährleistet sein. Hier wird Username/Passwort-Authentisierung zunehmend durch eine zertifikatsbasierte, starke Authentisierung ersetzt werden müssen, die im Rahmen von geeigneten Identity Management Maßnahmen verwaltet wird.

- **Zertifikat eines signierten Mails überprüfen**

  Jedes Unternehmen sollte seinen Mitarbeiterinnen und Mitarbeitern, die in unternehmensübergreifende sichere Geschäftsprozesse eingebunden sind, die technische Möglichkeit zur Verfügung stellen, signierte Mails zu empfangen, automatisch zu validieren und das Validierungsergebnis auch kenntlich zu machen.

- **Verschlüsselte E-Mail**

  Zur verschlüsselten Kommunikation mit einem externen Partner sollte sein aktuelles Verschlüsselungszertifikat aus dem veröffentlichten Bestand des Unternehmens verwendet werden, um sicherzustellen, dass immer aktuelles Schlüsselmaterial verwendet wird.

- **Dateisignatur**

  Mailverschlüsselung und -signatur wird als transportgebundene Sicherheit auf der SMTP-Ebene verstanden. Dabei sollte berücksichtigt werden, dass im S/MIME-Format Versender gleich Signierer ist. Zusätzliche Dateisignatur ist notwendig, wenn auf Dateiebene ein rechtsgültiger Verbindlichkeitsnachweis benötigt wird.

3.3 Das Szenario

Mittelfristig entstehen bei den Marktteilnehmern Anwendungen, die zertifikatsbasiert sichere, firmenübergreifende Transaktionen realisieren. Die erste Anwendung wird dabei zweifellos E-Mail (SMTP) sein. Diese Anwendungen beziehen sich nur zum Teil auf Transaktionen zwischen den Marktteilnehmern, die im Rahmen der Deregulierung relevant sind. Die dort verwendete Plattform („VEDIS-Plattform“) soll auch in anderen Geschäftsbeziehungen oder auch E-Governmentprozessen verwendbar sein.

Die technische Interoperabilität ist durch Anwendung internationaler Standards gemäß dem VDEW-Dokument „Technische PKI-Interoperabilität“ bezüglich ISIS-MTT und Definition der Zertifikatsinhalte gewährleistet.

Die organisatorische Sicherheit wird durch weitere Dokumente, wie die „PKI-Policy“ und „Umgang mit Schlüsselmaterial“ und das „des VDEW“ definiert.

Trotz dieser einheitlichen Rahmenbedingungen wird voraussichtlich in kurzer Zeit ein sehr heterogenes Gesamtszenario entstehen:

Gemäß den „Umsetzungsempfehlungen“ entscheidet sich eine Gruppe von Marktteilnehmern für die Einrichtung von „virtuellen Poststellen“. Andere entscheiden sich für den Aufbau einer eigenen PKI für bestimmte oder alle Arbeitsplätze. Die Zertifikate für beide Gruppen werden entweder bei öffentlichen Zertifizierungsdienstleistern bezogen oder gemäß den Sicherheitsanforderungen der VDEW-Empfehlungen selbst erzeugt.

Die „Trustcenter“ können gemäß deutschem Recht akkreditiert sein oder nicht; es können qualifizierte Zertifikate verwendet werden oder fortgeschrittene oder es können beide Zertifikatstypen parallel in einem Unternehmen oder gar bei einem Mitarbeiter vorliegen. Akkreditierte Trustcenter werden öffentliche Zertifizierungsdienstleister sein - vielleicht entschließt sich aber auch eine private Certification Authority zur Anzeige bei der Regulierungsbehörde für Telekommunikation und Post (RegTP)[1] - heute Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, um qualifizierte Zertifikate ausstellen zu können oder gar zur Akkreditierung, bei der dann zusätzlich die Root-CA der Bundesnetzagentur Wurzelinstanz in der Zertifizierungskette ist.

Es werden auch von ausländischen Zertifizierungsdienstleistern (akkreditiert oder nicht nach heutigem deutschem Recht) Zertifikate in der Branche verwendet werden können, wenn sie den Anforderungen der VDEW-Empfehlungen entsprechen.

Die Anforderungen an dieses Szenario sind gemäß den Ausführungen in Abschnitt 3.2 zusammengefasst folgende Punkte:

- Der Kommunikationspartner (besser: sein Zertifikat mit den öffentlichen Schlüsseln) muss gefunden werden können (z. B. wegen Verschlüsselung einer Nachricht an ihn).

[1] Mit dem Gesetz über die Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (Artikel 2 des Zweiten Gesetzes zur Neuregelung des Energiewirtschaftsrechts vom 7. Juli 2005 (BGBl. I S. 1970ff.) wurde die RegTP in Bundesnetzagentur umbenannt.

- Die Validierung, also die Überprüfung des Zertifikats auf Gültigkeit, muss sicher gestellt sein.
- Gemäß der zentralen Aussage in der gemeinsamen Erklärung der Verbände muss eine vertikale Interoperabilität zwischen qualifizierten und fortgeschrittenen Signaturen im Rahmen der VEDIS-Einsatzpotentiale gewährleistet sein.
- Festlegungen auf Standards dürfen keine Festlegungen auf einen Hersteller oder gar ein Produkt sein.
- Es muss nach wie vor ein offenes Teilnehmermodell sichergestellt sein, d. h. niemand wird zur Teilnahme an Diensten gezwungen, sondern muss lediglich technische Interoperabilität und organisatorische Sicherheitskriterien gewährleisten.
- Das Modell darf keine Marktausschlusskriterien enthalten, d. h. ein „Nein“ zu bestimmten Vorgehensweisen darf nicht unverhältnismäßig viele Ausschlusskriterien nach sich ziehen.
- Make- or Buy-Entscheidungen müssen prinzipiell offen sein. Dies gilt für technische Komponenten und für Dienstleister.

3.4 Ziel des Dokumentes

Das vorliegende Dokument soll einerseits die zwingenden technischen und organisatorischen Maßnahmen prinzipiell beschreiben, die aus Sicherheitsgesichtspunkten heraus zur Teilnahme am Verfahren zum sicheren elektronischen Datenaustausch nötig sind. Die Komplexität der dabei entstehenden oder wenigstens denkbaren Topologie orientiert sich an oben skizziertem Szenario.

Andererseits sollen Dienste beschrieben werden, mit denen Einrichtung oder Betrieb dieser Maßnahmen leichter bewerkstelligt werden können. Diese Dienste werden im Allgemeinen kostenpflichtig angeboten bzw. setzen die Mitgliedschaft in Organisationen voraus, sie dienen aber lediglich der bequemeren Implementierung und besonders dem bequemeren Betrieb.

Zwingende technische Maßnahmen stellen die Orientierung am Standard ISIS-MTT dar. Das Dokument „Technische PKI-Interoperabilität“ definiert einen sehr einfach gehaltenen Subset an Funktionalitäten bzw. Zertifikatsinhalten, der aus Interoperabilitätsgründen eingehalten werden muss. Dies ist bei Einsatz von Standardprodukten meist sogar schon in „Default-Einstellungen“ gewährleistet. Zwingend ist natürlich auch die Veröffentlichung der Zertifikate. Für die Verschlüsselung wird vor dem Versand der öffentliche Schlüssel des Kommunikationspartners benötigt; für die Signaturvalidierung wird nach dem Versand der öffentliche Schlüssel benötigt. ISIS-MTT schreibt für beide Methoden getrennte Schlüsselpaare vor.

In diesem Dokument ist die aktuelle ISIS-MTT Version 1.1 Arbeitsgrundlage. Weiterhin wurden die sich abzeichnenden leichten Veränderungen, die im Rahmen des deutschen Signaturbündnisses (AG Technik) diskutiert wurden, berücksichtigt.

In praktischen Tests erwies sich das ISIS-MTT Testbed als hilfreich, um zunächst bei einem Kommunikationspartner grundsätzliche Konformität mit der Norm zu erhalten. Halten sich Zertifikate und eingesetzte Produkte konform zu diesem Testwerkzeug, so ist auch in der bilateralen Kommunikation Interoperabilität wahrscheinlich oder kann leicht durch Parametrisierung erreicht werden.

Seit 2. November 2004 liegt ein ISIS-MTT Profil für Authentisierung vor.

Ziel dieses Dokumentes ist es, das Anforderungsverständnis zu unterstützen und zu sicherem, interoperablen, normgerechten und nicht zuletzt wirtschaftlichem Datenaustausch zu führen.

3.5 Weitere technische Interoperabilitätsaspekte

Der Inhalt der Zertifikate wird in dem Dokument „Technische PKI-Interoperabilität“ beschrieben. Zur Generierung der Zertifikate werden Sicherheitskriterien in der „PKI-Policy“ und im „PKI-Zertifizierungspolitik des VDEW (CP, Certificate Policy)“ dargestellt. Zur Beschaffung werden in den „Umsetzungsempfehlungen“ Hinweise gegeben.

Im erstgenannten Dokument werden 3 verschiedene Zertifikate empfohlen: Authentisierung, elektronische Signatur und Verschlüsselung. Das Authentisierungs- und Signaturzertifikat sind gemäß Empfehlung technisch gleich aufgebaut, um z. B. aus Kapazitätsgründen der SmartCard auf eines verzichten zu können. Der Unterschied besteht darin, dass z. B. bei einer SSL-Authentisierung kein Zugriff auf Verzeichnisdienstinformationen vorgesehen ist, sondern der Austausch Teil des Protokolls ist. Dies ist oft das Hauptargument für eine Trennung, da die Signatur eine bewusste Willenserklärung sein soll. Verschlüsselungszertifikat und Signatur- bzw. Authentisierungszertifikat unterscheiden sich gemäß Empfehlung insbesondere durch das Feld „Key Usage“ (keyEncipherment AND dataEncipherment bzw. digital Signature).

In jedem Fall findet bei zertifikats-basierten, sicheren Kommunikationsprozessen auch ein Austausch der Zertifikate statt. Dies kann und wird in einer Initialisierungsphase bilateral erfolgen. Allerdings ist es bei einer gewissen Komplexität und vor allem bei den unvermeidlichen Fluktuationen, die bei einer großen Zahl an teilnehmenden Firmen und Mitarbeitern auftreten, der Pflegebedarf nicht zu unterschätzen. Erfolgt die Pflege nicht mehr zeitnah, entstehen zwangsläufig Sicherheitslücken.

Während der Austausch von sogenannten End-Entity-Zertifikaten (Benutzer- und Serverzertifikate) in der Anfangsphase noch pragmatisch erfolgen kann, ist dies beim Austausch von CA-Zertifikaten (bzw. Root-CA) undenkbar. CA-Zertifikate sind zwingend erforderlich, um die gesamte Kette validieren zu können. Da diese als sicher akzeptierten CA-Zertifikate in der eigenen PKI anerkannt, also durch die eigene Root-CA signiert werden müssen, entsteht die Cross-Zertifizierungsproblematik, auf die im nächsten Kapitel eingegangen wird. Auch der unternehmensübergreifende Austausch von Sperrlisten (CRL) ist sicherheitskritisch.

Die Anforderung von (User-)Zertifikaten erfolgt mit dem Protokoll LDAP. Diese Anforderungsmöglichkeit muss technisch freigeschaltet werden (s. u.). Diese Anforderung darf aber nicht zu einer Sicherheitslücke und auch nicht zu einem Ausspähen des jeweiligen Unternehmens führen. Die Zertifikatsanfrage muss deshalb vollqualifiziert sein und damit maximal lediglich einen Treffer, nämlich das angeforderte Zertifikat, erzielen. Dies wird heute mit der weltweit eindeutigen E-Mail-Adresse (SMTP) erreicht, die häufig Bestandteil der Visitenkarte ist und als isolierte Information kein Firmengeheimnis darstellt. Allerdings sollte wegen der Spam-Problematik ein externer Abruf vieler E-Mail-Adressen nicht möglich sein. Die Möglichkeit, firmenfremde Zertifikatsanfragen zuzulassen, entspricht de facto einer Zertifikatsveröffentlichung in einem externen LDAP-Verzeichnis.

Die Validierung von Zertifikaten, insbesondere also die Überprüfung, ob das Zertifikat in der Sperrliste enthalten ist, erfolgt nach dem entsprechenden Eintrag im Zertifikat (CDP, Certificate Distribution Point). Sperrlisten werden entweder dezentral verteilt bzw. durch den Client importiert, wo sie von Anwendungsprogrammen angesprochen werden können. Ab einer gewissen strukturellen Komplexität ist dieser Vorgang aufwendig oder nicht mehr praktikabel. Alternative ist die zentrale Prüfung mit Hilfe des Online Certificate Status Protokolls (OCSP).

In der Regel werden dabei lediglich die für die Praxis notwendigen Status gültig, ungültig oder unbekannt zurückgemeldet. Bei mehreren oder gar vielen Zertifizierungsinstanzen ist es sinnvoll, jedes Zertifikat nur in dem Verzeichnis zu veröffentlichen, das der jeweiligen CA zugeordnet ist. Dies garantiert, dass eine zeitnahe Revozierung erfolgen kann, die bei redundanter Zertifikatsspeicherung erst zeitversetzt nachvollzogen werden müsste.

3.6 Keystatements

- **Zertifikate sollten öffentlich bzw. in einer geschlossenen Benutzergruppe zur Verfügung gestellt werden.**
- **Bei der Zertifikat-liefernden Stelle sollte dies in Form eines externen LDAP-Verzeichnisses geschehen.**
- **Eine unkontrollierte Öffnung des LDAP-Ports ist nicht wünschenswert, bzw. sicherheitskritisch.**
- **Es ist wünschenswert, dass eine Applikation (z. B. ein E-Mail-Client) ohne vorherigen expliziten und damit umständlichen Zertifikatsaustausch im laufenden Betrieb sich online das benötigte Zertifikat holen kann. Das Zugriffsprotokoll ist bevorzugt LDAP V3.**

4 PKI-Topologien

4.1 Vertikale Interoperabilität bei elektronischen Signaturen

Bereits mit dem ersten deutschen Signaturgesetz von 1997 wurde bei der Bundesnetzagentur eine Root-CA als Wurzelinstanz aufgebaut, die öffentliche Zertifizierungsdiensteanbieter, die sich einer freiwilligen Akkreditierung unterziehen, in einer 2-stufigen Hierarchie zertifiziert. Firmen-PKI haben sich bisher diesem Verfahren nicht unterzogen. Grund ist fast ausschließlich die Tatsache, dass die Kosten für den Einsatz qualifizierter Zertifikate besonders im Client-Bereich (Chipkarten, Chipkartenleser Class 3) gescheut werden. Trotz dieser wirtschaftlichen Vorbehalte sind die qualifizierten Zertifikate mit Anbieterakkreditierung von großer Bedeutung, weil nur damit „Urkunden“ signiert werden dürfen. Die betroffenen Bereiche im BGB hat das sogenannte Formanpassungsgesetz von 2001 geregelt, in dem die Anwendungsfälle im bürgerlichen Recht behandelt sind, wo die „Gesetzlich elektronische Form“ der Papierform gleichgestellt wurde.

VEDIS spricht Empfehlungen aus, wo die „vereinbarte elektronische Form“ vertraglich definiert werden muss, also Geschäfte elektronisch abgewickelt werden sollen (Geschäftsverkehr).

Hierbei werden im Energiemarkt fortgeschrittene Signaturen mit gewissen, in den VEDIS-Dokumenten empfohlenen Qualitätsmerkmalen an die Infrastruktur den qualifizierten Signaturen dahingehend gleichgestellt, dass die Marktteilnehmer beide Signaturvarianten als Verbindlichkeitskriterium im Rahmen der Transaktionen im Energiemarkt akzeptieren.

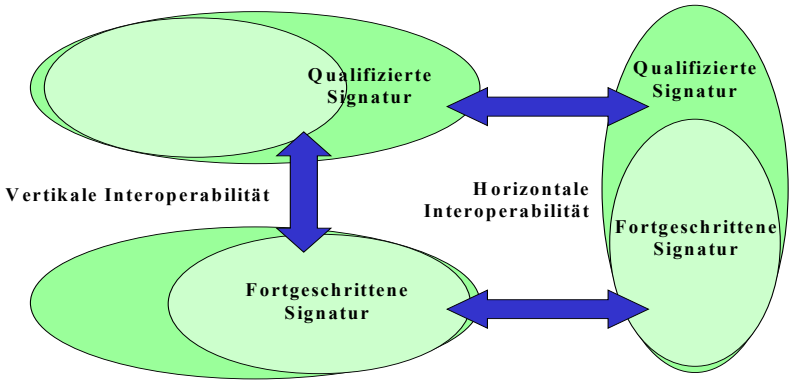
Technisch konfrontieren diese Anforderungen, mit der Notwendigkeit eine „Vertikale Interoperabilität“ zwischen fortgeschrittenen und qualifizierten Signaturen bzw. den eingesetzten Zertifikaten zu gewährleisten, um eine interoperable Verarbeitung sicher zu stellen. Dies ist prinzipiell möglich. Allerdings ist der Umgang mit fortgeschrittenen Signaturen in Verbindung mit international gängigen Standards und Produkten derzeit unproblematischer.[2]

4.2 Horizontale Interoperabilität

Weiterhin muss die „Horizontale Interoperabilität“ in nicht-hierarchischen Topologien gelöst sein. Die im VEDIS-Projekt betrachtete PKI-Thematik ist prinzipiell durch eine nicht-hierarchische Topologie gekennzeichnet. Mehrere bis viele PKI können und sollen koexistieren und kooperieren, ohne dass eine übergeordnete Instanz wieder Hierarchie herstellt. Nicht-hierarchische PKI-Topologien verlangen die Entscheidung, welche „Vertrauensanker“

[2] Technische Einzelheiten siehe Anhang 1

akzeptiert werden können und welche nicht. Viele Maßnahmen und Dokumente in VEDIS tragen dieser Tatsache Rechnung.



Vertrauensanker ist natürlich immer das Zertifikat der Zertifizierungsinstanz in der eigenen PKI, gleich, ob sie unter eigenem oder fremden Namen betrieben wird. Ein weiterer Vertrauensanker ist das Root-Zertifikat der Bundesnetzagentur.

Wurzelzertifikaten öffentlicher Zertifizierungsdiensteanbieter, die qualifizierte und fortgeschrittene Zertifikate signieren, können zumindest in Deutschland ebenfalls vertraut werden. Auch in Europa hat sich mittlerweile eine liberale Kryptopolitik durchgesetzt, die die kryptoanalytische Kontrolle, etwa durch Geheimdienste, weitgehend ausschließt. Dies kann international jedoch nicht verallgemeinert werden.

Insbesondere die VEDIS-Policy und das VEDIS-CP formulieren Anforderungen an Public Key Infrastrukturen, deren Wurzelinstanz im Geschäftsverkehr der Branche als Vertrauensanker akzeptiert werden können.

In Deutschland hat vor allem das Deutsche Forschungsnetz DFN wichtige Arbeit bei der nicht-hierarchischen PKI-Thematik geleistet. Hochschul-PKI werden nach dem Prinzip „Cross-Zertifizierung“ vernetzt, so dass vollständige Validierungsketten möglich werden. Bei der Cross-Zertifizierung erstellt jede Root-CA ein Zertifikat für den öffentlichen Schlüssel der jeweils anderen Root-CA, so dass jede CA dann zwei Zertifikate, nämlich das selbstsignierte und das fremdsignierte, besitzt.

Sobald mehrere Root-CA bzw. gleichberechtigte CA in der Topologie existieren, ist die Garantie und die Validierung der Vertrauensketten technisch anspruchsvoller. Dazu muss zuerst garantiert werden, dass auch das fremde Root-Zertifikat auf sicherem Weg bereitgestellt wurde und vor Manipulationen geschützt ist.

Dazu gibt es mehrere Möglichkeiten:

1) Root-Zertifikate werden in den Quellcode der Applikationen integriert. Dieser Weg wird z. B. bei WWW-Browsern verwendet.

2) Root-Zertifikate werden in die Applikationen integriert. Über ein spezielles User-Interface kann der Hashwert des Zertifikats angezeigt und manuell überprüft werden. Dieser Vorgang wird von den meisten Standardapplikationen unterstützt, z. T. über zentrale Update-Policies. Über die gleiche Schnittstelle ist auch eine automatische Validierung möglich.

3) Root-Zertifikate werden zusammen mit den privaten Schlüsseln in den SoftToken bzw. SmartCards der Nutzer gespeichert. Dabei wird der Zugriffsschutz der verwendeten Token als Vertrauensbasis genutzt. Dieses Vorgehen hat jedoch den Nachteil, dass neue Vertrauensanker nur bedingt in die vorhandenen Token integriert werden können.

VEDIS setzt aufgrund der wichtigen EDI-Kommunikationsbeziehungen vor allem auf die zweite Möglichkeit. Dabei sollte prinzipiell die manuelle und die automatische Validierung unterstützt werden. Grund ist die Tatsache, dass ein gültiges Zertifikat noch lange nichts über die Vertrauenswürdigkeit der PKI aussagt. Diese wird durch die PKI-Zertifizierungspolitik des VDEW (CP, Certificate Policy) und seine Einhaltung definiert.

4.3 Warum Sicherheit im elektronischen Datenaustausch

Der liberalisierte Strommarkt erfordert eine Fülle an Datenaustausch und damit geschäftliche Transaktionen zwischen den Marktteilnehmern. Der VDEW schätzt das Nachrichtenvolumen auf ca. 2´5 Milliarden EDI-Nachrichten pro Jahr.

Mit der Definition von sogenannten „Marktschnittstellen“ auf Basis von UN/EDIFACT- oder auch XML-Sprachmitteln wurde dem standardisierten Kommunikationsbedürfnis im Markt Rechnung getragen.

Die Risikominimierung in der normalen Geschäftspraxis stellt darüber hinaus einige Sicherheitsanforderungen.

- Man möchte sich auf die Inhalte verlassen können.
- Man möchte sicher sein, dass der Absender stimmt.
- Man möchte sicher sein, dass der Absender zu der Geschäftstransaktion steht bzw. dass eine Veränderung „unterwegs“ nicht möglich ist.
- Man möchte sicher sein, dass die Inhalte vertraulich bleiben.

Integrität, Authentizität, Verbindlichkeit und Vertraulichkeit bleiben also unverändert Grundanforderungen an geschäftliche Transaktionen. Ihre Wahrung bekommt aber beim elektronischen Datenaustausch oder gar Massendatenaustausch einen veränderten Stellenwert. Dies gilt für die Informationsgesellschaft generell und für den liberalisierten Energiemarkt im Besonderen.

Interessanterweise bestehen nicht nur Sicherheitsanforderungen aus einem reinen Schutzbedürfnis heraus. Viele Maßnahmen, z. B. bei Anforderungen an die Verbindlichkeit von Geschäftstransaktionen, sind Voraussetzungen für die Abwicklung der Transaktionen in elektronischer Form. Hier wird Sicherheit zum Business Enabler für den verstärkten Einsatz von Informationstechnik.

4.4 Übergang auf offene Netze

Im letzten Jahrzehnt wurden Maßnahmen zur Verbesserung der IT-Sicherheit vor allem auf die Intra-Enterprise Transaktionen angewendet. In diesem Zusammenhang entstanden auch erste firmeninterne Public Key Infrastrukturen. Für organisationsübergreifende Transaktionen wurden, wenn überhaupt, mehr transportgebundene, leitungsbezogene Sicherungsverfahren genutzt. Meist wurden ISDN-Wählverbindungen oder X.400-Boxen als ausreichend angesehen.

Durch die zunehmend bessere Dienstgüte und Verbreitung des Internets verlagern sich immer mehr geschäftlich relevante Kommunikationsverbindungen in dieses offene Netz. Transportgebundene Sicherungsverfahren, z. B. VPN-Tunnel, erweisen sich dabei außerhalb von Remote Access-Lösungen aber als relativ unflexibel. Asymmetrische Kryptographie und damit PKI-Mechanismen auf der Informationsebene ist deshalb vielfach das Mittel der Wahl, um z. B. auf E-Mail-Ebene und/oder Dokumentenebene Vertraulichkeit, Integrität und Authentizität über Firmengrenzen hinaus zu sichern.

4.5 Identität im E-Business

Elektronische Anwendungen haben alle grundsätzlich gleiche Phasen:

Anmeldung, Dateneingabe, Datenprüfung, Datenfreigabe, Verarbeitung und Speicherung.

Sicherheitsrelevant sind vor allem die Phasen:

- Anmeldung mit digitaler Identität als Authentisierung („Wer bin ich?“)
- Freigabe als Willenserklärung („Was will ich?“)
- Archivierung zur langfristigen Beweiswerterhaltung („Wie kam es an?“)

Sehr häufig wird die legitime Anmeldung auch auf die Datenfreigabe bezogen, was heute in den seltensten Fällen problematisch ist.

VEDIS möchte Authentizität und Verbindlichkeit im Hinblick auf weitere rechtliche und technologische Entwicklungen (z. B. Webservices) bereits heute möglichst logisch getrennt behandeln und empfiehlt unterschiedliche Mechanismen (3 zertifizierte Schlüsselpaare für Authentisierung und elektronische Signaturen plus Verschlüsselungsschlüssel), bei denen die ersten beiden Zertifikate allerdings gleich aufgebaut sein können.

4.6 Kryptographische Schlüssel, PKI

Der elektronische Geschäftsverkehr der Mitgliedsunternehmen in der deutschen Elektrizitätswirtschaft per Electronic Data Interchange oder anderer Verfahren soll sicherer und verbindlicher werden. Dazu wird im Rahmen einer firmenübergreifenden Vertrauensinfrastruktur zertifiziertes kryptographisches Schlüsselmaterial im Rahmen von Public-Key-Infrastruktur eingesetzt.

Mit dem Begriff "Vertrauensinfrastruktur" soll hier die Summe an technischen und organisatorischen Maßnahmen bezeichnet werden, die zwischen den Marktteilnehmern sichere und verbindliche Kommunikation und damit verlässlichen Geschäftsverkehr ermöglicht. Auch wenn technisch auf Standardlösungen zurückgegriffen wird, so muss sorgfältig mit dem kryptographischen Material (Schlüssel, PIN, Schlüsselträger) umgegangen werden (siehe das VEDIS-Dokument Umgang mit Schlüsselmaterial). Hier hat jeder Marktteilnehmer einerseits disziplinarisch durchsetzbare Regelungen zu schaffen. Andererseits sollte aber auch ein freiwilliges Sicherheitsbewusstsein bei den Mitarbeitern und Führungskräften gefördert werden.

4.7 Automatisierung

Für EDI-Transaktionen bis hin zur Netzentgeltrechnung lässt sich ein hoher Automatisierungsgrad erreichen. Selbst die Netzentgeltrechnung lässt sich vielfach nach Plausibilisierung mit vorliegenden Daten „durchbuchen“ ohne dass weitreichende manuelle Prüfungen erforderlich sind. Erfahrungsgemäß wird der erreichbare Automatisierungsgrad auch angestrebt. Dies ist aber bei geschäftlichen Transaktionen nur vertretbar, wenn durch angemessene Sicherheitsrahmenbedingungen auch bedenkenlos automatisiert, also ohne ständige menschliche Überwachung verarbeitet werden kann. Dies gilt besonders für die Transportqualität, um die man sich nicht ständig kümmern will. Geeignete Sicherheitsrahmenbedingungen, wie sie VEDIS vorschlägt, halten „den Rücken frei“ für weitere Automatisierungsschritte. Sie ermöglichen sichere organisationsübergreifende Geschäftsprozesse.

4.8 Wo und wie können die Zertifikate des Kommunikationspartners gefunden werden?

Sichere zertifikatsbasierte externe Kommunikation setzt externe Verfügbarkeit von eigenen und fremden Zertifikaten voraus. Die Verzeichnisse sollten der Einfachheit halber unter ldap://ldap.evu.de oder http://www.evu.de/pki liegen.

Eine Abfrage sollte per LDAP oder http(s) möglich sein. Die Abfrage sollte vollqualifiziert über die E-Mail-Adresse erfolgen können. Teilqualifizierte Anfragen, also sog. Wildcards sollten erst gar nicht unterstützt werden, um keinen Angriffspunkt für Spamming zu geben. Es sollten nur die 3 Attribute Common Name (CN), Mailaddress und Certificate bereit gestellt werden. Das Zertifikat kann über die weitaus meisten Client-Systeme auf einfache Weise in den Zertifikatemanager importiert werden. Damit lässt sich sofort eine E-Mail verschlüsseln

ohne zuvor in einem Dialogschritt vom Kommunikationspartner das Zertifikat bekommen zu müssen.

4.9 Wie werden die eigenen Zertifikate dem Kommunikationspartner zur Verfügung gestellt?

Es ist heute „State-of-the-Art“, dass Mitarbeiterdaten in einem zentralen Verzeichnis geführt werden. Dies reduziert den Pflegeaufwand erheblich und sorgt für Konsistenz. Werden zudem nach dem „Einbahnstraßenprinzip“ nur vertrauenswürdige Quellen, wie z. B. das Human Ressources System, benutzt, so ist auch die erforderliche Datenqualität gewährleistet. Dieses zentrale Verzeichnis ist auch der geeignete Ort, um intern Zertifikate zu speichern.

Über entsprechende Mechanismen (Shadowing/Chaining) kann ein Teil dieser Daten extern bereitgestellt werden, ohne Redundanzen in Kauf nehmen zu müssen.

Dieses externe Verzeichnis oder englisch Repository enthält mit Namen und E-Mail-Adresse unkritische, aber immerhin personenbezogene Daten von Mitarbeitern und sollte mit der Personalvertretung abgestimmt werden. An dieser Stelle sollten auch Sperrlisten liegen (ldap://ldap.evu.de bzw. http://www.evu.de/pki/crl). Die Sperrlisten (certificate revocation lists, CRL) sollten ebenfalls aus Datenschutzgründen keine Sperrgründe enthalten.

Das externe Verzeichnis sollte per LDAP oder http abrufbar sein. Die Suchbasis (LDAP-Attribut) soll leer sein. Die heute gebräuchlichen Client-Programme unterstützen durchweg LDAP, aber http nicht automatisch.

LDAP bzw. auch secure LDAP wird heute meist nicht standardmäßig durch Firewalladministratoren zugelassen, weil Sicherheitslücken befürchtet werden.

Die Firewall-Port-Problematik kann jedoch durch die Kaskadierung von LDAP Proxy Servern, wie folgt, gelöst werden:

- Die Clients fragen den internen Proxy Server über Port 389 an.
- Dieser leitet die Anfrage an den zweiten in der DMZ (Demilitarisierte Zone) installierten LDAP Proxy Server weiter.
- Dieser Zugriff erfolgt dediziert zwischen diesen Proxy-Servern.
- Ein Zugriff aus dem Internet ist über die externe und die interne Firewall über den gleichen Port nicht möglich.

Als Beispiel sei hier das Siemens External Repository genannt:

Zur Nutzung des External Repositories muss ein Geschäftspartner dieses als LDAP-Verzeichnis in seinem E-Mail-Verschlüsselungsprogramm einbinden und konfigurieren oder indirekt über den virtuellen Verzeichnisdienst der European Bridge-CA ansprechen:

Zugang	Domain Name	IP-Adresse	Port	Suchbasis
Siemens	cl.siemens.com	194.138.38.161	389	O=Trustcenter
Bridge-CA	directory.bridge-ca.org	213.61.227.207	389	Keine

Die Anfrage geht dabei, wie allgemein üblich, über die vollqualifizierte E-Mail-Adresse. Rückgabewert ist gemäß LDAP-Protokoll der Distinguished Name (DN). Weil der DN oft Identifikatoren enthält, die durch automatisierte, manipulierte Veränderung zu neuen Treffern führen kann, über die E-Mail-Adressen ausspioniert werden könnten, wird im Inbound-Proxy von Siemens der DN nur verschlüsselt geliefert. Dies verhindert eine verstärkte Automatisierung, allerdings ist der DN auch Bestandteil des Zertifikats, so dass manuelles Sammeln von E-Mail-Adressen zu Spam-Zwecken nie ganz ausgeschlossen werden kann. Der Identifikator ist in diesem Beispiel eine 8-stellige alphanumerische Global-ID, die durch den Zeichenvorrat von 8 hoch 33 (23 Buchstaben und 10 Ziffern) auch bei sehr großen Mitarbeiterzahlen im Unternehmen langfristig (über 100 Jahre) Eindeutigkeit erzielt. Über den unkenntlichen DN können dann trotzdem die Zertifikate angefordert werden. Es werden z. B. zwei X.509-Zertifikate zu einem Eintrag gefunden (Verschlüsselung und Signatur).

Durch ein solches Vorgehen ist einerseits dem Datenschutz Rechnung getragen. Andererseits hat eine kontrollierte Öffnung der Kommunikationsbeziehungen stattgefunden, durch die lediglich das personengebundene Datum „Zertifikat“ extern bereit gestellt wird. Mitbestimmungsrechtlich sollte dies über eine Betriebsvereinbarung unproblematisch möglich gemacht werden können.

4.10 Wie können die Zertifikate genutzt werden?

VEDIS legt die Normensammlung ISIS-MTT zugrunde. Die Zertifikate sind nach der Norm X.509 Version 3 aufgebaut und im VEDIS-Dokument Technische PKI-Interoperabilität beschrieben. Die Anwendung dieser Zertifikate im Rahmen von E-Mail folgt dem S/MIME-Standard. S/MIME ist mittlerweile in neueren Microsoft-Outlook- und Lotus-Notes Versionen ohne zusätzlichen Plug-In anwendbar. Es kann jedoch auch mit Plug-In gearbeitet werden. Für S/MIME Verschlüsselung kann die Importierung in einen unternehmens-zentralen (virtuelle Poststelle) oder lokalen Key Store bzw. Certificate Store (Client plus evtl. Plug-In) empfohlen werden. Wenn sich der Schlüssel überraschend ändert, so kann höchstens eine E-Mail nicht entschlüsselt werden. Der Empfänger wird sich in diesem Fall melden.

Dieses Prinzip lässt sich bei Überprüfung der S/MIME-Signatur nicht anwenden. Deshalb sollte in angemessenen Zeiträumen am Ort seiner Pflege der Signaturschlüssel überprüft werden bzw. automatisch validiert werden, ob ein Zertifikat gesperrt ist. Im Zertifikat wird dazu das Feld CDP (CRL Distribution Point) ausgelesen und an aktueller CRL die Gültigkeit überprüft. Delta-CRL sollten nicht verwendet werden.

Neben Verschlüsselung und Signatur auf E-Mail-Ebene sollte auch das Mittel der Datei-Signatur unterstützt werden. Die S/MIME-Norm hat einige Restriktionen:

- Bei S/MIME ist Unterzeichner gleich Versender.
- S/MIME unterstützt deshalb auch keine Mehrfach-Signaturen, wie sie z. B. in Geschäftsbriefen nötig sind oder in anderen Anwendungsbereichen mit Mehrfachverantwortung. Auch ein „Durchreichen“ von Daten ohne Verantwortungsnahme kann damit nur schwer ohne sprechende Erläuterung abgebildet werden.
- S/MIME packt Text und Attachments in einen "verplombten" Container. Archivierung und Zugriff z. B. Volltextsuche wird dadurch problematisch.

Aus diesen Gründen und damit verbundenen wirtschaftlichen Konsequenzen sollte auch die Signatur auf Dateiebene angewendet werden. Allerdings ist neben der S/MIME-Verschlüsselung eine zusätzliche Verschlüsselung der Datei in den meisten Fällen unnötig.

Ein gewisses Problem stellt die Visualisierung der Signatur in Ausdrucken dar. Hier haben sich aber durchaus Möglichkeiten ergeben (siehe auch VEDIS-Dokument Umsetzungsempfehlungen).

4.11 Wie wird überprüft, ob der Schlüssel korrekt ist?

Die richtige Zuordnung von Schlüssel zu Person wird durch ein Zertifikat bestätigt. Dieses wird von der Zertifizierungsinstanz (CA) für diesen Schlüssel elektronisch unterschrieben. Gegebenfalls gibt es zu dieser CA noch eine übergeordnete Instanz, die wiederum den öffentlichen Schlüssel dieser CA bestätigt. Die oberste Instanz (Root) wird gerne als Vertrauensanker bezeichnet, denn dieser muss Vertrauen per se entgegengebracht werden. Es gibt im Allgemeinen zu jeder Organisation eine solche oberste Instanz. Technisch wird dies abgebildet, indem dieser öffentliche Schlüssel jeweils selbst signiert wird. Ein Schlüssel ist dann korrekt, wenn das zugehörige Zertifikat und die gesamte Kette korrekt ist. Diese Kette endet bei der Root-CA. Diesen wird aus der eigenen Organisation dann Vertrauen entgegengebracht, wenn der Schlüssel durch die eigene CA signiert wird (und meist auch umgekehrt). Dies wird Cross-Zertifizierung genannt. Es ist eine bilaterale Vertrauensbeziehung und wird z. B. zwischen Hochschulen im Deutschen Forschungsnetz praktiziert.

Oder es wird eine gemeinsame Instanz akzeptiert, die eine Liste von Root-Schlüsseln signiert und sicher an alle Organisationen verteilt. Dies ist das Prinzip einer Bridge-CA. Beispiel sind die European Bridge-CA (EB-CA) oder die Federal Bridge-CA in USA. Es ist eine multilaterale Vertrauensbeziehung.

VEDIS hat technische und vor allem organisatorische Sicherheitsanforderungen an PKI gemacht. Werden diese eingehalten, so steht einer gegenseitigen Vertrauensbeziehung nichts im Wege. Die Anforderungen sind konform zur EB-CA, es ist aber auch eine bilaterale Cross-Zertifizierung eingeschlossen.

4.12 Wie können Vertrauensbeziehungen technisch (möglichst automatisiert) abgebildet werden?

Automatisierung und Etablierung von sicheren organisationsübergreifenden E-Business-Prozessen bedeutet, dass Sperrlisten und die ganze Zertifikatskette automatisch überprüft werden bzw. auf Benutzeranstoß (Klicken auf Symbol) automatisch erfolgen kann. Dies ist heute ohne zusätzliche Benutzereingriffe und mit Standard-Software möglich. Allerdings müssen insbesondere fremde Vertrauensanker, also Root-Zertifikate, durch das eigene Unternehmen oder durch den Anwender bewusst akzeptiert und damit importiert oder abgelehnt werden. Mitglieder der EB-CA müssen diese Vertrauensanker neben dem eigenen CA-Zertifikat integrieren. Dies ist nichts Ungewöhnliches. Es müssen auch bei der Erneuerung des Root- bzw. CA-Schlüssels zwei eigene CA-Schlüssel in der Übergangszeit parallel existieren.

Bevor ein Anwender einen Vertrauensanker akzeptiert, sollte er den Fingerprint überprüft haben. Bei zukünftigen Kommunikationsbeziehungen ist dann auf sicherer Basis kein Benutzereingriff mehr nötig.

Ein fremdes Zertifikat wird also zunächst auf Gültigkeit anhand des CRL Distribution Point überprüft. Ist es dort nicht als gesperrt gemeldet, wird die ausgebende CA überprüft und ggf. eine nächste Ebene. Um diese Zertifikatsketten nicht zu lang werden zu lassen, sollten lediglich maximal 3 Ebenen (User, CA, Root) existieren.

Technisch wird im Zertifikat in der Feldgruppe CRL-Verteilungspunkte im Idealfall sowohl eine HTTP- als auch die LDAP-Adresse angegeben und durch den Bezeichner „certificateRevocationList“ begonnen und abgeschlossen und damit maschinell auswertbar. Wenn mehrere CA unter einer Root-CA hängen (z. B. für End-Entity-Zertifikate und Maschinenzertifikate) sollte eindeutig der Bezug zur CA deutlich werden.

Ein Beispiel für einen Eintrag wäre:

...

certificateRevocationList

URL=http://ch.evu.de/UID-EE-CA.crl

URL=ldap://ldap.evu.de, CN=UID-EE-CA

certificateRevocationList

UID-EE-CA steht für den logischen Namen der End-Entity-CA (Suchbasis sollte leer sein).

Weitere Informationen sind im VEDIS-Dokument „Technische PKI-Interoperabilität“ festgehalten.

4.13 Wie können Schlüssel langfristig verwaltet werden?

Daten gehören dem Unternehmen und nicht (nur) dem Anwender.

Es ist dabei grundsätzlich zwischen Verschlüsselung und Signatur zu unterscheiden.

Private Signaturschlüssel verlassen oft gar nicht mehr eine SmartCard, auf der sie gemeinsam mit dem öffentlichen Schlüssel generiert worden sind. Nur der öffentliche Schlüssel wird in einem genormten Verfahren (PKCS#10-Request) z. B. bei der Teilnehmer-Registrierung zur Zertifizierung exportiert. Eine externe Verwaltung verbietet sich für private Signatur-Schlüssel und für deren Zugriffsschutz (PIN).

Zur langfristigen Signaturprüfung muss lediglich auch auf alte öffentliche Schlüssel zurückgegriffen werden können. Meist wird dies aber in Unternehmensarchiven umgangen, indem regelmäßig (z. B. täglich) neue Dateien im Archiv zeitgestempelt werden und dieser Vorgang in regelmäßigen Abständen wiederholt wird. Der Zeitstempel entspricht einer erneuten Signatur des Hashwertes einer Datei. Dadurch bekommt die Datei einen eigenen Integritätsschutz, der bei mit fortschreitender technischer Entwicklung ungenügenden Schlüssellängen oder Algorithmen trotzdem den Beweiswert sichert. Bei sehr vielen Dateien können sogenannte Hashbäume gebildet werden. Die Prinzipien in der PKCS#7-Welt (Containerprinzip) sind gut verstanden, dokumentiert und in Produkten umgesetzt worden im Rahmen des ArchiSig-Projektes (www.archisig.de). Weitere Umsetzungen in der XML-Welt werden folgen (siehe Kapitel 5.1 Langzeitarchivierung). Diese Behandlung im Rahmen von Langzeitarchivierung umfasst alle Datentypen (klassisch, verschlüsselt, signiert). Beim Löschen oder Teilen von Archiven werden die Hashwerte von Dateien und Dateibäumen der Einfachheit halber im Archiv gelassen und nur die Datei gelöscht. Dies ist heute kein organisatorisches oder wirtschaftliches Problem.

Bei verschlüsselten Daten wird zum Dechiffrieren der private Schlüssel des Empfängers benötigt. Der Empfänger muss also alte Verschlüsselungsschlüssel in seinem Personal Security Environment aufheben, um alte, an ihn verschlüsselte Mails oder Dateien lesen zu können.

Gleichzeitig muss das Unternehmen im Bedarfsfall auf diese verschlüsselten Daten zugreifen können. Verschlüsselte Daten müssen also zu jeder Zeit unter Wahrung von Datenschutzgesichtspunkten kontrolliert eingesehen werden können. Dazu wird bei großen Anbietern von PKI-Lösungen ein Key-Archive angeboten, in dem diese Schlüssel sicher abgelegt und aus dem unter strengen Zugriffsregeln nach Rollen- und Vier-Augen-Prinzipien ein Key-Recovery vorgenommen werden kann.

4.14 Signaturanwendungsfälle

Standardanwendungen, wie E-Mail oder Remote Access Lösungen brauchen hier nicht betrachtet zu werden.

Erst im mehr oder weniger individuellen Anwendungskontext müssen bei Anwendung der elektronischen Signatur Differenzierungen gemacht werden, um zu wiederverwendbaren Modulen zu kommen.

Erste Differenzierung ist eine Einzelsignatur und Massensignaturen.

Die Einzelsignatur stellt eine bewusste, Einzelfall-bezogene Willenserklärung des Unterzeichners dar. Dazu wird das Personal Security Environment (PSE), das sich unter der alleinigen Kontrolle des Signaturschlüsselinhabers befindet, durch die PIN-Eingabe aktiviert und durch die Signaturerstellungseinheit (z. B. SmartCard) ein Dokument unterzeichnet. Auch Signaturen im 4-Augen-Prinzip (z. B. sachlich richtig - rechnerisch richtig) sind in diesem Sinne Einzelsignaturen.

Bei Massensignaturen wird in einer Anwendung, die stereotypen Output erzeugt (z. B. ein Rechnungslauf), das PSE aktiviert und es werden viele Signaturen erzeugt. Oft wird für diese Signaturen ein Pseudonym verwendet (z. B. Leiter Rechnungswesen), sie bleiben aber auf eine natürliche Person bezogen. In diesem Kontext ist ein deutlich stärkerer organisatorischer Schutz erforderlich.

Eine weitere, oft benötigte Komponente ist die Digitalisierung des Posteingangs. Dazu wird gescannt, das Scanergebnis (in repräsentativen Stichproben) geprüft, die digitale Kopie signiert und das Papieroriginal zur Vernichtung freigegeben. Die signierte Kopie wird gleichzeitig über die gebräuchliche COLD-Schnittstelle an das Archivsystem gegeben und referenziert (scan - sign - delete - archive). Dieses Vorgehen wird vielerorts in zahlreichen Projekten gerade auch im E-Government-Umfeld mit qualifizierten Signaturen gemäß Signaturgesetz praktiziert und ist durch das Verfahrensänderungsgesetz von 2002 rechtlich gedeckt.

4.15 European Bridge-CA (EB-CA)

Die EB-CA (oft nur Bridge-CA genannt) ist eine Initiative namhafter deutscher Firmen und des Bundes unter der Leitung des TeleTrusT Deutschland e.V. Der Bund wird durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) vertreten.

Wie jede Bridge-CA verteilt die EB-CA eine signierte Liste vertrauenswürdiger CA. Der Betreiber der CA muss in einer Selbsterklärung dem CP der EB-CA zustimmen.[3]

Zusätzlich wurden weitere Dienste aufgebaut. Die Dienste bilden quasi einen virtuellen Verzeichnisdienst bzw. Validierungsdienst (OCSP) zwischen den Mitgliedsinstitutionen

[3] Die EB-CA signiert das eigene Zertifikat und die CRL. Mit einem damit zertifizierten End-Entity-Schlüssel wird die Liste der CA der Mitgliedsorganisationen signiert. OCSP-Auskünfte werden zukünftig durch einen weiteren, durch die EB-CA zertifizierten Schlüssel unterschrieben.

(Firmen, Behörden) ab und können gleichzeitig auch die öffentlichen Verzeichnisse der Zertifizierungsdienstleister abfragen. So kann ohne Diskriminierung einer Zertifikatsklasse eine vertikale Interoperabilität zwischen fortgeschrittenen und qualifizierten bzw. akkreditiert qualifizierten Zertifikaten auf der Sicherheitsstufe der fortgeschrittenen Signatur erreicht werden. Auf dieser Basis sind heute schon E-Government-Anwendungen gesetzlich etwa durch die Steuerdatenübermittlungsverordnung (StDÜV) oder im Rahmen von Online-Rentenauskünften bei der Bundesversicherungsanstalt für Angestellte (BfA) geregelt.

Die virtuellen Dienste der Bridge-CA werden mit Hilfe von sogenannten Proxy-Lösungen, also Gateways, realisiert.[4] [5]

Sie stellen neben der ersten und eigentlichen Bridging-Funktion der EB-CA, der durch eine Certification Authority des TeleTrusT Deutschland e.V. signierten Liste (signed list) vertrauenswürdiger CA der Mitgliedsunternehmen eine qualitativ bedeutsame Erweiterung des Angebots der Bridge-CA dar.

Mit der Bridge entfällt die Cross-Zertifizierung und mit den EB-CA-Diensten die eigene Administration von fremden End-Entity-Zertifikaten in vertrauenswürdigen Institutionen.

Die EB-CA hat zunächst pragmatisch die Teilnahme von Mitgliedern am Verfahren gesichert (Phase 2) und ist nun dabei, das weitere Vorgehen beim Regelwerk und neuen Diensten zu ordnen.

Die Phasenbeschreibungen finden sich unter folg. URL und werden hier Stand 04.08.2003 zitiert:

http://www.bridge-ca.de/architektur/pdf/bridgeca_teilnahme_roadmap.pdf

Zur Zeit befinden sich die beteiligten Institutionen im Übergang von Phase 2 zu Phase 3.

Die Anwendung ist zunächst nur E-Mail im Opaque signed-Modus.

Die zur Zeit in der EB-CA organisierten Teilnehmer, zwischen denen interoperabler sicherer E-Mail-Verkehr möglich ist, nutzen 6 verschiedene CA-Implementierungen, wenigstens 4 verschiedene E-Mail-Clients mit wenigstens 6 verschiedenen S/MIME-Plug-In (Stand 4.8.2003).

Bridge-CA Verzeichnisdienstproxy

Mittlerweile hat sich LDAP als Zugriffsprotokoll auf interne Verzeichnisdienste durchgesetzt. LDAP nutzt den Port 389, dessen Öffnung nach außen aber meist nicht im Einklang mit der Sicherheitspolitik der Firewallkonfiguration steht. Der Einsatz von Verzeichnisdienstproxies kann ohne Sicherheitseinbußen Abhilfe schaffen. Die meisten LDAP-fähigen Standardprodukte sind zu dieser Gateway-Funktion in der Lage.

[4] Der Verzeichnisdienst-Proxy wurde im Auftrag der Fa. Boing realisiert. Ziel dieser Entwicklung war ausdrücklich NICHT die Vermarktung, sondern die sichere Anbindung von Zulieferfirmen. Die Software ist Open Source. Die Pflege für Europa wurde an die Fa. Noventum, Münster, übertragen.

[5] Der Validierungsdienst-Proxy ist eine Entwicklung der Fa. Secaron, Hallbergmoos. Die Positionierung erfolgt ähnlich wie bei dem Verzeichnisdienst-Proxy.

Üblicherweise richtet ein Client-System im Intranet eine LDAP-Anfrage über einen LDAP-Proxy an einen internen, LDAP-fähigen Verzeichnisdienst. Dazu wird im eigenen Netz (Intranet) der Port 389 verwendet. Wird das gesuchte Zertifikat nicht im internen Verzeichnis gefunden, kann der LDAP-Proxy im geschützten Intranet an einen weiteren LDAP-Proxy auf einem Rechner der Demilitarisierten Zone (DMZ) über eine frei wählbare 5-stellige Port-Nummer (z. B. 10389) weiterrouten. Dieser LDAP-Proxy übernimmt die eigentliche Zertifikatsanfrage im Internet beim Bridge-CA Verzeichnisdienst-Proxy mit einer vollqualifizierten SMTP-Adresse im Argument und wieder über Port 389.

Bridge-CA Validierungsdienstproxy

Analog zum LDAP-basierten Vorgehen kann bei der Validierung ein OCSP-basiertes Vorgehen gewählt werden. Die Routing-Mechanismen bleiben prinzipiell gleich. Im ersten Fall wird das Zertifikat über das Lightweight Directory Access Protocol (LDAP) geholt, um mit dem öffentlichen Schlüssel und den im Zertifikat angegebenen Algorithmen eine Verschlüsselung vornehmen zu können. Eine Validierung eines Zertifikats im Rahmen einer Signaturprüfung kann über das Online Certificate Status Protocol erfolgen.

Mit der Statusabfrage über OCSP gird ermittelt, ob ein Zertifikat noch gültig oder gesperrt ist. Dem Verfahren nach richtet ein OCSP-Client eine Statusanfrage an den OCSP-Server. Diese wird beantwortet mit gut, gesperrt oder unbekannt. Die Antwort kann durch den Server signiert sein.

OCSP hat das ältere Protokoll CRL teilweise verdrängt, weil bei CRL immer die komplette Widerrufsliste heruntergeladen werden muss, OCSP sich hingegen auf die Statusabfrage eines einzelnen Zertifikats richtet.

Die an den OCSP-Server gerichteten Anfragen werden von der Zertifizierungsstelle (CA) beantwortet, die den Status der Zertifikate im Server aktualisiert. Das OCSP-Protokoll wurde von der IETF (Internet Engineering Taskforce, www.ietf.org) spezifiziert und standardisiert, ersetzt teilweise das ältere CRL und baut auf dem http-Protokoll auf.

Die EB-CA kommt dem „virtuellen“ Verzeichnisdienst und dem Validierungsdienst einer Vereinbarung nach, wonach in dieser Phase automatisierbare**,** sichere, organisationsübergreifende Geschäftsprozesse über die Kommunikationsplattform EB-CA möglich sein sollen. Für die Teilnehmer bedeutet dies die Einführung von externen Zertifikatsverzeichnissen als zwingende Voraussetzung für hohen Automatisierungsgrad, denn nur so lassen sich für den Endbenutzer weitgehend transparent, z. B. vor einem Verschlüsselungsvorgang, ein externes Verschlüsselungszertifikat automatisiert beziehen.

Die „Gemeinsame Erklärung zu Sicherheitsrahmenbedingungen“ der Verbände fordert im Publikationskriterium auf Seite 5.

Zitat:

„Die Unternehmen sollten aber die elektronisch verschlüsselte und/oder signierte Form der Nachrichten von anderen Marktteilnehmern unter nachfolgenden Bedingungen

akzeptieren:...wenn ihre Zertifikate mit den öffentlichen Schlüsseln zur Verschlüsselung bzw. zur Unterschriftsvalidierung zur Verfügung stehen (Publikationskriterium).“

Dies schließt auch weniger komfortable Mechanismen des Schlüssel- und Zertifikatsaustausches ein. Mittelfristig bedeutet jedoch die Öffnung eines Unternehmens für weitergehende E-Business-Prozesse auch die komfortable Bereitstellung der dazu nötigen Informationen für die Geschäftspartner.

Keystatements zur EB-CA

- **Die EB-CA ist z. Zt. ein vielversprechender Ansatz, branchenneutral PKI zu einer gemeinsamen Vertrauensinfrastruktur zu verbinden. Problematisch ist die noch geringe Resonanz.**
- **Eine Nutzung der Dienste gegen Entgelt und eine Mitgliedschaft in der EB-CA ist immer optional. Alternative ist die Eigenverwaltung der externen Vertrauensbeziehungen.**
- **Die Nutzung der Dienste und selbst die Teilnahme an der EB-CA als Vollmitglied ist jederzeit problemlos wieder korrigierbar, wenn sich die EB-CA nicht durchsetzt.**

4.16 Bestätigungen, Quittungswesen

Willenserklärungen können allgemein Vorgänge im Rahmen von Bestellungen, Verträgen, Anträgen oder Aufträgen sein. Auch die wichtigsten EDI-Transaktionen im liberalisierten Strommarkt können im weitesten Sinn rechtlich als Willenserklärung des sendenden Unternehmens verstanden werden.

Daneben können auch Bestätigungen von vergleichbarer rechtlicher Bedeutung sein. Beispiele sind etwa Empfangsbescheinigungen, Quittungen, Dokumentationen, Protokolle, Bescheide oder Statusinformationen. Willenserklärungen und Bestätigungen können Fristenregelungen (z. B. Einspruchsfrist) auslösen.

So verlangt etwa der Gesetzgeber, dass eine Rechnung „zugestellt“ werden muss. Dabei gilt der Postweg als hinreichend sicher, während über den elektronischen Weg bisher keine Aussagen getroffen wurden. Auch technisch existieren hier prinzipielle Defizite. So hat das Basisprotokoll für E-Mail (SMTP) keine immanenten Quittungsmechanismen. Es besteht lediglich in vielen Mailclients die Möglichkeit, eine angeforderte Empfangs- bzw. Lesebestätigung zuzulassen oder abzulehnen. Dies wird aber häufig auf Serverebene wieder eingeschränkt (z. B. keine externen Bestätigungen). Im Gegensatz dazu existieren bei EDIFACT (auf der Anwendungsebene) Mechanismen (Nachrichtentypen CONTRL, APERAK).

Korrespondierende Bestätigungen haben theoretisch den gleichen Schutzbedarf wie die Willenserklärungen, auf die sie sich beziehen:

Sie müssen authentisch sein und unverfälscht bleiben. Wenn sie Rückschlüsse auf die Willenserklärung erlauben, so ist auch gegebenenfalls Vertraulichkeit zu gewährleisten.

Im praktischen Einsatz können konsequent ausgetauschte Quittungen aber auch problematisch sein. So werden im Allgemeinen diese Nachrichten zeitversetzt zurückkommen und müssen der entsprechenden Transaktion zugeordnet werden. Quittungen werden auf unterschiedlichen Ebenen unterschiedliche Bedeutung haben. Sie können Eintreffen der Nachricht signalisieren, die formatgerechte Behandlung betreffen (z. B. nicht konvertierbar von EDIFACT in Inhouse-Format) oder die inhaltliche Richtigkeit betreffen.

Selbstverständlich müssen im Negativfall auf den betreffenden Ebenen immer Antwortmechanismen an die sendende Stelle angewendet werden.

Im Positivfall sollte je nach Anwendungsfall differenziert werden. So kann bei eingespielten Verfahren im Massendatenaustausch durchaus dann auf Quittungsmechanismen verzichtet werden, wenn dies beide Geschäftspartner vereinbaren.

Bei singulären Transaktionen von entsprechender Bedeutung liegt es im Interesse der Geschäftspartner, die elektronisch abgewickelte geschäftliche Transaktion bestätigt, authentisch, integer und vertraulich abzuwickeln. Damit verbundene technische Quittungsbelege sollten wie die inhaltlichen Daten (z. B. Dokument) so archiviert werden, dass sie eine langfristige Beweissicherung ermöglichen.

5 Rechtliche, technische und organisatorische Anforderungen an die wichtigsten Stützprozesse

5.1 Langzeitarchivierung elektronisch signierter Daten

Die Signatur muss auch im Archivierungsprozess logisch untrennbar mit den Daten verknüpft bleiben.

Bei steuerrechtlichen und handelsrechtlichen Anforderungen sind damit im Allgemeinen 6 oder 10 Jahre Aufbewahrung verbunden. Baugenehmigungen sind z. B. unbegrenzt zu archivieren.

Die elektronische Welt stellt hier neue Ansprüche, die nach 3000 Jahren Erfahrungen mit dem Medium Papier schon gesellschaftspolitische Auswirkungen haben.

Rechtlich formuliert muss der Beweiswert der elektronischen Form gewahrt bleiben, so lange er durch gesetzliche Archivierungsfristen oder durch Geschäftsanforderungen, wie Haftung, Gewährleistung, Anspruch, etc. erforderlich ist.

Eine elektronische Signatur ist technisch der verschlüsselte Hashwert der Daten. Die Daten werden also einer Einwegfunktion unterzogen, der Hashfunktion, die irreversibel einen Bitstring erzeugt, der einen Fingerabdruck der Daten bzw. des Dokumentes darstellt. Diese sehr große Zahl (MD5 128 Bit, SHA-1 160 Bit) wird mit dem privaten Signierschlüssel, meist unter Anwendung des RSA-Algorithmus, verschlüsselt. Dabei entsteht heute ein 1024 Bit langer Ausdruck, der elektronische oder digitale Signatur genannt wird.[6]

Der Empfänger bildet ebenfalls den Hashwert mit der gleichen Funktion über das erhaltene Dokument und entschlüsselt die Signatur mit dem öffentlichen Schlüssel des Unterzeichnenden. Stimmt der selbst gebildete Hashwert mit dem übertragenen und entschlüsselten Wert überein, so wurden die Daten unterwegs nicht verändert und stammen unzweifelhaft vom Unterzeichnenden.

Allerdings geht die technische und mathematische Entwicklung weiter. Schlüssellängen können nicht mehr ausreichen oder sogar Algorithmen unsicher werden. Das Bundesamt für Sicherheit in der Informationstechnik veröffentlicht deshalb regelmäßig im Bundesanzeiger Gültigkeitszeiträume für Schlüssellängen und kryptographische Algorithmen, wie Hashfunktionen und Verschlüsselungsalgorithmen. Zurzeit werden Schlüssellängen in Verbindung mit dem RSA-Algorithmus von mindestens 1024 Bit bei Anwendersignaturschlüsseln und von mindestens 2048 Bit bei Schlüsseln in Zertifizierungsinstanzen (die Zertifikate unterschreiben) per Verordnung als gültig bis 2006 erklärt. Auch wenn es heute höchst unwahrscheinlich erscheint, kann theoretisch ein Datenträger mit signierten Daten unter bestimmten Voraussetzungen manipuliert werden.

[6] Die Hashfunktion SHA-1 wird höchstwahrscheinlich zukünftig vom BSI nicht mehr empfohlen und wird ersetzt durch SHA256.

Ein vorstellbarer Fall ist dabei, dass mit enormen Rechenaufwand der private Schlüssel des Unterzeichners ermittelt wird und dann Daten verändert werden, die mit Hilfe des korrumpierten Schlüssels neu signiert werden. Mit Hilfe eines baugleichen Datenträgers, wie der ursprüngliche Datenträger, könnten dann alle Daten kopiert werden, wobei die alte Datei durch die manipulierte und neu signierte Datei ersetzt wird.

Analog und deutlich spektakulärer wäre eine unsicher gewordene Hashfunktion, wie der häufig angewendete Secure Hash Algorithmus Nr. 1 (SHA-1) oder gar der RSA-Algorithmus, der weltweit am häufigsten eingesetzte asymmetrische, also in Public Key Verfahren eingesetzte, Verschlüsselungsalgorithmus.

Um diesen theoretischen, aber nicht ausschließbaren Bedrohungsszenarien zu begegnen, ist bei der Langzeitarchivierung nach einer gewissen Zeit eine Nachsignatur im §17 der Signaturverordnung vom 22.11.2001, also bei qualifizierten Signaturen, vorgeschrieben.

„Daten mit einer qualifizierten elektronischen Signatur sind nach § 6 Abs. 1 Satz 2 des Signaturgesetzes neu zu signieren, wenn diese für längere Zeit in signierter Form benötigt werden, als die für die Erzeugung und Prüfung eingesetzten Algorithmen und zugehörigen Parameter als geeignet beurteilt sind. In diesem Falle sind die Daten vor dem Zeitpunkt des Ablaufs der Eignung der Algorithmen und der zugehörigen Parameter mit einer neuen qualifizierten elektronischen Signatur zu versehen. Diese muss mit geeigneten neuen Algorithmen oder zugehörigen Parametern erfolgen, frühere Signaturen einschließen und einen qualifizierten Zeitstempel tragen.“

Diese Nachsignatur bezieht sich auf zeitlich neue Absicherung des Beweiswertes durch einen Zeitstempel.

(Es ist also keinesfalls vom Unterzeichnenden eine neue Signatur erforderlich!)

Rechtliche Anforderungen des § 17 SigG an die Nachsignatur sind dabei:

- Erneute Signatur muss rechtzeitig und mit geeigneten Verfahren erfolgen.
- Erneute Signatur muss die gleiche Qualitätsstufe haben, wie die Ausgangssignatur.
- Erneute Signatur muss alle vorherigen Signaturen eines elektronischen Dokuments umschließen.
- Eine erneute Signatur kann viele Dokumente umschließen.

Diese Anforderungen an beweiskräftige Langzeitarchivierung elektronischer Signaturen in einem rein elektronischen Geschäftsverkehr müssen praktikabel sein und sich mit Anforderungen aus der Praxis verbinden lassen.

- Es wäre nicht praktikabel, wenn Dokumente neu mit einem Anzeige- bzw. Bearbeitungswerkzeug geöffnet werden müssten.
- Ein hoher Automatisierungsgrad muss gewährleistet bleiben.
- Es muss, z. B. aus Datenschutzgründen, in Teilen des Archivs gelöscht werden dürfen.
- Verschlüsselte Daten dürfen aus Gründen des Datenschutzes oder Geheimnisschutzes nicht vorher entschlüsselt werden müssen.

- Bei firmenpolitischen Prozessen, wie Ausgliederungen und Umgruppierungen rechtlich eigenständiger Einheiten müssen Archive geteilt und neu gruppiert werden können.
- Wenn die elektronisch archivierten Dokumente Beweismittel sein sollen, müssen sie verkehrsfähig sein.

Es hat sich gezeigt, dass rechtliche und praktische Anforderungen keine Widersprüche darstellen, sondern technisch und organisatorisch mit vertretbarem Aufwand erfüllt werden können. Vertretbar heißt hier besonders wirtschaftlich vertretbar, weil der Nutzen des elektronischen Archivs den Aufwand deutlich überwiegen muss.

Das technische Prinzip nutzt dabei aus, dass der Hashwert das Dokument bzw. die Datei bzw. die Daten eindeutig repräsentiert. Es muss also der Beweiswert des Hashwerts gesichert bleiben. Hashwerte aus geeignet zusammengehörenden Dateien können zudem konkateniert, also sequentiell zusammengesetzt werden, und dann neu mit einem Zeitstempel versehen werden. Diese Vorgehensweise, über Hashbäume effektiv ganze Datenträger nachsignieren zu können, ohne bei den oben genannten Anforderungen Abstriche machen zu müssen, wurde im Rahmen eines Förderprojektes des Bundes, ARCHISIG, entwickelt und implementiert. Ein sogenannter „Reduced archive timestamp“ benötigt dabei für den Fall, dass die Hashfunktion gültig bleibt, lediglich die Aufbewahrung von Hashwerten, Hashfolgen von Sohnknoten im Pfad sowie Zeitstempel über den Wurzelhashwert. Dies ist relativ wenig Zusatzaufwand und Zusatzdaten, da ein Hashwert lediglich 128 Bytes groß ist.

ARCHISIG geht dabei über die Aussagen im RFC 3126 hinaus (Electronic Signature Formats for long term electronic signatures) und hat die Praxistauglichkeit durch Implementierung und Anwendung nachgewiesen.

Sollte der unwahrscheinliche Fall eintreten, dass heute gebräuchliche Hashfunktionen unsicher werden, so müssen alle Dateien im Archiv neu mit einer anderen Einwegfunktion gehasht werden, wenn sie einzeln zur Verfügung stehen sollen. Ansonsten können mehrere/viele Dateien zusammengefasst werden. Auch dieser Fall wäre noch gut beherrschbar.

Auch der kryptographische „Worst Case“, ein unsicher gewordenes RSA-Verfahren, kann aufgefangen werden, indem die Hashwerte nach einem alternativen Verfahren, (z. B. mittels Elliptische Kurven) neu verschlüsselt werden.

Diese durchgespielten Möglichkeiten sollen zeigen, dass Langzeitarchivierung elektronisch signierter Daten auch dann beherrschbar bleibt, wenn die Kryptoanalyse ungeahnte Fortschritte machen sollte.

Weil es sich zudem bei der ersten Anwendung um medizinische Daten mit ihren hohen datenschutzrechtlichen Anforderungen handelt, kann die entstandene Lösung als branchenübergreifend repräsentativ betrachtet werden, die über das Niveau der Zeitstempel-Signaturen (fortgeschritten, qualifiziert) sicherheitstechnisch skaliert werden kann.

Das in ARCHISIG angewendete Prinzip des „Reduced archive timestamp“ wurde deshalb in die ISIS-MTT-Norm eingebracht. Auch bei der IETF liegt ein entsprechender Normungsvorschlag eines Trusted Archive Protokolls vor.

Erste Implementierungen in Archivsystemen anerkannter Hersteller sind ebenfalls abgeschlossen.

Die Langzeitarchivierung hat damit ihren Status als Unsicherheitsfaktor beim Wechsel in diese Technologien verloren.

Wenn qualifiziert signierte Dokumente langzeitarchiviert werden müssen, so sind auch qualifizierte Zeitstempel erforderlich. Dies ist eine signifikant wirtschaftliche Belastung, wenn dazu originäre, vom qualifizierten Timestamping Service (qTSS) angeforderte Zeitstempel benutzt werden.

Einen wichtigen Beitrag zu Einsparungen können Intervall-Qualifizierte (IQ) Zeitstempel leisten. Hierzu wird in regelmäßigen Abständen (z. B. einmal pro Arbeitstag) ein qualifizierter Zeitstempel angefordert.

„Durch den geschickten Einsatz einer kryptographischen Hashfunktion, deren Einwegeigenschaft eine relative zeitliche Ordnung zwischen den verschiedenen (qualifizierten und selbsterzeugten) Zeitstempeln induziert, kann - unter üblichen kryptographischen Annahmen - bewiesen werden, dass der IQ-Zeitstempel in der Zeit zwischen zwei bestimmten qualifizierten Zeitstempeln erstellt wurde.“ (zitiert nach Detlef Hühnlein, "Intervall-qualifizierte Zeitstempel", erschienen im Tagungsband Elektronische Geschäftsprozesse 2004, IT-Verlag).

5.2 Visualisierung und Massensignaturen

Grundsätzlich sollte bei elektronischen Signaturen das Prinzip „What You See Is What You Sign“ überprüft und eingehalten werden. D. h. es muss sichergestellt sein, dass keine verdeckten Informationen signiert werden („weiße Schrift auf weißem Grund“). Gerade im kommerziellen Umfeld des elektronischen Massendatenaustauschs sollte jedoch diese Forderung unproblematisch sein, weil EDI-Verkehr in den steuerrechtlich und handelsrechtlich geregelten Bereich der ordnungsgemäßen elektronischen Buchführung fallen. Dafür ist Revisionssicherheit durch einen Wirtschaftsprüfer zu testieren. Die Produktionsabläufe selbst, z. B. eines Rechnungslaufes, sind also als revisionssicher einzustufen. Eine explizite Visualisierung muss in diesem Standardprozess nicht stattfinden. Es kann mit technisch geeigneten Maßnahmen eine Massensignatur stattfinden.

Hinweise auf gesetzlich erwartete Rahmenbedingungen für qualifizierte Signaturen im Massenbetrieb finden sich z. B. bei der Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen bei den Frequently Asked Questions (Frage 18).[7]

[7] http://www.bundesnetzagentur.de/enid/ba08087c570be2cf1cfa23b1d7f9fbd6,0/FAQ/Antwortss8_wt.html

Außer bei gesetzlich vorgeschriebenen Vorgängen, wie der rein elektronischen Rechnung nach §14 Umsatzsteuergesetz, wird im Rahmen der VEDIS-Empfehlungen lediglich eine fortgeschrittene elektronische Signatur erwartet.

Z. B. im Rahmen einer steuerlichen Außenprüfung kann eine „retrograde“ (vom Beleg ausgehende) Prüfung erfolgen. Bei diesem Prüfvorgang müssen Ursprungsdaten, konvertierte Daten (z. B. EDIFACT-Dateien) und Unterschriften geeignet visualisiert werden können.

Diese Forderung definiert sich insbesondere durch die Anforderungen aus der Abgabenordnung bzw. dem Umsatzsteuerrecht (inkl. Vorsteuerabzugsberechtigung) und aus den Archivierungsanforderungen gemäß den „Grundsätzen zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen“ (GDPdU, BMF-Schreiben vom 16.7.2001, Seite 5).

Bei dieser nachträglichen Visualisierung müssen alle Nettodaten, Zusatzinformationen und technischen Komponenten verfügbar sein. Dies schließt eine Abwärtskompatibilität bei Versionswechseln ein.

5.3 Validierungsinformationen

Im klassischen Workflow stellen Eingangsstempel oder weitere Zusätze das erhaltene Papierdokument in den zeitlichen und ablauforganisatorischen Kontext. Ähnlich sollen im elektronischen Prozess die Validierungsinformationen eineindeutig den Daten zugeordnet und mit den Daten zusammen archiviert werden.

Eine fehlerhafte Dokumentation der Signaturvalidierungsinformationen kann z. B. im Behördenumfeld gemäß § 44 Abs. 2 Nr. 1 Verwaltungsverfahrensgesetz (VwVfG) die Nichtigkeit des elektronischen Verwaltungsaktes zur Folge haben.

Validierungsinformationen stellen somit bilateral Verbindlichkeit her. Sie sind mehr als nur Beweiswerterhaltung des Empfängers gegenüber dem Absender. Es geht nicht nur um nachträgliche Nicht-Abstreitbarkeit, sondern um die revisionssichere Dokumentation der geschäftlichen Transaktion an sich. Aus diesem Grund muss die Signatur zeitnah zur Geschäftstransaktion validiert werden und das Ergebnis der Prüfung muss mit den Daten und der Signatur archiviert werden.

6 Quellen

Allgemeine Quellen

IETF RFC 2459, Internet X.509 Public Key Infrastructure Certificate and CRL Profile, R.Housley, W.Ford, W.Polk, D.Solo, January 1999, IETF draft-ietf-pkix-new-part1-11.txt (RFC 2459-bis), Internet X.509 Public Key Infrastructure Certificate and CRL Profile, R.Housley, W.Ford, W.Polk, D.Solo, October 2001, neu RFC3280

Bridge CA, Organisatorische und technische Anforderungen für die Teilnahme an der Bridge-CA, http://www.bridge-ca.org/

Common ISIS-MTT Spezifikation for PKI Applications from T7 & TeleTrusT, V1.0, September 2001

- http://www.teletrust.de/Dokumente/ISIS-MTT_Core_Specification_v1.1.pdf, 2004-03-16
- ISIS-MTT Testbed Prototype 1.1 (build 5 SP 1, 2003-08-13)

  (Als CD beziehbar von TeleTrusT e.V. Chamissostrasse 11. D-99096 Erfurt)
- ISIS-MTT: Profile for Authentication Certificates, V 1.0, 2004-11-02, in Veröffentlichung

VDEW-Veröffentlichungen

- Einsatz von Verschlüsselung und Elektronischer Signatur im elektronischen Geschäftsverkehr der deutschen Elektrizitätswirtschaft
  Studie
  VDEW-Materialie M-14/2002
- Sicherheitsrahmenbedingungen für den elektronischen Geschäftsverkehr im deutschen Strommarkt
  Gemeinsame Erklärung der Verbände
- Sicherheitspolitik (PKI-Policy), Version 1.0
  VDEW-Materialie M-14/2003
- Umgang mit Schlüsselmaterial, Version 1.0
  VDEW-Materialie M-17/2003
- Technische PKI-Interoperabilität, Version 1.0
  VDEW-Materialie M-15/2003
- Umsetzungsempfehlungen, Version 1.0
  VDEW-Materialie M-16/2003
- Zertifizierungsrichtlinie (Certification Practice Statement), Version 1.0
  VDEW-Materialie M-18/2003

7 Anhang 1

Nationale Aspekte technischer Sicherheitsrahmenbedingungen bei qualifizierten Signaturen

Technisch bestehen zwischen qualifizierten und qualifizierten Zertifikaten mit Anbieterakkreditierung auf unterschiedlichen Ebenen in Deutschland de facto erhebliche Unterschiede.

Die heutige Root-Certification Authority (Root-CA) der Bundesnetzagentur als Wurzelinstanz für akkreditiert qualifizierte Zertifikate unterstützt zur Signatur der CA-Zertifikate etwa von Zertifizierungsdiensteanbietern, ZDA, den Hashalgorithmus RIPEMD-160 (KeyUsage CertSign,). Dieser Algorithmus ist weltweit eher unüblich und wird in Standardanwendungen nicht per se unterstützt. Die Bundesnetzagentur hat im Dezember 2004 eine neue CA in Betrieb genommen, bei der dieser Algorithmus auch weiterhin angewendet wird. Die akkreditierten ZDA verwenden diesen Hashalgorithmus auch zur Signatur von Endbenutzerzertifikaten. Ein Zertifizierungsdiensteanbieter für qualifizierte Zertifikate, deren Wurzelinstanz nicht die Bundesnetzagentur ist, unterstützt auch den gängigen Hashalgorithmus SHA-1. SHA-1 wird auch nur im Standard in den Basisversionen der meistverbreiteten Mail-Clients unterstützt, so dass der Einsatz qualifiziert akkreditierter Zertifikate z. Zt. über sogenannte Plug-Ins erreicht werden muss, wenn auf Datei oder S/MIME-Ebene signiert werden soll. Die Plug-Ins sind aber bei allen ZDA für neuere Microsoft- und Lotus-Notes-Versionen verfügbar; für LINUX besteht noch teilweise Nachholbedarf bei einzelnen ZDA. Als Begründung durch die Bundesnetzagentur für die Verwendung von RIPEMD-160 wird die Tatsache angeführt, dass der Algorithmenkatalog des Bundesamtes für Sicherheit in der Informationstechnik (BSI) für SHA-1 nur eine formale Gültigkeit bis Mitte 2009 vorsieht. Dieses Argument ist schwer nachvollziehbar. Bis zu diesem Zeitpunkt ist wahrscheinlich auch eine Schlüssellänge von 1024 Bit für CA-Schlüssel unverantwortlich, wie sie auch für die neuen Root-CA-Schlüssel der Bundesnetzagentur gilt. Bereits heute verwenden viele CA öffentlicher oder privater Institutionen deutlich längere Schlüssel.

Theoretisch könnte ein ZDA einen anderen Hashalgorithmus bei der Signierung von Endbenutzerzertifikaten anwenden. Dies ist jedoch im Allgemeinen nicht praktikabel, weil es sinnvoll ist, mit einem Algorithmus die komplette Validierungskette zu prüfen. Es soll jedoch an einer automatisierten Algorithmensuche gearbeitet werden.[8] Ein weiteres Hindernis war

[8] Zur Zeit kann oder will die Bundesnetzagentur noch keine neuen CA-Zertifikate ausstellen.
Folgende Ausnahme ist bei der Prüfung der qualifizierten Zertifikate zu beachten (Zitat Bundesnetzagentur):
Die beiden Root-Zertifikate der Bundesnetzagentur mit den Common Names
3R-CA 1:PN (Seriennummer: 990210003)
4R-CA 1:PN (Seriennummer: 990210004)
sind nicht über OCSP prüfbar, da der Public Key beider Root-Zertifikate einen negativen Exponenten enthält. Alle Zertifikate, die mit diesen beiden korrespondierenden Signaturschlüsseln ausgestellt wurden, lassen sich ebenfalls nicht über OCSP abfragen. Ein Download des Zertifikats über LDAP (und eine nachfolgende Prüfung auf Client-Seite) ist jedoch möglich. Begründung: Verschiedene Clientprogramme interpretieren Schlüssel mit negativen Exponenten unterschiedlich. Einige behandeln ihn ohne Änderung, andere aber sehen den Exponenten als positiv an und stellen ein Null-Byte voran. Bei einer Hashwertbildung über diesen öffentlichen Schlüssel führt dies dann zu unterschiedlichen Hashwerten. Dies ergibt Probleme bei dem OCSP-Protokoll, denn der in der OCSP-Anfrage notwendige IssuerKeyHash wird sich in solchen Fällen bei dem gleichen angefragten Zertifikat unterscheiden. Auch wenn es sich hierbei um ein Client-seitiges Problem handelt, wurde beschlossen, diese beiden Root-Zertifikate, alle Dienste-Zertifikate der Bundesnetzagentur sowie alle mit den beiden Root-Zertifikaten ausgestellten Zertifikate

bisher das unterschiedliche Validierungsmodell (Kettenmodell versus Schalenmodell). Beim Kettenmodell bleibt das ungesperrte Endbenutzer-Zertifikat unabhängig von der Gültigkeit des CA-Zertifikats bis zum im Zertifikat eingetragenen Gültigkeitsende gültig. Beim Schalenmodell werden sofort alle Benutzerzertifikate ungültig, wenn das Zertifikat der ausgebenden CA (genauer: ein Issuer-Zertifikat in der Validierungskette) ungültig wird. Im Rahmen des deutschen Signaturbündnisses wurde insbesondere auf Druck der deutschen Kreditwirtschaft eine Unterstützung des international üblichen Schalenmodells gefordert. Das Signaturänderungsgesetz vom 10.01.2005 lässt individuell vereinbarte Sperrgründe für qualifizierte Zertifikate zu. Damit wird auch rechtlich die technische Anwendung des Schalenmodells möglich. Technisch soll über unterschiedliche OID im Zertifikat die Anwendung des jeweiligen Modells signalisiert werden.

Die neue Root-CA lässt es zu, dass so genannte „Top-Level-Zertifikate“ anderer Länder aufgenommen werden können und bietet ein temporäres oder dauerhaftes Root-Hosting für andere Länder an. Zur Zeit sind Normierungsbestrebungen auf europäischer Ebene im Gange, um bei den entsprechenden Policy-Dokumenten Vergleichbarkeit zu garantieren. Dies gilt vor allem für qualifizierte Signaturen, die im inter-europäischen Kontext eingesetzt werden sollen. (siehe ETSI TS 101 456: "Policy requirements for certification authorities issuing qualified certificates").

Die “Vertikale Interoperabilität”, hier im Sinne als Maß von Koexistenz- oder gar Kooperationsfähigkeit, zwischen fortgeschrittenen und qualifizierten Signaturen scheiterte in der Vergangenheit oft an sogenannten Middleware-Problemen. Beim Einsatz mehrerer Karten bzw. unterschiedlicher Treiber kam es zu Konflikten. Hier soll auf Initiative von Microsoft, Kobil und Datev ein einheitlicher Cryptoserviceprovider Abhilfe schaffen. Dieser unterstützt gängige Kartentypen parallel, realisiert auch Prüfungen nach dem Kettenmodell, wird als Komponente nach dem Signaturgesetz zertifiziert und wird für neuere Standard-Microsoft-Betriebssysteme unentgeltlich zum Download bereit gestellt.

Trotz der genannten national abweichenden Rahmenbedingungen sind die genannten technischen Implikationen heute in Deutschland technisch beherrscht. Unabhängig von den rechtlichen Erfordernissen, ist eine qualifizierte Signatur zwar im Allgemeinen teurer als fortgeschrittene Signaturen, aber mit vertretbarem Aufwand einsetzbar. Allerdings führen die regulativen Rahmenbedingungen dazu, dass internationale Standardprodukte nur mit nationalen Ergänzungen eingesetzt werden können.

---

akkreditierter Zertifizierungsdiensteanbieter nicht über OCSP nachprüfbar zu halten, um der Gefahr von unterschiedlichen Statusauskünften zu einem Zertifikat vorzubeugen. Alle diese Zertifikate können jedoch über LDAP geladen und gegen die Sperrliste geprüft werden. Hier finden Sie eine komplette Liste der Seriennummern der hiervon betroffenen Zertifikate. http://www.nrca-ds.de/3r4rZertifikate.htm