DuD
Datenschutz und Datensicherheit

MailTrusT-PKI-Spezifikation

MailTrusT Version 2

Jobst Biester

Sicherheitslösungen in Anwendungen für offene Kommunikationssysteme wie E-Mail müssen mit Produkten unterschiedlicher Hersteller zusammenarbeiten können. Zu diesem Zweck wurde von TeleTrusT[1] 1996 mit der Version 1.1 der MailTrusT-Spezifikation ein Standard geschaffen, der interoperabel ist, in Produkten verschiedener Hersteller implementiert wurde und sich in der Praxis insbesondere auch in großen und komplexen Infrastrukturen bewährt hat. Mit der im Auftrag von TeleTrusT entwickelten Version 2 liegt nun seit März 1999 eine zu einem PKI-Standard weiterentwickelte Spezifikation vor.

Dipl.-Inform.
Jobst Biester

Security Consultant der Secorvo Security Consuling GmbH, Karlsruhe.
Hauptarbeitsgebiete: Netzwerk- und Systemsicherheit, Sicherheitskonzepte, Public Key-Infrastrukturen.
E-Mail: biester@secorvo.de

[1] http://www.teletrust.de

Einleitung

Seit der Verabschiedung der Version 1.1 der MailTrusT-Spezifikation im Jahr 1996 [MTRUST 96] hat es eine Vielzahl neuer Entwicklungen gegeben, die alle Teile der Spezifikation betreffen. Auf nationaler Ebene ist hier insbesondere das Signaturgesetz zu nennen, das Rahmenbedingungen für digitale Signaturen geschaffen hat. Auf internationaler Ebene wurden bestehende Standards weiterentwickelt und neue Standards geschaffen.

Die Erfahrungen beim Einsatz von MailTrusT-konformen Produkten in verschiedenen Projekten (z.B. der Einsatz in der Bundesverwaltung, im Gesundheitswesen und im Bankenumfeld) haben gezeigt, daß eine Berücksichtigung der nationalen und internationalen Entwicklungen durch eine Fortschreibung und Weiterentwicklung der Spezifikation erforderlich ist.

In diesem Beitrag wird die Gesamtkonzeption im Überblick dargestellt und es wird auf die Zielvorgaben der Spezifikation sowie den Aufbau und die Komponenten einer MailTrusT-PKI genauer eingegangen.

1 Gesamtkonzeption

Während die Spezifikationen der Version 1.1 auf einzelne wesentliche Aspekte einer PKI beschränkt waren, wurde der spezifizierte Bereich in der vorliegenden Version 2 wesentlich ausgedehnt. Außerdem wurde die Spezifikation an den aktuellen Stand der nationalen und internationalen Standardisierung angepaßt.

Wesentliche Aspekte der Version 2 der MailTrusT-Spezifikation sind:

- Ergänzung von bislang nicht oder nur unzureichend spezifizierten Anteilen, wie dem Aufbau einer PKI, PKI-Management-Nachrichten oder Schnittstellen zu Sicherheits-Token (z.B. Chipkarten).
- Integration von MailTrusT-Profilen auf der Basis aktueller Standards wie X.509v3 [ITU-T X.509 97] für Zertifikate und Sperrlisten in die Systemspezifikation MailTrusT. Die Profile stimmen im wesentlichen mit den Profilen der PKIX-Arbeitsgruppe der IETF [PKIX-PRO 98] und der Interoperabilitätsspezifikation zum Signaturgesetz [SIGI-ZERT 99] überein.
- Berücksichtigung der durch den Einsatz von MailTrusT-Produkten in der Praxis gewonnenen Erfahrungen in Form zusätzlicher Interoperabilitätsanforderungen. So wurden z.B. zusätzliche Vorgaben für die Behandlung von Attachments in die Spezifikation aufgenommen.
- Aktualisierung durch Anpassung der Algorithmen und Aufnahme zusätzlicher Anforderungen wie z.B. die Trennung von Signatur- und Verschlüsselungsschlüsseln.

2 Zielvorgaben

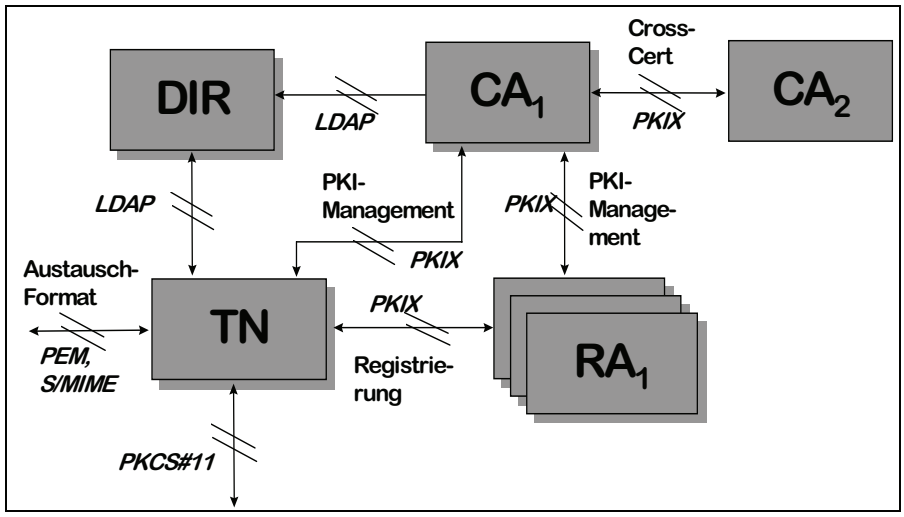
Orientierungspunkte bei der Fortschreibung und Weiterentwicklung zur vorliegenden Version 2 der Spezifikation waren folgende Zielvorgaben:

- **Interoperabilität:** Die Spezifikation gewährleistet, daß Produkte unterschiedlicher Hersteller, die dieser Spezifikation genügen, ohne Modifikationen oder weitere Abstimmungen direkt interoperabel sind.
- **Minimalität:** Die Spezifikation ist minimal, um Produktherstellern eine maximale Gestaltungsfreiheit zu erhalten. Sie ist im wesentlichen auf die für die Interoperabilität verschiedener Komponenten erforderlichen Festlegungen für einen in der Regel ausreichenden Funktionsumfang beschränkt (soviel wie nötig, so wenig wie möglich).
- **Kontinuität:** Sowohl für die Hersteller als auch für die Kunden MailTrusT-

konformer Komponenten wird durch Kontinuität Investitionssicherheit in größtmöglichem Umfang gewährleistet. Mit der Version 2 konforme Produkte sind mit den im Einsatz befindlichen MailTrusT-Komponenten kompatibel, soweit eine Beschränkung auf die Funktionalität dieser Produkte erfolgt. In diesem Sinne kann die Version 1.1 als Teilmenge von Version 2 angesehen werden.

- **Universalität:** Die Spezifikation setzt kein bestimmtes Modell einer PKI voraus; sie unterstützt zentrale, dezentrale und kombinierte Modelle. Die Spezifikation ist auch nicht auf bestimmte Anwendungen beschränkt. Sie ist vielmehr für eine breite Palette von Anwendungen entworfen.
- **Modularität:** Die Spezifikation besteht aus mehren aufeinander abgestimmten Modulen, die Teile eines umfassenden Systemkonzepts sind. Im Gegensatz zur Version 1.1 der MailTrusT-Spezifikation muß nicht jeder Hersteller alle Module realisieren, um ein MailTrust-konformes Produkt anbieten zu können. Da die Module aufeinander abgestimmt sind, können Module verschiedener Hersteller miteinander kombiniert werden. Durch die Token-Schnittstelle können z.B. Komponenten eines Herstellers Chipkarten eines anderen Herstellers verwenden.
- **Standardkonformität:** Die MailTrusT-Spezifikation basiert soweit als möglich auf etablierten und verbreiteten Standards. Neben PEM, X.509 und PKCS11 („Cryptoki“), auf denen die Version 1.1 basiert, werden für die Version 2 insbesondere auch die Spezifikationen der PKIX-Arbeitsgruppen der IETF und die Interoperabilitätspezifikation[2] des BSI zum Signaturgesetz berücksichtigt. Auf der Basis dieser Standards werden Profile definiert, die die Standards interoperabel machen und den Zielen von MailTrusT gerecht werden.
- **Unabhängigkeit:** Die MailTrusT-Spezifikation wurde allein auf der Grundlage von Erfahrungen und sachlichen Argumenten erstellt. Proprietäre Lösungen einzelner Produkthersteller waren kein Maßstab für die Spezifikation.

[2] Zur Interoperabilitätsspezifikation siehe Berger, in diesem Heft.



3 Aufbau und Komponenten

Die vorliegende Spezifikation setzt im Gegensatz zur Version 1.1 kein festes Modell einer Zertifizierungsinfrastruktur voraus. Der Aufbau einer Zertifizierungsinfrastruktur nach der Version 2 der MailTrusT-Spezifikation (MailTrusT-PKI) kann deshalb wesentlich flexibler den jeweiligen Anforderungen angepaßt werden.

Jede MailTrusT-PKI besteht aus folgenden Grundkomponenten:

- Teilnehmer-Komponenten (TN)
- Zertifizierungsstellen (CA)
- Registrierungsstellen (RA)
- Verzeichnisdienst (DIR)

Jede dieser Komponenten hat innerhalb der PKI eine bestimmte Funktion und deshalb bestimmte Aufgaben zu erfüllen. Die Aufgabenzuweisung soll möglichst flexibel an die Anforderungen der jeweiligen PKI angepaßt werden können. Deshalb erfolgt keine feste Zuweisung von Aufgaben zu Komponenten. Es werden lediglich Empfehlungen gegeben.

Zwischen den Komponenten gibt es eine Vielzahl spezifizierter online-Schnittstellen für die wesentlichen Interaktionen. Schnittstellen sind auch für die Kommunikation zwischen verschiedenen Teilen einer Grundkomponente definiert.

In der folgenden Abbildung wird der prinzipielle Aufbau einer MailTrust-PKI mit ihren Komponenten und Schnittstellen auszugsweise dargestellt.

Im folgenden werden die Komponenten mit ihren Aufgaben, ihrer Funktionsweise und den Schnittstellen dargestellt. Es erfolgen auch Abgrenzungen zu Objekten, die nicht Gegenstand der Spezifikation sind.

3.1 Teilnehmer-Komponente

Für die Zwecke der Beschreibung des Aufbaus einer MailTrusT-PKI wird mit dem Begriff Teilnehmer ausschließlich der Endanwender als eigentlicher Nutzer der PKI bezeichnet. Es wird zwischen dem Teilnehmer als Person und der Teilnehmer-Komponente unterschieden, die er verwendet.[3]

Der Teilnehmer ist Inhaber eines oder mehrerer Schlüsselpaare, die er entweder selbst generiert hat oder von einer CA/RA generieren gelassen hat.[4] Diese und ggf. weitere sensitive Informationen werden in einem sog. Token gespeichert, auf das innerhalb der Teilnehmer-Komponente über eine Token-Schnittstelle zugegriffen wird.

Über die Token-Schnittstelle werden nicht nur kryptographische Informationen abgerufen, sondern auch die Durchführung kryptographischer Operationen in einer sicheren Umgebung angestoßen. Entsprechend dem Modulkonzept können Tokenhersteller und Hersteller von MailTrusT-Anwendungen verschieden sein. Für die Hersteller der Anwendungen gibt es eine Programmierschnittstelle, über die sie die erforderlichen kryptographischen Operationen aufrufen können.

Die Spezifikation enthält ein MailTrusT-Profil für eine Token-Schnittstelle auf der Basis der in [PKCS11 97] spezifizierten (Cryptoki-) Schnittstelle, das als „MTT-

[3] Diese Komponente wird häufig auch als Client oder Anwenderstruktur bezeichnet.

[4] In der Regel verfügt ein Teilnehmer mindestens über zwei Schlüsselpaare, da er für die Signaturbildung und die Entschlüsselung von Dokumenten verschiedene Schlüssel verwendet.

Cryptoki“ bezeichnet wird und im Dokument „Token“ beschrieben ist.

Ein sicherer lokaler Speicher für private Schlüssel und andere sensitive Informationen des Teilnehmers wird allgemein als das Personal Security Environment (PSE) bezeichnet. Das Format der PSE ist nicht Gegenstand der vorliegenden Spezifikation.[5]

Die Schnittstelle zwischen verschiedenen Teilnehmer-Komponenten bildet den Schwerpunkt der Version 1.1 der MailTrusT-Spezifikation. Diese Schnittstelle, für die MailTrusT-Nachrichten auf der Basis von PEM[6] definiert sind, ist im wesentlichen unverändert geblieben.[7] Zur Vorbereitung eines schrittweisen Übergangs zu MailTrusT-Nachrichten auf der Basis von S/MIME wurde ein MailTrusT-Profil für S/MIME auf der Basis der „Cryptographic Message Syntax“ (CMS) [SMIME CMS 98] spezifiziert.

Über die Schnittstellen zu RA, CA und DIR, die im folgenden beschrieben werden, erfolgt die Registrierung des Teilnehmers, können PKI-Management-Nachrichten ausgetauscht sowie Zertifikate und Sperrlisten abgerufen werden.

3.2 Registrierungsstelle (RA)

Jeder Teilnehmer einer PKI muß zunächst identifiziert und registriert werden, bevor die CA für ihn Zertifikate ausstellen kann. Eine zuverlässige Identifizierung des Teilnehmers setzt voraus, daß der Teilnehmer bei einer für die Registrierung geeigneten Instanz vorstellig wird und sich ausweist. In der Regel wird es nicht ausreichend sein, daß es nur eine solche Instanz gibt (zentrales Modell).[8] Die vorliegende Spezifikation geht deshalb von einem dezentralen Modell aus, bei dem die Identifizierung und Registrierung auch durch mehrere RAs erfolgen kann.[9]

Jede RA muß stets über ein Zertifikat verfügen, mit der sie PKI-Management-Nachrichten digital signieren kann. Sie muß daher wie ein Teilnehmer identifiziert und registriert werden. Sie benötigt auch eine Token-Schnittstelle. Da PKI-Management-Nachrichten ein im Rahmen der vorliegenden Spezifikation neu definierter Typ einer MailTrusT-Nachricht sind, muß sie auch MailTrusT-Nachrichten verarbeiten können. Die RA verfügt insofern über die gleichen Schnittstellen wie ein Teilnehmer.

Originäre Aufgabe einer RA ist die Identifizierung und Registrierung von Teilnehmern. Daneben können den RAs weitere Aufgaben übertragen werden. Dazu zählen die Generierung von Schlüsseln und Zertifizierungsanträgen für Teilnehmer, die Entgegennahme und Weiterleitung von Sperranträgen sowie die Personalisierung und Ausgabe von Token.[10]

Die Spezifikation enthält keine Vorgaben hinsichtlich der Zuordnung dieser Aufgaben zu Komponenten. Aus den o.g. Gründen wird empfohlen, die Identifizierung und Registrierung durch eine RA durchführen zu lassen. Für die anderen Aufgaben kann keine allgemeine Empfehlung gegeben werden. Die Spezifikation ist jedoch darauf ausgerichtet, daß eine RA-Komponente diese Aufgaben erledigen kann. Auf diese Weise wird das größtmögliche Maß an Flexibilität gewährleistet.

Im folgenden werden die möglichen Aufgaben einer RA ein Überblick dargestellt:

Identifizierung und Registrierung

Die RA prüft die Identität des Teilnehmers anhand eines zuverlässigen Identitätsnachweises (z.B. eines amtlichen Ausweises). Bei der Registrierung erhält der Teilnehmer ein Sperrpaßwort mitgeteilt (bzw. kann ein selbstgewähltes Sperrpaßwort registrieren lassen), das er später für die Zwecke der Authentisierung von Sperranträgen verwenden kann.

Falls der Teilnehmer selbst Zertifizierungsanträge generieren und direkt an die CA übersenden will, erhält er auch einen initialen Authentisierungsschlüssel (Inital Authentication Key, IAK).[11] Der IAK darf nur für den ersten Zertifizierungsantrag des Teilnehmers verwendet werden. Es wird davon ausgegangen, daß der Teilnehmer sich ein Signaturschlüssel-Zertifikat ausstellen läßt und anschließend alle PKI-Management-Nachrichten digital signiert.[12]

Bei Sperrpaßwort und IAK handelt es sich um geheime Schlüssel, die zur Bildung eines sog. MACs (Message Authentication Code) verwendet werden. Diese Schlüssel müssen zusammen mit den bei der Registrierung angefallenen Daten vertraulich an die CA übermittelt werden.

Die Übermittlung dieser Daten ist nicht Gegenstand der Spezifikation. CA und RA können frei entscheiden, ob bzw. wie sie diese Daten unter Verwendung einer MailTrusT-Nachricht elektronisch austauschen.

Generierung von Schlüsseln und Zertifizierungsanträgen

Die Generierung von Schlüsseln und Zertifizierungsanträgen kann der Teilnehmer durch seine Komponente, seinen Token oder von der RA durchführen lassen.[13] Zertifizierungsanträge werden anschließend unter Verwendung der im Dokument „PKI-Management“ beschriebenen Nachrichten an die CA übermittelt.

Es wird empfohlen, daß die RA eine Vorprüfung eines durch den Teilnehmer generierten Zertifizierungsantrags durchführt, um Fehler frühzeitig erkennen und korrigieren zu können.[14]

---

[5] Eine Standardierung in diesem Bereich erfolgt z.Zt. durch den „Personal Information Exchange Syntax Standard“ [PKCS12 97].

[6] Privacy Enhanced Mail; siehe Horster/Portz, DuD 6/1994, S. 434-442.

[7] Aus diesem Grunde sind unter Beachtung gewisser Randbedingungen Komponenten nach der Version 1.1 zu Komponenten nach der vorliegenden Version kompatibel.

[8] Ein entscheidender Kostenfaktor beim Betrieb einer PKI sind die zeitlichen Aufwände der Teilnehmer, die anfallen, bevor der Teilnehmer das erste Zertifikat erhalten hat. Wegezeiten sind dabei von wesentlicher Bedeutung.

[9] Das zentrale Modell kann als Spezialfall des dezentralen Modells angesehen werden, bei den es nur eine RA gibt, die räumlich bei der CA angesiedelt ist.

[10] Zu den Aufgaben der RA gehört nicht die Zertifizierung von Schlüsseln, eine originäre Aufgabe einer CA.

[11] Der Teilnehmer verfügt zu diesem Zeitpunkt noch nicht über ein Signaturschlüssel-Zertifikat, so daß er sich nicht mittels digitaler Signatur authentisieren kann.

[12] Dies gilt grundsätzlich auch für Sperranträge. Ein häufiger Grund für einen Sperrantrag ist jedoch, daß der Teilnehmer seine PSE verloren hat und deshalb nicht mehr in der Lage ist, digitale Signaturen zu generieren. Aus diesem Grunde soll der Teilnehmer stets über ein Sperrpaßwort verfügen.

[13] Dabei wird davon ausgegangen, daß die Generierung von Schlüsseln und Zertifizierungsanträgen durch die gleiche Instanz erfolgt, d.h. es gibt kein gesondertes Protokoll für die Übertagung von Schlüsseln.

[14] Erfahrungen aus der Praxis haben gezeigt, daß fehlerhafte Zertifizierungsanträge keine Ausnahmeerscheinungen sind. Eine CA kann diesen in der Regel nur mit einer für den Teilnehmer mehr oder weniger verständlichen Fehlermeldung zurückweisen. Da RAs verglichen mit den Teilnehmern in der Regel über ein tieferes Verständnis der Anforderungen an einen Zertifizierungsantrag verfügen, kann eine Vorprüfung des Antrags einen positiven Effekt auf den Aufwand und damit die Kosten haben.

Die RA ist in der Regel auch in der Lage, eindeutige Namen für die Teilnehmer zu vergeben bzw. zu prüfen, ob ein vom Teilnehmer gewählter Name den Anforderungen entspricht und eindeutig ist.

Generierung von Sperranträgen für Teilnehmer-Zertifikate
Sperranträge können von Teilnehmern direkt oder von der RA an die CA gerichtet werden. In der Regel wird der Teilnehmer den Sperrantrag direkt an die CA richten. Die Beauftragung der RA kann jedoch z.B. dann vorteilhaft sein, wenn der Teilnehmer Chipkarte und Sperrpaßwort verloren hat.

Personalisierung und Ausgabe von Token
Die Personalisierung von Token ist nur Gegenstand der Spezifikation, soweit die Token-Schnittstelle hiervon betroffen ist. Teilnehmer, RA und CA müssen in der Lage sein, Token über diese Schnittstelle zu personalisieren. Für die optische Personalisierung von Token werden keine Vorgaben gemacht.

Auch die Ausgabe des Tokens ist nicht Gegenstand der Spezifikation. Unter Sicherheitsgesichtspunkten ist es in der Regel vorteilhaft, daß der Token dem Teilnehmer direkt übergeben wird. Allerdings macht dies in der Regel einen weiteren Besuch des Teilnehmers bei der RA erforderlich.

3.3 Zertifizierungsstelle (CA)

Eine CA kann eine echte „vertrauenswürdige dritte Partei“ (Trusted Third Party, TTP) sein. Dies wird jedoch von der Spezifikation nicht vorausgesetzt. Häufig werden die CA und die Teilnehmer der gleichen Organisation angehören.

Für den inneren Aufbau einer CA enthält die Spezifikation keine Vorgaben. Die CA-Komponente wird häufig aus mehreren online- und offline-Komponenten bestehen, wobei der private Signaturschlüssel der CA nur über die offline-Komponente erreichbar ist.

Jede CA einer MailTrusT-PKI muß alle o.g. Aufgaben einer RA ausüben können, d.h. Identifizierung und Registrierung, Generierung von Schlüsseln und Zertifizierungsanträgen, Generierung von Sperranträgen sowie Personalisierung und Ausgabe von Token.

Auch die Identifizierung und Registrierung, eine originäre Aufgabe einer RA, muß von der CA-Komponente geleistet werden können, da dies zumindest für die Zertifizierung von RAs erforderlich ist. Eine RA-Komponente ist damit zugleich Teil eine CA-Komponente.

Mindestens eine CA innerhalb einer PKI muß in der Lage sein, RAs zu registrieren. Das Zertifikat der RA muß zwar nicht von der CA ausgestellt sein, für die sie tätig wird. Eine RA kann somit für mehrere CAs einer PKI tätig werden, wobei sie nur ein Zertifikat benötigt. Eine gegenseitige Registrierung von RAs ist nicht zu empfehlen. Selbst in diesem Fall müßte jedoch zumindest eine RA von einer CA registriert werden.

Originäre Aufgabe der CA ist die Generierung von Zertifikaten und Sperrlisten.

Generierung von Zertifikaten
Die CA generiert Zertifikate auf Antrag. Mit der PKI-Management-Nachricht „Zertifizierungsanfrage“ beginnt der Zertifizierungsprozeß, in dessen Verlauf weitere PKI-Management-Nachrichten, eine „Zertifizierungsantwort“ und eine „Bestätigungsnachricht“ ausgetauscht werden.

Nach Eingang einer positiven Bestätigungsnachricht stellt die CA das Zertifikat per LDAP in einem Verzeichnis bereit, falls der Teilnehmer dies wünscht. Das Zertifikat ist dann per LDAP öffentlich abrufbar.

Generierung von Sperrlisten
Die CA-Komponente muß in der Lage sein, Sperranträge, d.h. PKI-Management-Nachrichten vom Typ „Sperrantrag“, entgegenzunehmen und Sperrlisten zu generieren. Sperrlisten werden ebenfalls per LDAP in das Verzeichnis eingestellt, aus dem sie dann per LDAP öffentlich abrufbar sind.

Die Spezifikation erlaubt jedoch auch, daß die Sperrungen mehrerer CAs in sog. indirekten Sperrlisten enthalten sind. Eine CA generiert in diesem Fall eine Sperrliste für mehrere CAs, die dann keine eigenen Sperrlisten herausgeben müssen.

3.4 Verzeichnisdienst (DIR)

Ein Verzeichnisdienst einer MailTrusT-PKI stellt Zertifikate einer oder mehrerer CAs und die zugehörigen Sperrlisten zum Abruf bereit. Es ist somit nicht erforderlich, daß jede CA ihren eigenen Verzeichnisdienst betreibt.

Zertifikate und Sperrlisten werden von den CAs über einen geschützten Zugriff, der unautorisierte Änderungen des Verzeichnisinhalts verhindert, im Verzeichnis bereitgestellt. Der Abruf von Zertifikaten und Sperrlisten erfolgt anonym.

4 Fazit

Mit der Version 2 der MailTrusT-Spezifikation wird ein Standard gesetzt, der auf der Grundlage bewährter Zielvorgaben folgendes erreicht:

- Förderung der technischen Umsetzung und des praktischen Einsatzes des Konzepts der Digitalen Signatur in konkreten Produkten und Anwendungen durch die Entwicklung und Fortschreibung technischer Standards.
- Unterstützung und Motivation von Herstellern zur Neu- und Weiterentwicklung problemadäquater, interoperabler und standardkonformer Produkte zum sicheren Dokumentenaustausch.
- Unterstützung von Anwendern bei der Auswahl geeigneter Lösungen und Produkte zur Realisierung eines sicheren Dokumentenaustauschs durch Schaffung einer anerkannten, einheitlichen Bewertungsgrundlage bei der Produktentscheidung und damit zugleich Sicherstellung von Investitionssicherheit.

Die vollständige Spezifikation findet sich im Internet unter http://www.secorvo.de und http://www.teletrust.de.

Literatur

[ITU-T X.509 97] ITU-T X.509: Information Technology – Open Systems Interconnection – The Directory: Authentication Framework; 1997

[MTRUST 96] Fritz Bausspieß, TeleTrusT: MailTrusT Spezifikation, Version 1.1; Dezember 1996

[PKIX-CMP 98] C. Adams, S. Farrell: Internet X.509 Public Key Infrastructure – Certificate Management Protocols; Mai 1998

[PKIX-PRO 98] R. Housely, W. Ford, W. Polk, D. Solo: Internet X.509 Public Key Infrastructure – X.509 Certificate and CRL Profile; September 1998

[PKCS11 97] PKCS #11: Crytograhic Token Interface Standard; RSA Laboratories; Version 2.01; 22. Dezember 1997

[PKCS12 97] PKCS #12: Personal Information Exchange Syntax Standard; RSA Laboratories; Version 1.0 DRAFT; 30. April 1997

[SIGI-ZERT 99] Signatur-Interoperabilitätsspezifikation (SigI); Zertifikate; Version 3.0; Januar 1999

[SMIME CMS 98] Housley, R.: Cryptographic Message Syntax; Dezember 1998