Kryptographie- und Sicherheitsstandards

Diplomarbeit

Universität Hildesheim
Institut für Informatik
Samelsonplatz 1
D-31141 Hildesheim

Bearbeitet von:	Carsten Eilers[1] Hemmendorf Alte Heerstraße 24 D-31020 Salzhemmendorf
Abgabetermin:	2. März 1998
Gutachter:	Prof. Dr. Birgit Pfitzmann
Zweitgutachter:	Prof. Dr. Joachim Biskup
Betreuung:	Prof. Dr. Birgit Pfitzmann[2] & Matthias Schunter[3]

[1] e-mail: ceilers@informatik.uni-hildesheim.de
[2] e-mail: pfitzmann@cs.uni-sb.de
[3] e-mail: schunter@compuserve.com

Zusammenfassung

Diese Diplomarbeit behandelt Standards und Normen im Bereich Sicherheit, speziell in der Kryptographie, und dort besonders solche bezüglich Frameworks, d.h. Normen und Standards, die einen Rahmen für die Verwaltung und Anwendung kryptograpischer Verfahren spezifizieren.
In Kapitel 1 werden einige einleitende Definitionen und Erklärungen zusammengefaßt, in Kapitel 2 werden die existierenden Normungsinstitute und ihre Aufgaben beschrieben, in Kapitel 3 folgt eine Beschreibung der Standardisierung im Internet und die Gruppen, die sich im Rahmen der Standardisierung im Internet mit dem Bereich Sicherheit beschäftigen, werden in Kapitel 4 beschrieben. In Kapitel 5 werden einige Organisationen beschrieben, die Industriestandards definieren.
Danach werden in Kapitel 6 eine Anzahl von Standards über Frameworks genauer betrachtet und verglichen und in Kapitel 7 werden Vergleiche der in den Frameworks verwendeten Funktionen in Tabellenform zusammengefaßt. In Anhang C werden alle (gefundenen) Normen aufgelistet.

Erklärung

Hiermit versichere ich, daß ich diese Diplomarbeit selbständig erstellt und keine anderen als die angegebenen Quellen verwendet habe.

Hemmendorf, den 2. März 1998

Vorwort

Über diese Arbeit

Diese Diplomarbeit behandelt Standards und Normen im Bereich Sicherheit, speziell in der Kryptographie, und dort besonders solche bezüglich Frameworks, d.h. Normen und Standards, die eine Rahmen für die Verwaltung und Anwendung kryptograpischer Verfahren spezifizieren.
Im Kapitel 1 werden einige einleitende Definitionen und Erklärungen zusammengefaßt: Was ist ein Standard, was ist eine Norm, was ist Normung und einiges mehr. Danach wird in Kapitel 2 beschrieben, welche Normungsinstitute es gibt, welche Aufgaben sie haben und in welcher Beziehung sie zueinander stehen. In Kapitel 3 folgt eine Beschreibung der Standardisierung im Internet und die Gruppen, die sich im Rahmen der Standardisierung im Internet mit dem Bereich Sicherheit beschäftigen, werden in Kapitel 4 beschrieben. In Kapitel 5 werden einige Organisationen beschrieben, die Industriestandards definieren.
Danach wird in Kapitel 6 eine Auswahl von Standards genauer betrachtet, wobei der Schwerpunkt auf Frameworks liegt. Im sich anschließenden Kapitel 7 werden Vergleiche der in den Frameworks verwendeten Funktionen in Tabellenform zusammengefaßt.
In Anhang A werden die Mitglieder des europäischen Normungsinstituts CEN (siehe Abschnitt 2.2.1) aufgelistet, in Anhang B die des internationalen Normungsinstituts ISO (siehe Anschnitt 2.3.1). In Anhang C werden dann alle (gefundenen) Normen aufgelistet.

Danksagungen

Offiziell betreut wurde diese Arbeit von Prof. Dr. Birgit Pfitzmann (jetzt Universität des Saarlandes, Saarbrücken), real auch von Matthias Schunter (jetzt Universität Dortmund). Gerrit Bleumer (jetzt AT&T Research) lieferte einige Einstiegspunkte zum Thema „Standardisierung“, und Dr. Michael Waidner (IBM Research Zürich) war an der Entwicklung des Themenschwerpunktes (Frameworks) beteiligt und lieferte viele Anfangspunkte dazu. Bei allen vier möchte ich mich hiermit herzlich bedanken. Aufgrund der besonderen Umstände durch die Schließung der Informatik an der Universität Hildesheim wurde diese Arbeit weitgehend aus der Ferne betreut, eine für mich interessante Erfahrung, für die ich mich bei der niedersächsischen Landesregierung unter Ministerpräsident Schröder, dem Niedersächsischen Ministerium für Wissenschaft und Kultur sowie Frau Ministerin Schuchardt bedanken möchte.
Ebenso danke ich Prof. Dr. Joachim Biskup (jetzt Universität Dortmund), der sich bei der anfänglichen Planung der Diplomarbeit bereit erklärte, sie zu betreuen, sowie Wolfgang Heidrich (BAPT, Abteilungsleiter für Standardisierung, Technische Vorschriften, Zulassung und Sicherheit in der Telekommunikation, Chanisiusstraße 21, 55122 MAINZ, wolfgang.heidrich@bapt.de), der mir auf eine Anfrage

nach der in Deutschland für die Normung im Bereich Telekommunikation zuständigen Institution eine sehr ausführliche Antwort-Mail schickte, und Stewart Sanson (CEN, Manager - Promotion and information, Rue de Strassart 36, B-1050 Brüssel, sanson@cenclcbel.be), der mir auf meine Anfrage nach einem Bild der CEN-Organisation und einer Liste der CEN-Mitglieder einige sehr hilfreiche Broschüren schickte.

Kurze Inhaltsübersicht

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Kapitel 1

Einleitung

In diesem Kapitel werden einige einleitende Definitionen und Erklärungen zusammengefaßt - zum einen, um einen ersten Überblick über Sinn und Zweck dieser Arbeit zu geben, zum anderen, damit „man weiß, worüber man spricht“.

1.1 Was sind Standards und Normen?

Nach [Broc_??] ist eine *Norm* eine „allgemein anerkannte Regel“, nach [PCLe_94] ist sie „eine technische Beschreibung, die für jedermann zugänglich ist und die im Einvernehmen aller interessierter Kreise erstellt wurde. Sie beruht auf abgestimmten Ergebnissen von Wissenschaft, Technik und Praxis. Sie erstrebt einen größtmöglichen Nutzen für die Allgemeinheit.“ Diese Definitionen gelten analog auch für Standards.
Standards werden in zwei Kategorien unterteilt: *de facto* und *de jure*.
Die De-facto-Standards sind die Standards, die sich aufgrund der hohen Akzeptanz eines Produkts oder einer Produktreihe ergeben haben, ohne daß dies durch einen formellen Plan so vorgegeben war. Ein Beispiel für De-facto-Standards sind die IBM-kompatiblen PC als kleine Bürocomputer, der dadurch entstand, daß viele Hersteller die Originalmaschinen von IBM weitgehend identisch nachbauten und diese auch von den Anwendern gekauft wurden [Tane_97]. De-jure-Standards sind formelle Gesetzesnormen, die von einer autorisierten Normungsinstitution entwickelt wurden [Tane_97]. Diese Normungsinstitute können in zwei Gruppen eingeteilt werden: Diejenigen, die aufgrund von Regierungsverträgen entstanden sind, und die freiwilligen Organisationen, die aus dem Zusammenschluß an einer Normung interessierter Kreise entstanden sind. Die Normungsinstitutionen werden im Kapitel 2 beschrieben.
Der Begriff *Norm* wird meist für die von offiziellen Normungsinstituten von Amts wegen herausgegebenen Standards verwendet, d.h. für die De-jure-Standards, während mit *Standard* die de facto vom Markt übernommenen Technologien oder die von nicht offiziellen Organisationen veröffentlichten Standards, also die De-facto-Standards, bezeichnet werden. Diese Verwendung der Begriffe Norm und Standard ist jedoch weder definiert noch normiert. In dieser Arbeit wird diese Konvention ebenfalls (weitgehend) eingehalten.

1.2 Was ist Normung?

Normung ist nach [Broc_??] eine „planmäßige, durch interessierte Kreise gemeinschaftlich durchgeführte einheitliche Festlegung (Norm) von Begriffen, Kennzeichen, Meßtechniken sowie produkt- oder materialspezifischen Eigenschaften (Qua-

lität, Abmessung, Form, Farbe, Rezeptur, technische Leistungsparameter). Normung fördert die Rationalisierung und Qualitätssicherung in Wirtschaft, Technik, Wissenschaft und Verwaltung, dient einer sinnvollen Ordnung und der Information auf dem jeweiligen Normungsgebiet, schafft Klarheit zwischen Lieferanten und Kunden, erleichtert Konstruktion, Fertigung und Instandhaltung, trägt zur Verständigung in Wissenschaft und Technik bei und setzt Maßstäbe für Qualität und Sicherheit.“
„Normung ist die einmalige, bestimmte Lösung einer sich wiederholenden Aufgabe unter den jeweils gegebenen wissenschaftlichen, technischen und wirtschaftlichen Möglichkeiten (Otto Kienzle, Mitbegründer des DIN, von [http://www.din.de]“.
Natürlich ist auch der Begriff Normung genormt: „Normung ist die planmäßige, durch die interessierten Kreise gemeinschaftlich durchgeführte Vereinheitlichung von materiellen und immateriellen Gegenständen zum Nutzen der Allgemeinheit.“ [DIN_820, Teil 1]
Neben diesen ausführlichen Definitionen kann man Normung aber auch einfach als die Tätigkeit der „Erstellung von Normen“ betrachten.

1.2.1 Wozu Normung?

Vorteile, die sich aus der Normung ergeben, sind in [http://www.iso.org] aufgeführt. Im folgenden werden davon diejenigen aufgeführt, die sich für den Bereich der Sicherheit in der Informationstechnik ergeben:

- Verbesserung der Produktqualität und Zuverlässigkeit zu einem angemessenem Preis
- Größere Kompatibilität und Interoperabilität
- Vereinfachungen für eine Verbesserung der Handhabung
- Verringerung der Anzahl an Systemen und damit eine Verringerung der Kosten
- Steigerung der Distributionseffizienz und Vereinfachung der Wartung

Als Gründe, die für die Normung allgemein sprechen, sind in [http://www.iso.org] außer den Vorteilen noch aufgeführt:

- Weltweiter Fortschritt bei der Liberalisierung des Handels durch einheitliche Grundlagen in Form der Normen.
- Gegenseitige Durchdringung von Sektoren, wenn Produkte eines Sektors auch in einem anderen verwendet werden, wie z.B. die Verwendung von elektronischer Datenverarbeitung in allen Bereichen von Industrie, Handel und Dienstleistung.
- Weltweite Kommunikationssysteme, die auf einer einheitlichen Stufe standardisiert sein müssen.
- Globale Standards für neue Technologien, um z.B. die Terminologie zu vereinheitlichen.
- Entwicklungsländer brauchen eine Standardisierungs-Infrastruktur als Basis ihrer Entwicklung.

1.2.1.1 Vorteile von Normung gegenüber Standardisierung

Wieso sind nun aber Normen Industriestandards vorzuziehen? Zum einen begibt man sich bei Industriestandards - unabhängig davon ob solche einzelner Unternehmen oder solcher von Verbänden wie z.B. der ECMA - immer auf eine mehr oder weniger große „Insel", auf der man auf die Versorgung durch einige wenige Unternehmen angewiesen ist, während man bei der Verwendung von offiziellen Normen auf das Angebot vieler konkurrierender Anbieter zurückgreifen kann.
Zum anderen ist besonders im Bereich der Kryptographie die Gefahr groß, daß bei Standards, die nicht von einer breiten Öffentlichkeit getragen werden, und die evtl. sogar nur unvollständig veröffentlicht werden, schwache Algorithmen oder sogar Algorithmen mit Hintertüren verwendet werden, die es der standardisierenden Stelle erlauben, verschlüsselte Texte unerkannt mitzulesen oder signierte Texte unerkannt zu verändern. Verwendet man dagegen genormte, öffentlich bekannte Verfahren, kann man diese zum einen selber genau untersuchen (lassen) und zum anderen darauf vertrauen, daß sie von vielen Spezialisten untersucht wurden und werden [Pfit_90], [WaPP_87]. Allerdings können auch Industriestandard untersucht und für Sicher befunden werden, wenn er öffentlich bekannt und eine einheitliche Lizensierung dieses Standards garantiert ist, da dann keine weiteren Unterschiede zu einer Norm bestehen außer dem, daß der Herausgeber keine öffentliche Organisation ist.
Die Normung hat aber auch einige Nachteile, so ist sie oft aufgrund des Entscheidungsprozeßes langsam, oder die Norm wird durch das Eingehen vieler Kompromisse unklar und gegenüber dem eigentlichen Ziel abgeschwächt, wie z.B. die Normung von RSA und DES fehlschlug und nur zu einer Norm von Protokollen, die kryptographische Systeme verwenden, führte [WaPP_87].

1.3 Was ist Sicherheit?

Nach [EN_45020] ist *Sicherheit* die „Freiheit von unvertretbaren Schadensrisiken (Anmerkung: In der Normung wird im allgemeinen die Sicherheit von Erzeugnissen, Verfahren und Dienstleistungen im Hinblick auf die Erzielung eines optimalen Ausgleichs einer Anzahl von Faktoren betrachtet, wobei auch nichttechnische Faktoren, wie menschliches Verhalten, eingeschlossen sind und wobei vermeidbare Schadensrisiken für Personen und Güter auf ein vertretbares Ausmaß vermindert werden) [EN_45020, Seite 13]"
Was bedeutet *Sicherheit* aber bezogen auf die Informatik, speziell für Rechnernetze? Eine „einfache" Definition von Sicherheit für diesen Bereich existiert nicht - statt dessen werden z.B. von Andreas Pfitzmann mögliche Bedrohungen und korrespondierende Schutzziele genannt [Pfit_93]:

- unbefugter Informationsgewinn, d.h. Verlust der *Vertraulichkeit*
- unbefugte Modifikation von Information, d.h. Verlust der *Integrität*
- unbefugte Beeinträchtigung der Funktionalität, d.h. Verlust der *Verfügbarkeit*

Kapitel 2

Normung

In diesem Kapitel werden die verschiedenen Normungsinstitute, ihre Aufgaben und Kompetenzen jeweils auf nationaler (Abschnitt 2.1), regionaler (europäischer) (Abschnitt 2.2, Seite 19) und internationaler (Abschnitt 2.3, Seite 29) Ebene beschrieben. Außerdem wird für jeden dieser Bereiche die Durchführung eines Normungsvorganges beschrieben.

2.1 Nationale Normung

Nationale Normung ist die Normung in bzw. für einen einzelnen Staat. Im folgenden wird die nationale Normung am Beispiel Deutschlands beschrieben.

2.1.1 Normung in Deutschland

Die Normungsinstitute für Deutschland sind das Deutsche Institut für Normung e.V. (DIN), die Deutsche Elektrotechnische Kommission im DIN und VDE (DKE) und das Bundesamt für Post und Telekommunikation (BAPT). (Diese Institute und ihre Aufgaben werden im folgenden näher beschrieben.)

2.1.1.1 Deutsches Institut für Normung e.V. (DIN)

Das *Deutsches Institut für Normung e.V.* (DIN), ein eingetragener Verein mit Sitz in Berlin, ist aufgrund des Normenvertrags (s.u) für die Normung in Deutschland zuständig. Das DIN ist keine staatliche Instanz, sondern eine Vereinigung von Herstellern, Handel, Verbrauchern, Handwerk, Dienstleistungsunternehmen, Wissenschaft, technischer Überwachung, Staat und allgemein jedem, der ein Interesse an der Normung hat. Seine Aufgabe besteht darin, den Stand der Technik zu ermitteln und daraus Deutsche Normen zu entwickeln. Diese Normen als „Regeln der Technik dienen der Rationalisierung, der Qualitätssicherung, der Sicherheit, dem Umweltschutz und der Verständigung in Wirtschaft, Technik, Wissenschaft, Verwaltung und Öffentlichkeit. Die Normungsarbeit wird in 4100 Arbeitsausschüssen ... geleistet. Fertige Normen werden mindestens alle 5 Jahre auf ihre Aktualität hin überprüft" [http://www.din.de], und je nach Notwendigkeit unverändert bestätigt, überarbeitet oder zurückgezogen.
Im Laufe der Zeit hat sich der Schwerpunkt der Normensetzung im DIN weg von der Entwicklung nationaler (DIN-)Normen hin zu der Entwicklung europäischer (CEN-)Normen und internationaler (ISO-)Normen gewandelt. Tabelle 2.1 zeigt die Schwerpunktverschiebungen in der Normungsarbeit des DIN[1].

[1] Die Werte wurden aus Grafiken in [DIN_95, Anlage 5 - 7] abgelesen; da diese Grafiken aber

Normung	1984	1990
Nationale Normung (Vorhaben)	> 80 %	< 30 %
Europäische Normung (Vorhaben)	< 15 %	> 55 %
Internationale Normung (Vorhaben)	ca. 5 %	> 15 %
Nationale Normung (Entwürfe)	> 60 %	< 40 %
Europäische Normung (Entwürfe)	< 10 %	> 30 %
Internationale Normung (Entwürfe)	< 30 %	< 35 %
Nationale Normung	> 60 %	ca. 60 %
Europäische Normung	ca. 5 %	> 10 %
Internationale Normung	ca. 30 %	ca. 25 %

Tabelle 2.1: Schwerpunktverschiebungen in der Normungsarbeit des DIN nach [DIN_95, Anlage 5 - 7] in % der Anzahl der herausgegebenen Normen

Die offizielle Grundlage für die Bedeutung von DIN-Normen in Deutschland und den Status des DIN ist im sogenannten *Normenvertrag* zwischen Deutschland und dem DIN von 1975 festgelegt [DIN2_75], in dem das DIN von der Bundesregierung als für Deutschland zuständige Normungsinstitution anerkannt wurde. Insbesondere ist dabei von Bedeutung, daß die Normen des DIN aufgrund ihrer Entstehung, Trägerschaft, Inhalt und Anwendungsbereich den Charakter von Empfehlungen mit einer technisch-normativen Wirkung haben. Aus sich heraus besitzen sie keine rechtliche Verbindlichkeit und die Beachtung ist für jedermann frei. Trotzdem werden die Normen, als Beschreibung des Standes der Technik, auch in Gesetzen für die Beschreibung technischer Sachverhalte verwendet [DIN2_75, Erklärung des DIN zum Normenvertrag].
Das DIN orientiert seine Arbeit nach [http://www.din.de] an folgenden zehn Grundgedanken:

1. Freiwilligkeit
   Niemand muß beim DIN mitarbeiten, die Arbeitsergebnisse sind Empfehlungen.

2. Öffentlichkeit
   Alle Normungsvorhaben und Entwürfe zu DIN-Normen werden öffentlich bekanntgemacht, Kritiker werden angehört. Das DIN informiert über alle technischen Regeln Deutschlands.

3. Beteiligung aller interessierten Kreise,
   zum einen durch die Möglichkeit der Mitgliedschaft, zum anderen durch Veröffentlichung der Normungsanträge, der Ankündigung der Veröffentlichung eines Normentwurfs etc. im DIN-Anzeiger für technische Regeln.

4. Einheitlichkeit und Widerspruchsfreiheit
   Das Deutsche Normenwerk umfaßt alle technischen Disziplinen, die Regeln der Normungsarbeit sichern seine Einheitlichkeit, die Normenprüfstelle sorgt für Widerspruchsfreiheit.

5. Sachbezogenheit
   DIN-Normen sind ein Abbild der Wirklichkeit und Niederschrift des technischen Erfahrungsstandes.

---

nur eine 10er-Einteilung für die %-Angaben haben, handelt es sich nur um ungefähre Werte. Die Werte für 1990 sind eine sich aufgrund der Halbjahres-Bilanz für 1990 abzeichnende Tendenz.

6. Konsens
   Das Normungsverfahren ist auf Konsens aufgebaut (siehe Normentwicklung, Abschnitt 2.1.1.1.2, Seite 12).

7. Ausrichtung am Stand der Technik
   Das DIN bewegt sich im Rahmen, den die naturwissenschaftliche Erkenntnis vorgibt.

8. Ausrichtung an den wirtschaftlichen Gegebenheiten
   Jede Normensetzung wird auf ihre wirtschaftliche Wirkungen hin untersucht. Es wird nur das unbedingt Notwendige genormt.

9. Ausrichtung am allgemeinen Nutzen
   Ausgehend von der naturwissenschaftlichen Erkenntnis, haben DIN-Normen gesamtgesellschaftliche Ziele einzubeziehen. Es gibt keine wertfreie Normung. Der Nutzen für alle steht über dem Vorteil einzelner oder weniger.

10. Internationalität

2.1.1.1.1 Die Organisation des DIN

Die Organisation des DIN ist in seiner Satzung [DIN_91] beschrieben. Die Organe des DIN und ihre Aufgaben sind im folgenden aufgelistet. Aufgaben, die die eigentliche Normungsarbeit betreffen, sind *kursiv hervorgehoben*, einige der Aufgaben, die die Normungsarbeit nicht betreffen, werden nicht erwähnt.
Abbildung 2.1 zeigt die Organe im Zusammenhang.

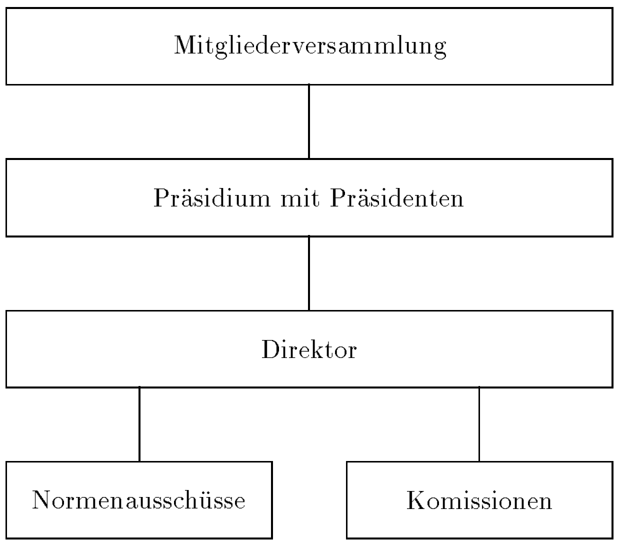

Abbildung 2.1: Die Organe des DIN

2.1.1.1.1.1 Die Mitgliederversammlung

Die Mitgliederversammlung wird vom Vorstand mindestens alle 2 Jahre einberufen. Sie ist zuständig für

- die Entgegennahme des Geschäftsberichts,
- die Entlastung des Präsidiums und
- die Wahl der Mitglieder des Präsidiums.

2.1.1.1.1.2 Das Präsidium

Das Präsidium besteht aus mindestens 30, höchstens 45 gewählten Mitgliedern, die ehrenamtlich tätig sind und im Berufsleben stehen müssen. Zusätzlich gehören von Amts wegen der Präsident, seine beiden Stellvertreter und der Direktor dem Präsidium an.
Das Präsidium tritt nach Bedarf, mindestens jährlich, zusammen. Es wählt auf der ersten Sitzung nach Beginn seiner Amtszeit aus seiner Mitte den Präsidenten und seine zwei Stellvertreter. Das Präsidium ist für alle Beschlüsse zuständig, die nicht ausdrücklich der Mitgliederversammlung oder dem Präsidenten vorbehalten sind. In der Geschäftsordnung des Präsidiums [DIN1_75] sind seine Aufgaben aufgeführt, von denen im folgenden die aufgeführt werden, die die Normungsarbeit betreffen:

- *Stellungnahmen zu Norm-Entwürfen*
- *Entscheiden über Gründung und Auflösung von Normenausschüssen und über Meinungsverschiedenheiten zwischen Normenausschüssen untereinander*
- *Entscheiden über die fachliche Zuständigkeit von Normenausschüssen und deren Namen*
- *Schlichten bei Meinungsverschiedenheiten zwischen Normenausschüssen und Direktor*
- *Entscheiden über das Ablehnen eines Normungsantrages bzw. das Absetzen einer Norm-Vorlage*
- *Festlegen einer Geschäftsordnung für das Schiedsverfahren*
- *Einsetzen von Schiedsausschüssen, Bestimmen des Vorsitzenden und gegebenenfalls von Mitgliedern*

Das Präsidium kann zum Erledigen seiner Aufgaben und zu seiner Unterstützung Ausschüsse einsetzen. Ständige Ausschüsse sind

- die Normenprüfstelle (NP) des DIN,
  die Norm-Entwürfe daraufhin überprüft, ob die Regeln und Grundsätze für die Normungsarbeit eingehalten sind und die Normen im Auftrag des Präsidenten in das Deutsche Normenwerk aufnimmt.
- der Verbraucherrat des DIN,
  der die Lenkungs- und Arbeitsgremien des DIN in Fragen berät, die für nichtgewerbliche Endverbraucher von Interesse sind.
- der Deutsche Rat für Konformitätsbewertung im DIN (DIN KonRat),
  der über alle Fragen der Konformitätsbewertung berät.

2.1.1.1.1.3 Der Präsident

Der Präsident und seine Stellvertreter sind Vorstand gemäß § 26 BGB. Jeder von ihnen ist alleinvertretungsberechtigt. Im Innenverhältnis des Vereins ist ausschließlich der Präsident handlungsbefugt, nur im Verhinderungsfall sein 1. Stellvertreter und, falls auch dieser verhindert ist, sein 2. Stellvertreter.
Seine Aufgaben werden ebenfalls in der Geschäftsordnung des Präsidiums [DIN1_75] festgelegt, im folgenden werden davon die die Normungsarbeit betreffenden aufgeführt:

- *Bestätigen der Gründung neuer Normenausschüsse*
- *Bestätigen der Vorsitzenden und deren Stellvertreter von Normenausschüssen sowie der Obleute von selbständigen Arbeitsausschüssen und gegebenenfalls deren Abberufung*
- Entscheiden über Einsprüche gegen Entscheidungen der Normenprüfstelle nach erfolglosem Vermittlungsversuch des Direktors
- Entscheiden in Eilfällen mit der Maßgabe, daß zu der Entscheidung nachträglich ein Beschluß des Präsidiums einzuholen ist.

2.1.1.1.1.4 Der Direktor
Der Direktor wird auf Vorschlag des Präsidenten und seiner beiden Stellvertreter vom Präsidium berufen und ist Angestellter des DIN. Er ist im Rahmen der von Mitgliederversammlung und Präsidium gefaßten Beschlüsse für eine ordnungsgemäße Geschäftsführung des DIN und der damit verbundenen Gesellschaften in fachlicher, organisatorischer und kaufmännischer Hinsicht verantwortlich.

2.1.1.1.1.5 Die Normenausschüsse (NA)
Arbeitsausschüsse werden zu Normenausschüssen (NA) zusammengefaßt. In ihnen wird die Normungsarbeit durchgeführt. Ihre Aufgaben, Stellung, Arbeitsweise und Finanzierung werden durch Festlegungen der jeweils zuständigen Organe des DIN beschlossen und in DIN 820 oder in Richtlinien oder ergänzenden Bestimmungen veröffentlicht. In Ausnahmefällen kann die Normungsarbeit auch in Arbeitsausschüssen durchgeführt werden, die keinem Normungsausschuß zugeordnet sind.
Die Aufgaben der Normenausschüsse sind in der Richtlinie für Normenausschüsse [DIN_90] folgendermaßen festgelegt: „Ein NA trägt verantwortlich die nationale Normung auf seinem Fach- und Wissensgebiet und nimmt auf diesem auch die Mitarbeit bei der europäischen und internationalen Normung wahr. Er setzt sich für die Einführung der Deutschen Normen seines Fachgebietes in den davon berührten Lebensbereichen ein und wirkt bei der Bearbeitung von Zertifizierungsaufgaben im Rahmen der „Grundsätze für die Zertifizierungsarbeit“ mit [DIN_95, Punkt2, Aufgaben eines NA]“.
Die Gründung eines NA kann vom Direktor des DIN dem Präsidium des DIN vorgeschlagen werden, wenn

1. ein Normungsantrag vorliegt, für den kein bestehender NA sich zuständig erklärt oder
2. nach Beratung in den/dem betroffenen NA mehrere NA zu einem NA zusammengefaßt werden sollen oder
3. wegen des Umfangs und/oder der Bedeutung eines Teiles des Arbeitsgebietes eines NA dieser Teil als neuer NA ausgegliedert werden soll.

Stimmt das Präsidium der vorgeschlagenen Gründung, dem Namen und dem Arbeitsgebiet zu, so lädt der Direktor des DIN die interessierten Kreise zu einer Gründungssitzung ein und beruft einen kommisarischen Geschäftsführer. Die Gründungssitzung leitet ein Mitglied der Geschäftsleitung oder der Geschäftsführer.
Auf der Gründungssitzung wird festgestellt, ob alle interessierten Kreise eingeladen worden sind und ob Interesse an der Gründung eines neuen NA besteht. Dann wird der NA offiziell gegründet, das vorläufige Arbeitsprogramm aufgestellt, die Finanzierung festgelegt, ein Beirat, der Vorsitzende und seine Stellvertreter gewählt sowie gegebenenfalls Arbeitsausschüsse und deren kommissarische Obleute eingesetzt. Die Gründung, die Vorsitzenden und seine Stellverteter müssen durch den Präsidenten

des DIN bestätigt werden. Die Auflösung eines NA erfolgt durch Beschluß des Präsidiums des DIN.
Die Organisation ist auf das unbedingt notwendige Maß zu beschränken, die Organe eines NA sind:

1. der Mitarbeiterkreis,
   bestehend aus den Mitgliedern des Beirats und des Förderkreises, den Mitarbeitern der Fachbereiche, der Arbeitsausschüsse und der Unterausschüsse. Er wählt die Beiratsmitglieder und kann über die Selbstauflösung des NA entscheiden.

2. der Beirat oder Lenkungsausschuß,
   der aus maximal 21 Mitgliedern besteht, die für jeweils 3 Jahre gewählt werden. Seine Aufgaben umfassen unter anderem die Wahl des Vorsitzenden und seiner Stellvertreter und die Aufstellung des Arbeitsprogramms des NA unter Berücksichtigung der Wirtschaftlichkeit, des Standes der Technik, der Erkenntnisse der Wissenschaft und der Rechtsentwicklung sowie der europäischen und internationalen Harmonisierung technischer Regeln. Außerdem kann er Arbeitsausschüsse und Fachbereiche einsetzen oder auflösen. Er hat für die Darstellung des NA und seiner Arbeit in der Öffentlichkeit zu sorgen sowie für die Einführung seiner Normen in der Praxis zu sorgen.

3. der Vorsitzende,
   der ebenso wie seine Stellvertreter vom Beirat auf 3 Jahre gewählt wird. Er vertritt den NA nach außen und überwacht die Beachtung der DIN 820, der Beschlüsse des Präsidiums des DIN sowie der Beschlüsse des Beirats des NA.

4. die Arbeitsausschüsse oder Komitees,
   die aus maximal 21 Mitgliedern bestehen sollen. Ihre Aufgaben umfassen unter anderem

   - die Wahl seines Obmanns (oder -frau) und dessen Stellvertreter,
   - die Aufstellung des Arbeitsprogramms,
   - *als zentrale Aufgabe die Erarbeitung und (gegebenenfalls unter Einschaltung des Beirats) Verabschiedung entsprechender Normen,*
   - die aktive Beteiligung an der einschlägigen europäischen und internationalen Normungsarbeit,
   - die Beachtung der gemeinsamen Regeln von CEN/CENELEC,
   - die Abgabe der deutschen Stellungnahme zu europäischen Normen,
   - das Beschließen über die Annahme internationaler Normen
   - die Überprüfung, ob seine zu erarbeitenden und bereits vorhandenen Normen im Einklang mit dem Stand der Technik, den Erkenntnissen der Wissenschaft sowie den anderen Deutschen Normen stehen.
   - die Erläuterung, Überarbeitung, Ergänzung oder Zurückziehung der Normen, für die er innerhalb des NA zuständig ist.

5. der Geschäftsführer,
   der die Geschäftsstelle des NA am Sitz des DIN leitet. Er und seine Mitarbeiter sind Angestellte des DIN. Seine Aufgabe ist es, die Geschäfte des NA in fachlicher, organisatorischer und finanzieller Hinsicht im Rahmen der Beschlüsse des Präsidiums und des Beirats des NA sowie der Festlegungen des Direktors des DIN verantwortlich zu führen.

2.1.1.1.1.6 Kommissionen

Kommissionen dienen nach [DIN_95, Beschlüsse des Präsidiums, S. 33f] der Koordinierung von Arbeitsgebieten des DIN und deren Verzahnung mit der Tätigkeit anderer Institutionen. Sie werden für ein fest umrissenes Aufgabengebiet eingerichtet und aufgelöst, sobald sie ihre Aufgabe erledigt haben. Kommissionen erarbeiten keine Normen, sondern sprechen Empfehlungen aus, deren Durchsetzung dem Direktor obliegt.
Die Mitglieder werden in Zusammenarbeit mit den interessierten Kreisen vom Direktor für eine Amtsperiode von 3 Jahren berufen, wobei eine zweimalige Wiederberufung möglich ist. Vorsitzender der Kommissionen ist in der Regel der Direktor.
Nach [http://www.din.de] existieren zur Zeit (Juli 1997) die Kommissionen „Kommission Reinhaltung der Luft (KRdL) im VDI und DIN“ und „Kommission Informationsgesellschaft (KIG) im DIN“. Letztere ist hier von Interesse:
Das DIN hat mit Unterstützung der interessierten Kreise als Plattform für die Behandlung normungspolitischer Fragen im Zusammenhang mit dem Aufbau der Globalen Informationsgesellschaft (GIS) die Kommission Informationsgesellschaft (KIG) gegründet. Ihre Aufgaben sind nach [http://www.din.de, „Die Aufgaben der KIG“]:

- Beratung und Entwicklung der DIN-Politik in grundsätzlichen Fragen der Regelsetzung (Normen und Spezifikationen) für eine Globale Informationsgesellschaft;
- Wahrnehmung der Beziehungen zu GIS-Gremien innerhalb und außerhalb der europäischen und internationalen Normungsorganisationen;
- Erarbeitung von deutschen Stellungnahmen und Beiträgen zu den Re-engineering-Aktivitäten der europäischen und internationalen Normung auf dem Gebiet der Informations- und Kommunikationstechnik (IKT), soweit sie normenausschußübergreifend sind (z.B. hat das ISO/IEC JTC 1 (siehe Abschnitt 2.3.1) am Projektmanagement orientierte Prinzipien eingeführt, um die Arbeitsprogramme auf anwendungsrelevante Projekte zu beschränken und die Normungsprozesse zu beschleunigen);
- normenausschußübergreifende Bewertung der Anforderungen an die IKT-Normung im Zusammenhang mit dem Aufbau der Globalen Informationsgesellschaft und Ableitung von Prioritäten für die Beteiligung bzw. Federführung des DIN in internationalen und europäischen Projekten;
- Bündelung der deutschen Aktivitäten mit dem Ziel, bei normenausschußübergreifenden Themen einen wirkungsvollen deutschen Beitrag zu leisten;
- Koordinierung der GIS-Aktivitäten der betroffenen Normenausschüssen;
- Betreuung von IKT/GIS-Pilotprojekten bezüglich der Erarbeitung von Spezifikationen bzw. Normen unter Beteiligung der betroffenen Unternehmen und Organisationen;
- Kontrolle von (und Koordinierung der deutschen Meinungsbildung zu) normenausschußübergreifenden Vereinbarungen der europäischen und internationalen IKT-Normung.

Mitglieder der KIG kommen zur Zeit aus den Bereichen Automobilindustrie, Banken und Versicherungen, Bundesministerium des Inneren, Bundeswirtschaftsministerium, Deutsche Telekom AG, Forschung und Lehre, Handel, IKT-Hersteller und -Anwender sowie den betroffenen Normenausschüssen

- Normenausschuß Bibliotheks- und Dokumentationswesen (NABD),

- Normenausschuß Kraftfahrzeuge (FAKRA),
- Normenausschuß Daten- und Warenverkehr in der Konsumgüterwirtschaft (NDWK),
- Normenausschuß Informationstechnik (NI),
- Normenausschuß Maschinenbau (NAM),
- Normenausschuß Medizin (NAMed),
- Normenausschuß Technische Produktdokumentation (NATPD).

In Hinblick auf die Anwendungen in der Globalen Informationsgesellschaft soll die KIG um Vertreter aus dem Bereich der Informationsanbieter (content provider) erweitert werden.

2.1.1.1.2 Die Entwicklung einer DIN-Norm

Der Arbeitsablauf für die Erarbeitung einer Deutschen Norm wird in [DIN_820, Teil 4, Abschnitt 2] festgelegt. Er besteht im einzelnen aus den folgenden Schritten:

1. Behandeln eines Normungsantrages
   Die Normungsarbeit beginnt mit einem begründeten Normungsantrag, der möglichst auch einen Norm-Vorschlag enthalten soll und bei der Geschäftsstelle des zuständigen Normungsausschusses oder selbständigen Arbeitsausschusses oder des DIN gestellt wird. Ein Normungsantrag kann von jeder interessierten Stelle oder jedermann gestellt werden. Der Antrag wird dem zuständigen Normenausschuß vorgelegt. Erklären sich mehrere Normenausschüsse oder kein Normenausschuß als zuständig, entscheidet die Geschäftsleitung des DIN über die Zuständigkeit oder die Gründung eines neuen Normenausschuß. Berührt das Thema des Normungsantrags die Aufgabenbereiche mehrerer Normenausschüsse, wird ein federführender Normenausschuß vereinbart, dieser wird Träger der Norm, die anderen Normenausschüsse können als Mitträger aufgenommen werden.

   Der zuständige Normenausschuß muß innerhalb von 3 Monaten über Annahme oder Ablehnung des Antrags entscheiden. Bei Annahme ist der für die Bearbeitung zuständige Arbeitsausschuß oder das zuständige Komitee zu bestimmen oder über die Gründung eines neuen Arbeitsausschuß zu entscheiden. Wird der Antrag abgelehnt, kann der Antragsteller gegen diese Entscheidung die Geschäftsleitung des DIN und bei deren Ablehnung das Präsidium des DIN, das verbindlich entscheidet, einschalten.

2. Aufstellen einer Norm-Vorlage
   Liegt dem Antrag ein Norm-Vorschlag bei, so wird dieser vom zuständigen Normenausschuß unverändert dem zuständigen Arbeitsausschuß als erste Norm-Vorlage zur Behandlung vorgelegt. Liegt kein Norm-Vorschlag vor, wird vom hauptamtlichen Bearbeiter unter Mitarbeit eines kleinen Arbeitskreises des Arbeitsausschusses eine Norm-Vorlage für die weitere Beratung erarbeitet.

3. Beraten bis zum Verabschieden der Norm-Vorlage, Veröffentlichung der Norm-Vorlage
   Ist eine Norm-Vorlage soweit bearbeitet worden, daß das Ergebnis der Öffentlichkeit zur Stellungnahme vorgelegt werden kann, verabschiedet der Arbeitsausschuß die Norm-Vorlage zum Druck als Norm-Entwurf. Die verabschiedete Fassung wird durch den hauptamtlichen Bearbeiter als Manuskript für den

Norm-Entwurf bearbeitet, von der Inneren Prüfstelle des DIN auf Einhaltung der Grundsätze an die Normungsarbeit überprüft und, nachdem eventuell notwendige Korrekturen durch den hauptamtlichen Bearbeiter vorgenommen wurden, an den Beuth-Verlag zur Veröffentlichung weitergeleitet.

4. Stellungnehmen zum Norm-Entwurf
Jedermann kann zum Inhalt des Norm-Entwurfs Zustimmungen, Einsprüche, Änderungs- und Ergänzungsvorschläge mit Begründung beim zuständigen Normausschuß einreichen. Dafür wird die Herausgabe eines Norm-Entwurfs im DIN-Anzeiger für technische Regeln angezeigt.

5. Behandlung der Stellungnahmen zum Norm-Entwurf, Verabschieden der endgültigen Fassung der Norm
Ergeben sich bei der Behandlung der Stellungnahmen keine wesentlichen Änderungen am Norm-Entwurf, wird die endgültige Fassung der Norm verabschiedet. Andernfalls wird ein neuer Norm-Entwurf unter Beachtung der Stellungnahmen durch den zuständigen Arbeitsausschuß erarbeitet und wieder bei Schritt 3 fortgefahren.

6. Bearbeiten der verabschiedeten Fassung als Manuskript für die Norm.

7. Prüfen des Manuskriptes für die Norm durch die Normenprüfstelle und Anfertigen des Kontrollabzuges, dieser wird vom hauptamtlichen Bearbeiter auf Übereinstimmung mit dem Manuskript überprüft.

8. Aufnehmen der Norm in das Deutsche Normenwerk durch die Normenprüfstelle und Veröffentlichung der Norm. Der Kontrollabzug ist die Norm-Urkunde, diese wird vom Beuth-Verlag als Grundlage für den Druck der Norm verwendet.

Bei der Entwicklung einer Norm gibt es noch die folgenden Sonderfälle [DIN_820, Teil 4, Abschnitt 3]:

- Vornormen,
  die das Ergebnis einer Normungsarbeit sind, aber wegen Vorbehalten zum Inhalt oder wegen eines gegenüber einer Norm abweichenden Aufstellungsverfahrens vom DIN nicht als Norm herausgegeben werden. Ein Beispiel für eine Vornorm findet sich in [DIN_95]: Die Vornorm „DIN 820, Teil 2, Gestaltung von Normen“, die eine Vornorm ist, da zu ihr kein Norm-Entwurf veröffentlicht wurde.

  Sie befassen sich mit normungswürdigen Gegenständen und werden zum geeigneten Zeitpunkt und nach notwendigen Veränderungen nach dem üblichen Verfahren in eine Norm umgewandelt oder ersatzlos zurückgezogen.

  Für Vornormen gelten die gleichen, in DIN 820 niedergelegten Grundsätze wie für Normen, insbesondere die Forderung nach Einheitlichkeit und Widerspruchsfreiheit zum Deutschen Normenwerk, jedoch mit folgenden Einschränkungen [DIN_820, Teil 4, Abschnitt 3.1]:

  - Die Entwurfsöffentlichkeit kann entfallen.
  - Das Schlichtungs- und Schiedsverfahren ist vereinfacht.
  - Vornormen sind nicht Teil des Deutschen Normenwerks.
  - Die äußere Gestaltung von Vornormen ist gegenüber Normen deutlich abzuheben.
  - Eine Vornorm ist bereits nach drei Jahren erstmals daraufhin zu überprüfen,

    * ob sie in eine Norm überführt werden kann, oder
    * ob sie ersatzlos gestrichen werden soll, oder
    * ob sie als Vornorm fortbestehen soll.

  Diese Entscheidung ist danach jährlich zu überprüfen.

  – Während der Laufzeit einer Vornorm darf ein ordentliches Normungsverfahren zum gleichen Gegenstand eingeleitet werden.
  – Beim Erscheinen einer Vornorm wird gegebenenfalls der vorhandene entsprechende Norm-Entwurf zurückgezogen.

- Kurzverfahren ohne Veröffentlichung eines Normentwurfs,
  das nur angewendet werden kann, wenn die Normenprüfstelle zugestimmt hat. Diese Zustimmung kann erteilt werden, wenn die Notwendigkeit für das Überspringen des Norm-Entwurfs nachgewiesen wurde, im zuständigen Arbeitsausschuß nachweislich alle interessierten Kreise am Aufstellen der beabsichtigten Norm beteiligt waren und durch die Veröffentlichung des Normentwurfs keine neuen Gesichtspunkte erwartet werden.

  Das Kurzverfahren darf grundsätzlich nur für Folgeausgaben angewendet werden, für Erstausgaben nur, wenn normenartige Veröffentlichungen anderer Institutionen übernommen werden sollen.

- Übernahme normenartiger Veröffentlichungen
  anderer Institutionen und ausländische Normen im Einvernehmen mit den Herausgebern.

- Übernahme regionaler (d.h. europäischer) oder internationaler Normen oder normenartiger Veröffentlichungen
  in deutscher Übersetzung, wobei bei der Erarbeitung die deutsche Öffentlichkeit unterrichtet und zur Stellungnahme aufgefordert wurde und ihre Stellungnahmen bei der Erarbeitung der regionalen oder internationalen Norm berücksichtigt wurde, was z.B. dadurch geschieht, daß das DIN an der Entwicklung von CEN- und ISO-Normen beteiligt ist.

  Die Übernahme Europäischer Normen von CEN/CENELEC und ETSI wird in [DIN_820, Teil 13] geregelt, die Übernahme von Internationalen Normen der ISO und IEC in [DIN_820, Teil 15].

Bestehende Normen müssen spätestens alle 5 Jahre überprüft werden. Entspricht eine Norm nicht mehr dem Stand der Technik, den bestehenden Grundnormen und den in ihr zitierten Normen, so muß der Inhalt überarbeitet werden, wenn die Norm weiter gelten soll.
Für die Überarbeitung einer Norm mit dem Ziel einer Folgeausgabe gilt der gleiche Geschäftsgang wie für die Herausgabe einer Erstausgabe.
Eine bestehende Norm wird durch die Veröffentlichung eines Norm-Entwurfs einer beabsichtigten Folgeausgabe nicht ungültig, es sei denn, die Norm wird ausdrücklich zurückgezogen. Im Gegensatz dazu wird ein Norm-Entwurf beim Erscheinen der Norm oder eines neuen Norm-Entwurfes gegenstandslos.
Eine Norm wird ohne Ersatz zurückgezogen, wenn ihr Weiterbestehen wissenschaftlich, technisch oder aus anderen Gründen nicht mehr vertretbar ist oder kein praktisches Bedürfnis mehr besteht.

2.1.1.2 Elektrotechnische Normung in Deutschland

Die elektrotechnische Normung wird in Deutschland von der *Deutschen Elektrotechnischen Kommission im DIN und VDE* (DKE) durchgeführt, die vom DIN und dem

Verband Deutscher Elektrotechniker (VDE) gemeinsam gebildet wird. Sie ist deutsches Mitglied in IEC und CENELEC. Ihre Aufgaben und Zuständigkeiten wurden in einem Vertrag zwischen dem DIN und dem VDE niedergelegt.
Die Ziele der DKE sind laut [http://www.vde.de]:

- Sichere Elektrizitätsanwendung in Beruf, Heim und Freizeit.
- Hoher Stand der technischen Regeln.
- Lösung von Problemen des Umweltschutzes und der Verbraucherfragen durch Normung.
- Weltweite Öffnung der Märkte durch internationale und europäische Harmonisierung der Normen.

Die DKE ist in die folgenden 9 Fachbereiche unterteilt [http://www.vde.de]:

1. Allgemeine Elektrotechnik, Werkstoffe der Elektrotechnik
2. Allgemeine Sicherheit, Errichten, Betrieb
3. Betriebsmittel der Energietechnik
4. Betriebsmittel der Stromversorgung, Nachrichtenkabel
5. Geräte für Haushalt und ähnliche Zwecke, Installationsgeräte
6. Bauelemente und Bauteile der Nachrichtentechnik und Elektronik
7. Nachrichten- und Informationstechnik, Telekommunikationstechnik
8. Medizintechnik, Elektroakustik, Ultraschall-Laser
9. Leittechnik

2.1.1.3 Telekommunikations-Normung in Deutschland

Im Gegensatz zur Normung in der Industrie mit nationalen, regionalen und internationalen Normungsinstitutionen (DIN/DKE, CEN/CENELEC, ISO/IEC) existieren im Bereich der Telekommunikation aus historischen Gründen in nahezu allen Ländern der Welt keine nationalen Normungsgremien, sondern die jeweiligen nationalen Fernmeldeverwaltungen haben für den nationalen Markt mit der nationalen Industrie nationale Techniken entwickelt und die Spezifikationen in ihren Lieferbedingungen festgelegt.
Für den internationalen Fernmeldeverkehr wurden und werden die zur Zusammenschaltung der nationalen Netze erforderlichen Spezifikationen bei der ITU (siehe Abschnitt 2.3.3) von den Experten der Fernmeldeverwaltungen und Betriebsgesellschaften im Zusammenarbeit mit der Industrie erarbeitet und in Form von (freiwilligen) Empfehlungen verabschiedet. Es gibt keinen nationalen Unterbau zur Erstellung der Empfehlungen, jedoch in einigen Ländern, wie z.B. auch in Deutschland, nationale Vorbereitungsrunden für die Tagungen der einzelnen Studienkommissionen.
Im europäischen Bereich wurden diese Arbeiten unter der Schirmherrschaft der CEPT (Europäische Konferenz der Post- und Fernmeldeverwaltungen) ausschließlich von Mitarbeitern der Fernmeldeverwaltungen erledigt und als gemeinsame CEPT-Empfehlungen herausgegeben.
Im Zuge der Deregulierung und zur Sicherstellung eines einheitlichen europäischen Telekommunikationsmarktes wurde das ETSI gegründet (siehe Abschnitt 2.2.3).

Hier sind Hersteller, Netzbetreiber, Verwaltungen usw. gleichberechtigte Mitglieder, die in themenorientierten Arbeitsgruppen Spezifikationen erstellen. Diese Spezifikationen haben zunächst rein empfehlenden Charakter, können aber durch ein europaweites Abstimmungsverfahren, das über die jeweiligen nationalen Normungsorganisationen läuft, zu einer EN (Europanorm) erhoben werden. In Deutschland findet diese Abstimmung im „Technischen Beirat ETSI“ (TB ETSI) beim DKE statt. Dazu wurde bei der DKE, im Prinzip spiegelbildlich zur technischen Organisation von ETSI, Komitees und Unterkomitees eingerichtet, die für das Einspruchsverfahren und die nationale Übernahme der von ETSI angenommenen Normen in das Deutsche Normenwerk des DIN zuständig sind [Priv_97]. Die Anwendung der Spezifikationen und der Normen ist nach wie vor freiwillig, bei öffentlichen Ausschreibungen sind sie jedoch zu berücksichtigen.
Einen Sonderfall stellen die von der europäischen Kommission in Auftrag gegebenen Spezifikationen dar. Sie werden im Auftrag der EU beim ETSI erstellt (TBR, Technische Basis zur Regulierung) und der Kommission zur Genehmigung vorgelegt und anschließend im „Official Journal“ der EU veröffentlicht (CTR, common technical regulation). Damit erhalten sie einen rechtsverbindlichen Status und alle Hersteller sind verpflichtet, die in diesen Normen enthaltenen „grundlegenden Anforderungen“ in den Geräten zu berücksichtigen. Ihre Einhaltung wird im Rahmen einer Zulassung und Konformitätsprüfung überwacht.
In Bereichen, in denen es noch keine europäischen Spezifikationen/Normen gibt bzw. wegen eines zu geringen Marktes oder Allgemeininteresses keine europäische Normung vorgenommen wird, können die einzelnen Mitgliedstaaten eigene, nationale (rechtsverbindliche) Vorschriften herausgeben. Dies ist in der Regel bei Funkgeräten der Fall, um eine effiziente und möglichst störungsfreie Nutzung des Frequenzspektrums sicherzustellen. Alle nationalen Vorschriften müssen bei der EU notifiziert werden, um sicherzustellen, daß hiermit keine unzulässigen Markthemmnisse aufgebaut werden.
Für den Bereich Deutschlands nehmen das Bundesministerium für Post und Telekommunikation und das *Bundesamt für Post und Telekommunikation* (BAPT) als nachgeordnete Behörde alle o.g. Belange wahr. Das BAPT ist mit Experten sowohl bei der ITU als auch beim ETSI und in den Ausschüssen der EU vertreten. Der Konsens mit der nationalen Industrie wird in nationalen Vorbereitungsrunden für den Bereich der ITU und im „Ausschuß für technische Regulierung in der Telekommunikation“ (ATRT) für die nationalen Zulassungsvorschriften hergestellt.
Kryptographie- und Sicherheitsnormen, soweit sie den Bereich der Telekommunikation betreffen, werden beim ETSI im Technischen Komitee Security (TC SEC) erarbeitet und verabschiedet. Die deutsche Federführung hat auch hier das BAPT, das wesentlich an der Erstellung der Spezifikationen beteiligt war und noch ist (z.B. Digitale Signatur, Legal Interception, Fraud) [Heid_97].
Die Arbeitsschwerpunkte des BAPT sind nach [http://www.bapt.de]:

- Die Vergabe von Lizenzen
  für das Betreiben von Übertragungswegen über Grundstücksgrenzen hinweg für Mobilfunk-, Satellitenfunk- und Telekommunikationsdienstleistungen.

- Die Frequenzzuteilungen
  für die Nutzung elektromagnetischer Wellen für Funk- oder andere Zwecke, unter anderem für Mobilfunknetze und -anlagen im öffentlichen und nichtöffentlichen Mobilfunk, Satellitenfunkanlagen, Richtfunk und andere Festfunkverbindungen, CB-Funkanlagen, Empfangs- und Verteilanlagen für Rundfunksignale sowie Flug- und Seefunkanlagen.

- Die Marktbeobachtung
  im Bereich Post und Telekommunikation.

- Die Normung und Entwicklung Technischer Vorschriften
  im Bereich der Telekommunikation als Voraussetzungen für die weltweite Kommunikationsfähigkeit zwischen Endgeräten und Netzen.

  Das BAPT ist unter anderem Mitglied von CEN, ISO, ETSI und ITU. Deren Normen bilden die Grundlage für die Technischen Vorschriften (Zulassungsvorschriften mit rechtsverbindlichem Charakter) und Empfehlungen des BAPT.

  Bei fehlenden oder noch nicht fertiggestellten internationalen Normen erstellt das BAPT eigene Entwürfe und bringt diese in die internationalen Gremien ein.

  Eine weitere Aufgabe im Rahmen der Normung ist die Koordinierung und Vertretung der Interessen der deutschen Gremienmitglieder (Hersteller, Netzbetreiber, Diensteanbieter, Nutzer) im Rahmen der Delegationsleitung.

- Die Zulassung
  von Telekommunikationsendeinrichtungen, Funkanlagen und Qualitätsmanagementsystemen sowie von mit der ordnungsgemäßen Installation, Änderung und Instandhaltung von Telekommunikationsanlagen vertrauten Personen.

- Sicherheit und Datenschutz sowie Notfallvorsorge
  Die Sicherheit in der Telekommunikation sowie die Sicherstellung der Telekommunikation und des Postwesens bei Naturkatastrophen, in Unglücksfällen oder im Verteidigungsfall wird durch Tätigkeiten des BAPT in den Bereichen Technische Schutzmaßnahmen, Umsetzung von Überwachungsmaßnahmen, Sicherstellung des Dienstleistungsangebots im Postwesen und in der Telekommunikation sowie im Zivilschutz gewährleistet.

- Überprüfung der Elektromagnetischen Umweltverträglichkeit (EMVU)
  in Form der Einhaltung der weltweit wissenschaftlich anerkannten Personenschutzgrenzwerte in der Umgebung von ortsfesten Sendefunkanlagen.

- Die Akkreditierung
  von Prüflaboratorien und Zertifizierungsstellen auf den Gebieten der Telekommunikation und der elektromagnetischen Verträglichkeit (EMV).

- Die Frequenzverwaltung
  der Funkfrequenzen, um eine optimale Nutzung des Frequenzspektrums zu gewährleisten.

  Dabei vertritt das BAPT die deutschen Interessen bei internationalen Tagungen und in internationalen Gremien, die sich mit Frequenzangelegenheiten befassen.

- Testen
  Das BAPT führt in seinen nach der europäischen Norm EN45001 akkreditierten Laboratorien die für eine Zulassung von Telekommunikationsendeinrichtungen und Funkanlagen nötigen Prüfungen durch und erstellt entsprechende Testberichte.

- Sicherstellung der Elektromagnetischen Verträglichkeit von Geräten (EMV)
  durch Prüfungen von Geräten vor deren in Verkehrbringen sowie die umgehende Aufklärung von Störungen und die Beseitigung der Ursachen.

2.1.2 Normung in anderen Staaten

Ähnlich wie in Deutschland haben auch viele andere Staaten Normungsinstitute. In Europa sind dies z.B. für Großbritannien die *British Standards Institution* (BSI) und für Frankreich die *Association Francaise de Normalisation* (AFNOR), in der restlichen Welt z.B. das *American National Standards Institute* (ANSI) für die Vereinigten Staaten von Amerika, das *Committee of the Russian Federation for Standardization, Metrology and Certification* (GOST R) für die Russische Föderation oder für Japan das *Japanese Industrial Standards Committee* (JISC).

2.2 Regionale Normung in Europa

Ebenso wie für einzelne Staaten werden auch für Staatengemeinschaften gemeinsame Normen entwickelt. Im folgenden wird dies für die Normung in Europa beschrieben.
Ziel der europäischen Normungsarbeit, die die Gemeinsame Europäische Normungsinstitution, bestehend aus dem *Europäischen Institut für Normung* (CEN) (siehe Abschnitt 2.2.1) und dem *Europäischen Institut für Elektrotechnische Normung* (CENELEC) (siehe Abschnitt 2.2.2, Seite 24), sowie dem *Europäische Institut für Telekommunikationsstandards* (ETSI) (siehe Abschnitt 2.2.3, Seite 26) erfüllt, ist die Erstellung eines einheitlichen und modernen Normenwerks für den Europäischen Binnenmarkt.
Die Europäischen Normen (EN und ETS) orientieren sich an den Normen der internationalen Normungsorganisation ISO, der internationalen Elektrotechnischen Kommission IEC und der Internationalen Telekommunikationsunion ITU (früher CCITT für Internationaler beratender Ausschuß für den Telegraphen- und Fernsprechdienst). Liegen für einen Bereich keine geeigneten Ergebnisse der internationalen Organisationen vor, werden auch spezifische Europäische Normen erarbeitet. Einen Überblick über die Zuständigkeiten der Institute zeigt Tabelle 2.2 auf Seite 34.

2.2.1 European Committee for Standardization (CEN)

Das *European Committee for Standardization* (CEN) mit Sitz in Brüssel ist für die Normungsarbeit in allen Bereichen außer Elektrotechnik und Telekommunikation zuständig. Seine Mitglieder sind die nationalen Normungsorganisationen aller EU- und EFTA-Staaten (mit Ausnahme von Lichtenstein) sowie der Tschechischen Republik. Außerdem gibt es 14 dem CEN angegliederte Normungsinstitute aus Mittel- und Osteuropa sowie 5 Assoziierte Vereinigungen, die europäische Interessen der Hersteller, Konsumenten, kleinen und mittleren Unternehmen etc. vertreten [CEN_94]. Desweiteren besitzt CEN vier „Assoziierte Organisationen“ (ASBs), an die die Normungsarbeit in spezialisierten Bereichen delegiert wurde: Association Europeenne des Constructuers de Materiel Aerospatial (AECMA), European Committee for Iron and Steel Standardization (ECISS), Western European EDIFACT Board (WE/EB) sowie den *European Workshop for Open Systems* (EWOS), wo eine funktionale Norm analog zum OSI-Modell für den Informationsaustausch zwischen offenen Systemen entwickelt wird.
Die Mitgliedsländer des CEN besitzen im Gegensatz zu den Mitgliedern der ISO unterschiedliche Stimmgewichte je nach ihrer Wirtschaftskraft, siehe Tabelle A.1 in Anhang A, wo sich auch ausführliche Listen der Mitglieder befinden.
Die Aufgaben des CEN werden in [CEN_91, Teil 1] beschrieben. Sie umfassen insbesondere die folgenden Punkte:

- Harmonisierung der nationalen, von den CEN-Mitgliedern veröffentlichten Normen,
- Förderung der einheitlichen Einführung von internationalen Normen der ISO und anderer internationaler Normen oder Empfehlungen durch die CEN-Mitglieder,
- Erarbeiten von Berichten über den Stand der Harmonisierung der Normen der CEN-Mitglieder,
- Erarbeitung Europäischer Normen (EN) von Grund auf, wenn dies durch die Erfordernisse in Westeuropa gerechtfertigt ist und keine geeigneten internatio-

nalen oder anderen Normen vorhanden sind, die als Bezugsdokument benutzt werden können,

- Bereitstellung von Verfahren für die gegenseitige Anerkennung von Prüfergebnissen und Zertifizierungssystemen auf europäischer Ebene,
- Unterstützung der weltweiten Normung innerhalb der ISO,
- Zusammenarbeit mit der Europäischen Gemeinschaft (EG), der Europäischen Freihandelszone (EFTA) und anderen internationalen staatlichen Organisationen, so daß in deren Richtlinien und anderen Rechtsgrundlagen auf Europäische Normen (EN) und Harmonisierungsdokumente (HD) verwiesen werden kann,
- Zusammenarbeit mit internationalen Regierungs-, Wirtschafts-, Berufs- und Wissenschaftsorganisationen in Fragen, wo ein Zusammenhang mit Normung besteht,
- Zusammenarbeit mit dem Europäischen Komitee für Elektrotechnische Normung (CENELEC), dem anderen Bestandteil der Gemeinsamen Europäischen Normungsinstitution.

2.2.1.1 Die Organisation des CEN

Das CEN besteht aus

- seinen Mitgliedern, siehe Tabelle A.1 in Anhang A,
- den angegliederten Normungsinstituten (Tabelle A.2 in Anhang A),
- den assoziierten Vereinigungen (Tabelle A.3 in Anhang A),
- den *„Assoziierten Organisationen“* (ASBs), denen die Normungsarbeit in spezialisierten Bereichen delegiert wurde und die an der Generalversammlung teilnehmen und bestimmte Rechte in den technischen Sektorbüros haben (Tabelle A.4 in Anhang A);
- Ausschüssen, welche durch die Generalversammlung oder den Verwaltungsrat zur Unterstützung ihrer Arbeiten eingesetzt werden, wie dem Technischen Büro und dem CENCER-Lenkungskomitee (CENCER ist das Zertifizierungskomitee des CEN);
- Programmkomitees, Technischen Komitees und Unterkomitees, Arbeitsgruppen;
- Sekretariaten von Technischen Komitees und Unterkomitees, Berichter-Sekretariaten;
- Zertifizierungskomitees;
- einem Zentralsekretariat.

Seine Organe sind

- die Generalversammlung,
  die vom Generalsekretär auf Weisung des Verwaltungsrates einberufen wird. Die ordentliche Generalversammlung tagt zwischen April und November jedes Jahres.

- dem Verwaltungsrat,
  dessen Sitzungen vom Generalsekretär auf Weisung des Präsidenten einberufen werden.

  Jedes CEN-Mitglied hat das Recht, für den Verwaltungsrat einen permanenten und einen stellvertretenden Vertreter zu benennen.

- dem Zentralsekretariat,
  das vom Generalsekretär geleitet wird und das für CEN erforderliche Personal umfaßt.

- dem Generalsekretär,
  der als beratender Sekretär an Sitzungen von

  - Generalversammlung,
  - Verwaltungsrat,
  - und von diesen eingesetzten Ausschüssen

  teilnimmt.

  Er ist für die Ausführung der Beschlüsse dieser Gremien verantwortlich und verwaltet den Etat des CEN. Außerdem leitet er das Personal des Zentralsekretariates mit allen Befugnissen, Mitarbeiter einzustellen oder zu entlassen.

- dem Technischen Büro,
  das die Kontrollorganisation für die Normungsaktivitäten ist und für die Initiierung neuer Normungsvorhaben und die Unterstützung der Sekretariate zuständig ist.

- den Technischen Sektorbüros und Programmkomitees,
  zuständig für die Lenkung der eigentlichen Normungsarbeit, die in den

- Technischen Komitees
  geleistet wird.

Die Struktur des CEN ist in Abbildung 2.2 zu sehen.

2.2.1.2 Die Entwicklung einer Europäischen Norm des CEN

Das Vorgehen für die Erarbeitung von Normen ist für CEN und CENELEC identisch. (Daher gelten die folgenden Ausführungen sowohl für die Herausgabe von Normen durch CEN als auch durch CENELEC.)
Veröffentlichungen, die sich aus der Facharbeit von CEN/CENELEC ergeben und veröffentlicht werden, heißen Europäische Normen (EN), Harmonisierungsdokumente (HD), Europäische Vornormen (ENV) oder CEN/CENELEC-Berichte. Diese Dokumente unterscheiden sich folgendermaßen:

- **EN**
  sind die grundlegenden Dokumente, die mit dem Ziel veröffentlicht werden, die nationalen Normen der Mitglieder zu vereinheitlichen.

- **HD**
  werden erstellt, wenn die Überführung in identische nationale Normen unnötig oder unpraktisch ist.

- **ENV**
  sind beabsichtigte Normen zur vorläufigen Anwendung.

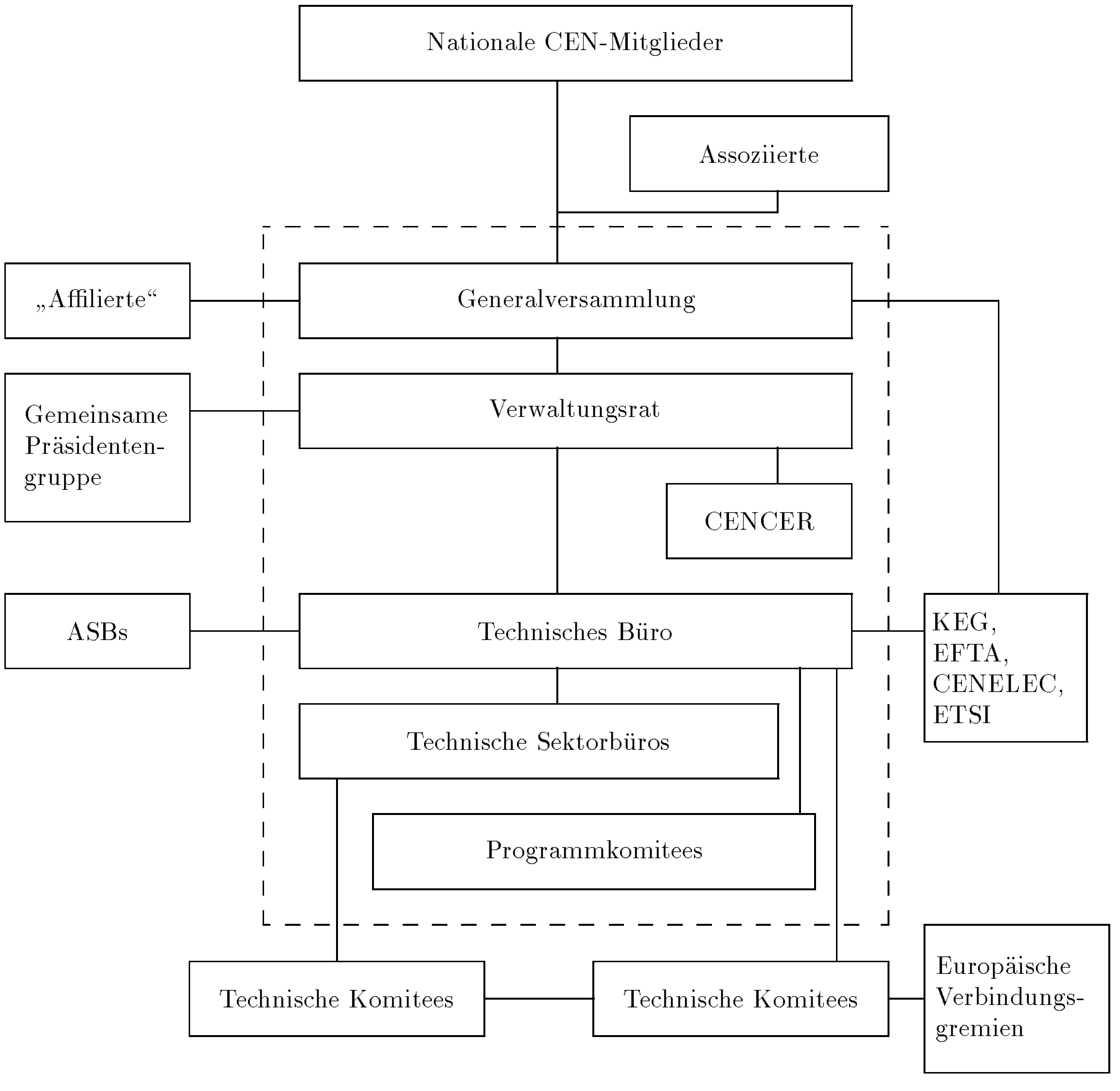

Abbildung 2.2: Die Struktur des CEN nach [CEN_94]

- **CEN/CENELEC-Berichte**
  dienen der Information.

Eine europäische Norm wird in folgenden Schritten entwickelt [CEN_91, Teil 2]:

- Auswahl der Projekte
  CEN/CENELEC beschäftigt sich nur mit klar abgegrenzten Gegenständen, die deutlich und dringend der Normung bedürfen, die mit intensiver Arbeit behandelt werden können und die für die Aufnahme in das Arbeitsprogramm angenommen sind.

  Die von nationalen, europäischen oder internationalen Institutionen, einem CEN/CENELEC-Fachgremium, der EG-Kommission oder dem EFTA-Sekretariat an das CEN/CENELEC-Zentralsekretariat gemachten Projektvorschläge werden vom Technischen Büro auf ihre Notwendigkeit zur Normung hin überprüft.

  Wurde die Notwendigkeit eines Normungsvorhabens festgestellt, wird zuerst überprüft, ob eine bestehende ISO/IEC-Norm oder Vorlagen hierfür übernommen werden können (Grundlage hierfür ist eine entsprechende Vereinbarung zwischen CEN/ISO und CENELEC/IEC) oder ob im Rahmen bestehender Vereinbarungen mit ISO und IEC dort eine entsprechende Norm erstellt werden kann, die sowohl den europäischen wie auch den internationalen Erfordernissen entspricht.

  Fehlt ein geeignetes ISO/IEC-Dokument, kann das Technische Büro, das zuständige Technische Komitee oder sein Sekretariat ein geeignetes anderes Dokument als Grundlage für die auf eine EN oder HD gerichtete Arbeit heranziehen.

- Fragebogenverfahren
  Im Rahmen eines Fragebogenverfahrens ermittelt das Technische Büro

  - ob genügend Interesse an der Harmonisierung des vorgeschlagenen Gegenstandes besteht
  - in welchem Grad eine nationale Harmonisierung mit dem betreffenden Referenzdokument besteht
  - ob dieses Dokument als EN, HD oder ENV annehmbar erscheint.

  Als Ergebnis des Fragebogenverfahrens ergibt sich eine der folgenden Möglichkeiten:

  - Die Stellungnahmen werden zur Einholung fachlichen Rates an ein Technisches Komitee oder ein Berichter-Sekretariat[2] oder eine besondere Adhoc-Gruppe verwiesen, bevor eine entgültige Entscheidung getroffen wird.
  - Das Referenzdokument wird zur Abstimmung als EN, HD oder ENV gestellt.
  - Das Referenzdokument erfordert weitere Facharbeit, die von einem bestehenden oder neu zu gründenden Fachgremium durchgeführt wird.
  - Eine Harmonisierung ist nicht notwendig oder infolge mangelnden nationalen Interesses nicht möglich.
  - Es wird ein CEN/CENELEC-Bericht herausgegeben, um über die Harmonisierungssituation zu berichten.

[2] Berichter-Sekretariate versorgen das Technische Büro mit Informationen über solche ISO/IEC-Arbeiten, die für CEN/CENELEC von Belang sein könnten.

- Verfahren im Technischen Komitee
  Ein technisches Komitee wird nur dann tätig, wenn keine geeigneten internationalen Ergebnisse übernommen werden können oder auf besonderen Antrag z.B. der Kommission der EU oder des EFTA-Sekretariats.

  Das Technische Komitee erarbeitet solange sukzessiv mehrere Entwürfe, bis eine Lösung des Problems gefunden wurde, die eine überwiegende, möglichst einstimmige Zustimmung erhält.

  Wenn diese Stufe erreicht wird, wird der vom Technischen Komitee angenommene Text vom Sekretariat des Technischen Komitees an das Zentralsekretariat gesandt und von diesem an die CEN/CENELEC-Mitglieder verteilt, um eine Stellungnahme der Öffentlichkeit einzuholen. Dieses Verfahren wird als „CEN/CENELEC-Umfrage“ bezeichnet.

  Als Ergebnis der CEN/CENELEC-Umfrage gibt es die folgenden Möglichkeiten:

  - Es ergibt sich eine ausreichende, vorzugsweise einmütige, Zustimmung für den Inhalt des Entwurfes, woraufhin das Sekretariat des Technischen Komitees einen endgültigen Text für die Annahme ausarbeitet. Dabei werden eingegangene fachliche Stellungnahmen berücksichtigt.
  - Es besteht eine ungenügende Zustimmung, das zuständige Technische Komitee darf maximal eine weitere Umfrage einleiten.
  - Der Vorschlag erhält nicht genug Zustimmung zur Annahme als EN. In diesem Fall wird das Erstellen eines HD erwogen.

- Abweichungen und besondere nationale Bedingungen werden berücksichtigt.

- Annahme von EN oder HD
  Die endgültige Annahme einer EN oder HD muß durch eine formelle Abstimmung der Mitglieder geschehen. Dies geschieht über Abstimmungsformulare, die zusammen mit dem endgültigen Wortlaut durch das Zentralsekretariat an die Mitglieder verteilt werden.

Europäische Vornormen (ENV) dürfen als beabsichtigte Normen zur vorläufigen Anwendung auf technischen Gebieten mit hohem Innovationsgrad (z.B. Informationstechnik) oder dann, wenn ein dringender Bedarf für eine Leitlinie besteht, erarbeitet werden, vornehmlich wenn Gesichtspunkte der Sicherheit von Personen oder Sachen keine Rolle spielen [CEN_91]. Sie können durch ein technisches Gremium des CEN/CENELEC mit nachfolgender Abstimmung in einer Sitzung oder durch kombiniertes Fragebogen- und Abstimmungsverfahren über ein geeignetes Referenzdokument. Europäische Vornormen (ENV) müssen ebenso wie Europäische Normen und Harmonisierungsdokumente in geeigneter Weise von den Mitgliedern auf nationaler Ebene verfügbar gemacht werden. Im Gegensatz zu Europäischen Normen dürfen bei Europäischen Vornormen entgegenstehende nationale Normen beibehalten werden, bis die ENV in eine EN umgewandelt wird.
Abbildung 2.3 zeigt die verschiedenen Wege zur Entwicklung einer Europäischen Norm.

2.2.2 European Committee for Electronical Standardization (CENELEC)

Das 1972 gegründete *European Committee for Electronical Standardization* (CENELEC) ist die Vereinigung der nationalen Elektrotechnischen Komitees Europas mit Sitz in Brüssel. Es ist verantwortlich für die Normung im Elektrotechnischen Bereich innerhalb Westeuropas.

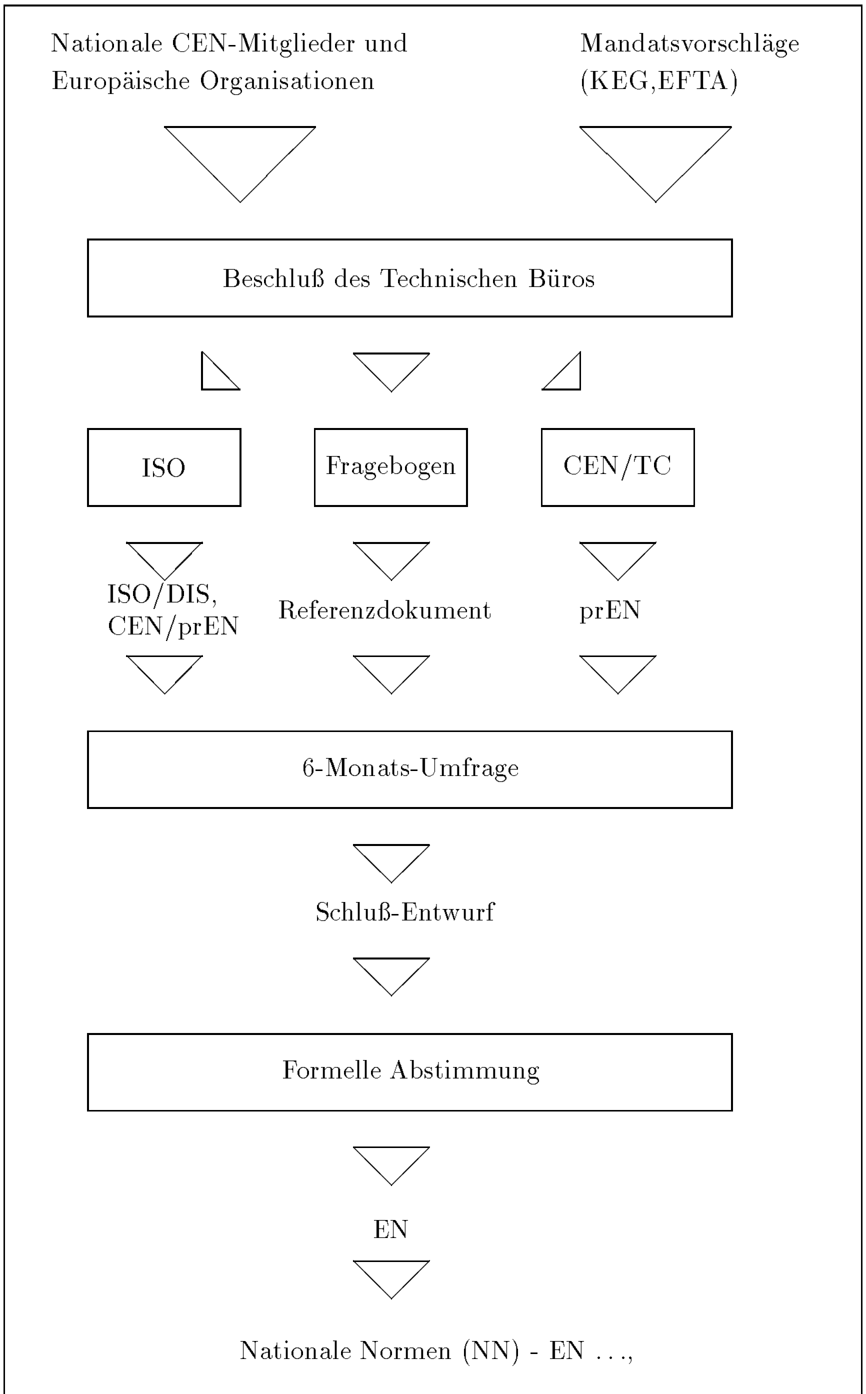

Abbildung 2.3: Die Entwicklung eine Europäischen Norm nach [CEN_94]

Die Organisation des CENELEC besteht nach [http://www.sis.se] aus

- der Generalversammlung (General Assembly),
  die einmal jährlich einberufen wird und die höchste Entscheidungsauthorität ist. Sie umfaßt den Präsidenten, den Vize-Präsidenten und eine Delegation aus jedem Mitgliedsland.

- dem Verwaltungsbeirat (Administrative Board),
  bestehend aus dem Präsidenten, drei Vize-Präsidenten, Schatzmeister, einem belgischen Mitglied, dem vorherigen Präsidenten (retiring President) und dem Generalsekretär.

- dem Technischen Ausschuß (Technical Board),
  der die technische Arbeit koordiniert und aus einer Delegation aus jedem Mitgliedsland besteht.

- dem Generalsekretariat,
  das vom Generalsekretär geleitet wird. Es teilt sich einige Funktionen und Versammlungsräume mit dem CEN.

  Ende 1994 hatte das Generalsekretariat 43 Angestellte.

Die Entwicklung einer CENELEC-Norm funktioniert ebenso wie die Entwicklung einer CEN-Norm, wie dies in Abschnitt 2.2.1.2 beschrieben ist.

2.2.3 European Telecommunications Standards Institute (ETSI)

Das *European Telecommunications Standards Institute* (ETSI), gegründet 1988, vereint die Interessenten auf dem Gebiet der Telekommunikation. Gründungsgrund für ETSI war die Feststellung, daß eine Gesamteuropäische Telekommunikationsinfrastruktur mit voller Interoperabilität die einzige Grundlage für die Entwicklung eines Europäischen Marktes für Kommunikationszubehör und -dienste sein kann. Seine Hauptaufgabe ist die Beschleunigung des technischen Harmonisierungsprozesses. ETSI ist das einzige Forum im Telekommunikationsbereich, das alle Schlüsselorganisationen zusammenbringt: Netzwerkbetreiber, Serviceprovider, Hersteller, Verwaltungen, Benutzer und Entwickler.
Die Mitglieder sind nach [http://www.etsi.org] aufgeteilt in

- Vollmitglieder (Full Membership),
  die an allen Sitzungen der Vollversammlung, der Spezialkomitees und der Organe innerhalb der Technischen Organisation teilnehmen können und dort Stimmrecht besitzen.

  Vollmitglieder können gesetzliche Personen sein (unabhängig davon ob ein Verband, ein Unternehmen, eine Gruppe, eine Organisation oder eine öffentliche Behörde), die

  - aus einem Land, das innerhalb der geographischen Grenzen der Europäischen Konferenz der Post- und Telekommunikationsverwaltungen (CEPT) liegt, stammen und
  - sich verpflichten, die Statuten und Regeln des ETSI und allen anderen Entscheidungen der Vollversammlung zu beachten,

  um an der Normungsarbeit des ETSI teilzunehmen und die Verbreitung dieser Normen zu unterstützen.

- Assoziierte Mitglieder (Associate Membership),
  die ebenfalls an allen Sitzungen teilnehmen können, aber kein Stimmrecht besitzen.

  Assoziierte Mitglieder können die gesetzlichen Personen sein, die die Anforderungen an Vollmitglieder nicht erfüllen, aber sich an der Arbeit des ETSI beteiligen wollen.

- Beobachtende Mitglieder (Observership),
  die ohne Stimmrecht an Sitzungen der Vollversammlung teilnehmen können.

  Beobachtende Mitglieder können die gesetzlichen Personen sein, die berechtigt sind, Vollmitglied zu werden.

Außerdem gibt es noch die Berater (Counsellor Status), die ohne Stimmrecht an den Sitzungen der Generalversammlung und der Arbeit im Board, den Technischen Komitees und der Technischen Organisation teilnehmen können. Es handelt sich dabei um Vertreter der Europäische Kommission und des Sekretariats der EFTA.
Eine weitere Einteilung erfolgt in die Kategorien, aus denen die Mitglieder stammen:

- Verwaltungen, Verwaltungsbehörden und Nationale Standardisierungsorganisationen,
- Öffentliche Netzwerkbetreiber,
- Hersteller,
- Benutzer,
- Service Provider, Entwicklungsinstitute, Beratungsfirmen und andere.

Nationale Organisationen, die die Funktionen von Verwaltung und Netzwerkbetreiber in sich vereinen, sollen in beiden Kategorien Mitglied sein und jede Mitgliedschaft soll getrennt repräsentiert werden.
Die Organe des ETSI sind nach [http://www.etsi.org]

- die Generalversammlung (General Assembly),
  die die höchste Autorität des Instituts ist und die offizielle Verantwortung für die Funktionen der technischen Abteilungen trägt. Sie bestimmt die generelle Politik und entscheidet über Management und Strategien der ETSI.

- das Board,
  das seine Aufgaben von der Generalversammlung erhält und hauptsächlich für den einwandfreien Ablauf der Arbeit in der Technischen Organisation sorgt sowie die laufenden Routineentscheidungen bezüglich des Betriebs des Instituts trifft.

- die Technische Organisation (Technical Organization),
  die die Strukturen liefert, in denen die technischen Experten effizient und effektiv an markt- und technologieorientierten Themen arbeiten sollen. Diese Strukturen umfassen

  - Technische Komitees (Technical Committees),
  - ETSI Projekte (ETSI Projects),
  - ETSI Partnerschaftprojekte (ETSI Partnership Projects) und für spezielle Aufgaben die
  - Sondereinheiten (Specialist Task Forces).

Einige hier interessierende Organe sind z.B. das Technische Komitee „Security“ (TC SEC), das ETSI Projekt „Pay terminals and systems“ (EP PTS) und das Spezialkomitee „Security Algorithms Group of Experts“ (SAGE).

- Spezialkomitees (Special Committees),
  die von der Generalversammlung für spezifische Aufgaben eingerichtet werden können.

Die Struktur des ETSI ist in Abbildung 2.4 zu sehen.

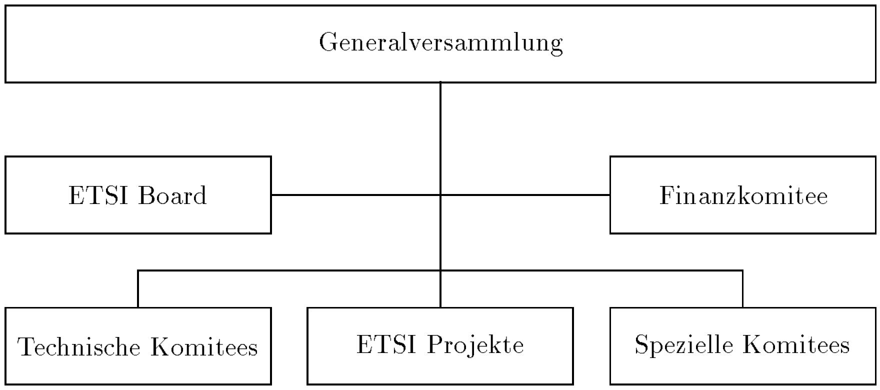

Abbildung 2.4: Die Struktur des ETSI frei nach [http://www.etsi.org]

2.3 Internationale Normung

Die weltweite Normung wird von der *International Organization for Standardization* (ISO), der *International Electrotechnical Commission* (IEC) und der *International Telecommunication Union* (ITU) (früher *Internationaler beratender Ausschuß für den Telegraphen- und Fernsprechdienst* (CCITT)), alle mit Sitz in Genf, wahrgenommen. Ihre Strukturen und Aufgaben werden im folgenden genauer beschrieben.

2.3.1 International Organization for Standardization (ISO)

Die *International Organization for Standardization* ISO besteht aus den nationalen Normungsinstituten aus 118 Ländern (Stand Juni 1997) und verfolgt das Ziel, mit weltweit einheitlichen Normen den internationalen Austausch von Gütern und Dienstleistungen zu erleichtern sowie die Zusammenarbeit auf wissenschaftlichem, technischem und ökonomischem Gebiet auf internationaler Ebene zu intensivieren. Sie wurde am 23. Februar 1947 gegründet und löste die *International Federation of the National Standardizing Associations* (ISA) ab, die 1926 gegründet wurde und ihre Arbeit 1942 aufgrund des 2. Weltkriegs einstellte. Der Schwerpunkt der ISA lag auf mechanischen Techniken. Die erste von der ISO herausgegebene Norm erschien 1951 mit dem Titel „Standard reference temperature for industrial length measurement“.
Die Kurzform ISO ist kein Akronym, sondern leitet sich aus den griechischem isos für „gleich“ ab, dem Wortstamm, aus dem z.B. isometrisch hervorgeht.
Eine nationale Mitgliedsorganisation der ISO ist diejenige nationale Organisation, die für die Normung in ihrem Land offiziell verantwortlich ist. Die Mitglieder werden in 3 Stufen eingeteilt [http://www.iso.org]:

- Vollmitglieder (Member bodies),
  die folgende 4 Aufgaben haben:

  1. Die Information potentiell interessierter Kreise in ihrem Land über die relevanten Normungsvorhaben.
  2. Die Vertretung der nationalen Interessen innerhalb der internationalen Normung.
  3. Die Sicherstellung der Existenz von ISO-Sekretariaten für die Bereiche der Normung, die für das Land von Interesse sind.
  4. Durch Zahlung der Mitgliedsbeiträge die Leistung des Landesbeitrages an den ISO-Finanzen.

  Die Vollmitglieder sind in Anhang B in Tabelle B.1 angegeben.

- Assoziierte Mitglieder (Correspondent Members),
  die diejenigen Staaten vertreten, die noch keine vollwertige nationale Normung besitzen. Sie übernehmen keinen aktiven Anteil an der technischen Arbeit, werden aber vollständig informiert.

  Die Assoziierten Mitglieder sind in Anhang B in Tabelle B.2 aufgelistet.

- Teilmitglieder (Subscriber Members),
  für Länder mit einer geringen Wirtschaftskraft. Sie bezahlen verringerte Mitgliedsbeiträge, haben aber trotzdem die Möglichkeit, Kontakt mit der internationalen Normung zu halten.

  Teilmitglieder sind die in Anhang B in Tabelle B.3 aufgeführten Staaten.

Die eigentliche Normungsarbeit der ISO erfolgt in Technischen Komitees (TC) und Subkomitees (SC).

2.3.1.1 Die Organisation der ISO

Die Organe der ISO sind nach [DIN_95] und [http://www.iso.org]

- die Generalversammlung (ISO General Assembly),
  die aus Vertretern aller Mitglieder besteht und die

- der Präsident
  leitet;

- der Rat (ISO Council),
  der die höchste Entscheidungsinstanz zwischen den Treffen der Generalversammlung ist und aus dem Präsidenten und den Vertretern von 18 Mitgliedsorganisationen besteht, die von den Mitgliedern für jeweils 3 Jahren gewählt werden;

- das Zentralsekretariat (ISO Central Secretariat)
  mit Sitz in Genf, zuständig für

  - allgemeine Verwaltung,
  - Planung und Koordinierung der Facharbeit,
  - Durchführung der Umfrage- und Annahmeverfahren,
  - Veröffentlichung von Internationalen Normen und Fachberichten,
  - Betreuung der Organe außer den Technischen Komitees

- dem Generalsekretär,
  der das Zentralsekretariat leitet;

- den Ad-hoc-Beratergruppen (Ad hoc Advisory Groups),
  die vom Präsidenten mit Zustimmung des Rates einberufen werden, um die ISO beim Verfolgen der strategischen Ziele zu beraten;

- das Technische Büro (ISO Technical Management Board),
  verantwortlich für die Koordinierung und das Aufstellen von Regeln für die Normungsarbeit, die Gründung neuer Komitees, die Unterstützung der Sekretariate und die Bestimmung der Vorsitzenden der Technischen Komitees;

- die Technischen Komitees (ISO Technical Comittees, TC),
  die jeweils für die Normierung eines Gebietes zuständig sind und in Subkomitees (Sub Committee, SC);

- und den Technischen Beratergruppen (Technical Advisory Groups),
  die bei Bedarf durch das Technische Büro eingerichtet werden, um es in grundlegenden, sektorbezogenen oder sektorübergreifenden Angelegenheiten zu beraten.

Die Struktur der ISO ist in Abbildung 2.5 zu sehen.
Hier interessieren insbesondere die Technischen Komitees JTC 1, „Information Technology“, und TC 68, „Banking, securities and other financial services“.
Das Technische Komitee JTC 1 ist ein gemeinsames Komitee von ISO und IEC, JTC steht für „Joined Technical Committee“.
Jedes ISO-Mitglied hat in den Organen der ISO eine Stimme, im Gegensatz zur CEN, bei der jedes Mitglied unterschiedliche Stimmgewichte besitzt, anhängig von seiner Wirtschaftskraft.

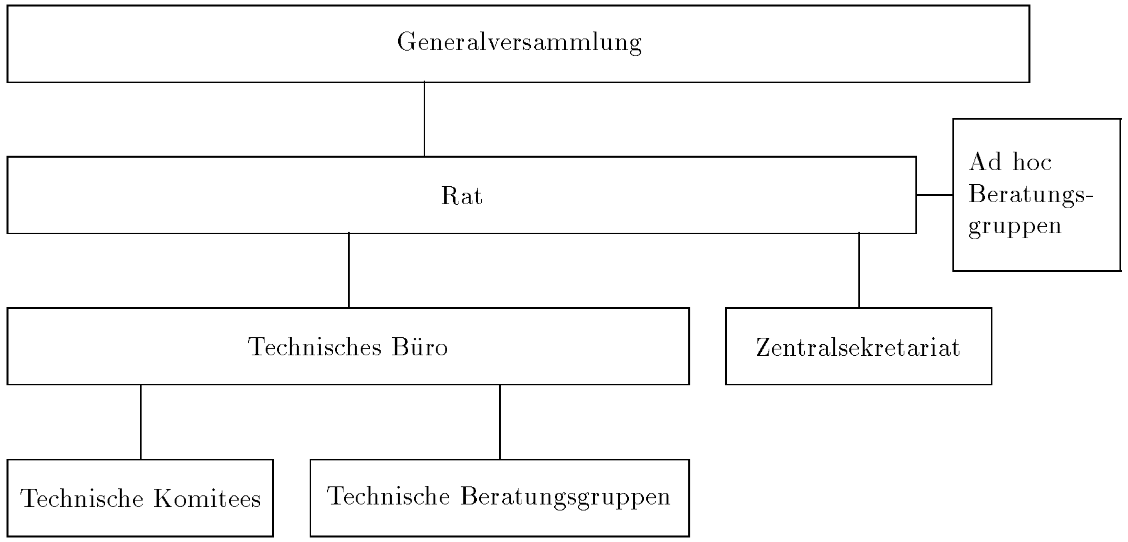

Abbildung 2.5: Die Struktur der ISO nach [http://www.iso.org]

2.3.1.2 Die Entwicklung einer ISO-Norm

Eine internationale Norm (ISO-Norm) ist das Ergebnis eines Vertrages zwischen den ISO-Mitgliedern. Sie kann in dieser Form benutzt werden oder von den Staaten in nationale Normen umgewandelt werden [http://www.iso.org].
Internationale Normen werden durch Technische Komitees (TC) oder Subkomitees (SC) der ISO in einem 6-Stufen-Prozeß entwickelt [http://www.iso.org]:

1. Vorschlag (Proposal stage)
2. Vorbereitung (Preparatory stage)
3. Komitee (Committee stage)
4. Untersuchung (Enquiry stage)
5. Zustimmung (Approval stage)
6. Veröffentlichung (Publication stage)

Falls beim Start des Normungsprojektes bereits ein Dokument vorliegt, das einen bestimmten Grad an Anerkennung besitzt, wie z.B. eine Norm einer anderen Organisation, können einige Stufen übersprungen werden. In diesem „Fast-track procedure“ genannten Fall wird das Dokument direkt als „Draft International Standard“ (DIS) an die ISO-Mitglieder verteilt (Stufe 4) oder, falls es sich um die Entwicklung einer vom ISO-Council anerkannten internationalen Normungsorganisation handelt, als „Final Draft International Standard“ (FDIS) (Stufe 5), ohne die vorhergehenden Stufen zu durchlaufen.
Nun eine Beschreibung der einzelnen Stufen:

Stufe 1: Vorschlag (Proposal stage)
Der erste Schritt bei der Entwicklung einer internationalen Norm ist die Feststellung, daß eine Internationale Norm benötigt wird. Ein neuer Arbeitsbereich-Vorschlag wird den Mitgliedern des zuständigen TC/SC zur Abstimmung vorgelegt. Wird der Vorschlag angenommen, so wird ein Projektleiter bestimmt.

Stufe 2: Vorbereitung (Preparatory stage)
Eine Arbeitsgruppe von Experten, deren Chairman der Projektleiter ist, wird vom TC/SC mit der Erarbeitung eines Arbeitsentwurfs beauftragt. Sukzessiv werden mehrere Entwürfe erarbeitet, bis die Arbeitsgruppe überzeugt ist, die beste technische Lösung des zugrundeliegenden Problems gefunden zu haben. An dieser Stelle wird der Entwurf zur Konsensbildung an das zuständige Komitee weitergeleitet.

Stufe 3: Komitee (Committee stage)
Sobald ein erster Komitee-Entwurf vorliegt, wird er vom ISO-Zentralsekretariat registriert. Er wird zur Kommentierung und (falls notwendig) Abstimmung an die stimmberechtigten Mitglieder des TC/SC weitergeleitet. Sukzessive können mehrere Komitee-Entwürfe benötigt werden, bis ein Konsens über den technischen Inhalt erzielt wird. Nachdem ein Konsens erreicht wurde, wird der Text für die Veröffentlichung als Draft International Standard (DIS) vorbereitet.

Stufe 4: Untersuchung (Enquiry stage)
Der Draft International Standard wird durch das ISO-Zentralsekretariat zur Kommentierung und Abstimmung für 5 Monate an alle ISO-Mitglieder verteilt. Wird der Draft International Standard akzeptiert, wird er als Final Draft International Standard (FDIS) veröffentlicht, wird er abgelehnt, so wird der Text zur weiteren Behandlung an das zuständige TC/SC zurückgegeben.

Stufe 5: Zustimmung (Approval stage)
Der Final Draft International Standard wird zur endgültigen Ja/Nein-Abstimmung für 2 Monate an alle ISO-Mitglieder verteilt. Ergeben sich weitere technische Kommentare, so werden sie in dieser Stufe nicht weiter berücksichtigt, sondern für eine zukünftige Revision der internationalen Norm registriert. Entweder der Text wird in der vorliegenden Form als internationale Norm akzeptiert, oder er wird zusammen mit den technischen Gründen für die Nein-Stimmen an das zuständige TC/SC zurückgegeben.

Stufe 6: Veröffentlichung (Publication stage)
Nachdem eine internationale Norm einmal akzeptiert wurde, werden nur noch kleine Textänderungen, sofern notwendig, durchgeführt und der Text an das ISO-Zentralsekretariat zur Veröffentlichung als Internationale Norm weitergeleitet.

Alle Internationalen Normen werden spätestens alle 5 Jahre vom zuständigen TC/SC überprüft und entweder bestätigt, geändert oder eingezogen.

2.3.2 International Electrotechnical Commission (IEC)

Die *International Electrotechnical Commission* (IEC) wurde 1906 gegründet und sorgt für die weltweite Vereinheitlichung auf dem elektrotechnischen Gebiet. Aufgrund einer 1976 mit der ISO getroffenen Vereinbarung bearbeitet die IEC die Gebiete elektrischer und elektronischer Technik, während die ISO die Zuständigkeit für alle anderen Bereiche übernimmt.
Die Ergebnisse der ISO- und IEC-Arbeit werden als internationale Normen veröffentlicht.

2.3.3 International Telekommunikation Union (ITU)

Die *International Telekommunikation Union* (ITU) wurde 1865 gegründet und mit Gründung der Vereinten Nationen 1947 dieser als spezielle Agentur der UN, zuständig

für die Telekommunikation, zugeordnet. Die ITU repräsentiert die öffentlichen Telekommunikationsinteressen von über 170 Staaten. Ihre Aktivitäten umfassen die Veröffentlichung von Normen, genannt „Recommendations", für technische, ausführende und tarifliche Belange. Diese Recommendations sind für die Mitgliedsstaaten nicht bindend, werden aber als Basis internationaler Telekommunikations-Verträge in vielen Bereichen, wie z.B. Netzwerkadressen, verwendet [Ford_94].
Bis 1993 wurden die Normungsaktivitäten in zwei Zweigen der ITU, genannt *International Telegraph and Telephone Consultative Committee* (CCITT) und *International Radio Consultative Committee* (CCIR), abgewickelt. 1993 wurde die interne Struktur der ITU geändert, diese Gruppen aufgelöst und die Normungsaktivitäten an den *ITU Telecommunication Standardization Sector* (ITU-T) übertragen.
Die nationalen Mitglieder der ITU werden von den nationalen Regierungen bestimmt, oft sind dies die staatlichen Telekommunikationsbetriebe oder, wie z.B. in den USA und Kanada, von der Regierung gebildete Ausschüsse. Die technische Arbeit in der ITU wird von den sogenannten Study Groups (SG) geleistet.

2.3.3.1 Die Organisation der ITU

Die ITU ist in folgende Organe eingeteilt [http://www.itu.org]:

- die Generalversammlung (Plenipotentiary Conferences),
  die die grundlegende Politik der Organisation beschließt und über ihren Aufbau und die Aktivitäten bestimmt. Sie ist für die langfristigen Entscheidungen zuständig.

  Die Generalversammlung besteht aus alle Mitglieder repräsentierenden Delegationen und wird alle 4 Jahre gewählt.

- der Rat (Council),
  der aus 64 von der Generalversammlung gewählten Mitgliedern besteht. Diese sollen aus allen 5 Kontinenten stammen.

  Der Rat ist für die Ausführung der Beschlüsse der Generalversammlung sowie die Kontrolle des Generalsekretariats und der drei Sektoren zuständig.

- die Weltkonferenzen zur Internationalen Telekommunikation (World Conferences on International Telekommunikations),
  an denen alle ITU-Mitglieder, die UN und ihre spezifischen Organisationen, regionale Telekommunikationsorganisationen, Satellitenbetreiber und die Internationale Atomenergieagentur teilnehmen können und auf denen generelle Prinzipien für die Telekommunikation beschlossen werden.

- das Generalsekretariat (General Sekretariat),

- der Radiokommunikations-Sektor (Radiocommunication Sector, ITU-R),
  zuständig für alle Belange der Radiokommunikation wie z.B. die Verteilung von Frequenzen.

- der Telekommunikations-Normungssektor (Telecommunication Standardization Sector, ITU-T),
  zuständig für die weltweite Normung im Bereich der Telekommunikation.

  Er ist in 5 Mitgliedsklassen gegliedert [Tane_97]:

  - Verwaltungen und Ministerien (staatliche *Post-, Telegraph- und Telefonverwaltungen* (PTTs)),
  - Anerkannte private Betreiber (z.B. AT&T, MCI, British Telecom),
  - Regionale Telekommunikationsorganisationen (z.B. ETSI),

- Telekommunikationsanbieter und wissenschaftliche Organisationen,
- Andere interessierte Organisationen (z.B. Bankinstitute und Fluggesellschaften).

Er umfaßt nach [Tane_97] etwa 200 Verwaltungen, 100 private Betreiber und mehrere hundert anderer Mitglieder.

Er arbeitet mit Hilfe

- der Welt Telekommunikations Normungskonferenz (World Telecommunication Standardization Conference),
  die alle 4 Jahre abgehalten wird und von von ihr eingesetzten Arbeitsgruppen unterstützt wird.

  Die Konferenzen beschließen, ändern oder annullieren die Recommendations genannten Normen der ITU.

  (Legislativer Teil der Normung)
- einer Beratenden Normungsgruppe (Advisory Group on Standardization) (Strategisch Anleitung),
- des Normungsbüros (Standardization Bureau),
  geleitet von einem Direktor, das für die Vorbereitung der Konferenzen, die Weiterleitung und Veröffentlichung von Dokumenten der Konferenz sowie technische Unterstützung der Normungsarbeit zuständig ist.

  (Verwaltung der Normungsaktivitäten).

Dabei werden folgende Aktivitäten abgedeckt:

- Telekommunikationsdienste und Netzwerkbetrieb
- Telekommunikationstarife und Abrechnungsprinzipien
- Wartung
- Schutz von außen liegenden Anlagen
- Datenkommunikation
- Telematik
- Schalter, Signale und Mensch-Maschinenkommunikation
- Übertragungsperformance, Systeme und Ausrüstung
- ISDN

• der Telekommunikations-Entwicklungssektor (Telecommunication Development Sector, ITU-D),
zuständig für die Entwicklung im Telekommunikationssektor.

2.4 Zuständigkeiten der Normungsinstitute im Überblick

Organisation \ Normung	allgemein	Elektrotechnik	Telekommunikation
Nationale Normung (Deutschland))	DIN	DKE	BAPT und DKE
Regionale Normung (Europa)	CEN	CENELEC	ETSI
Internationale Normung (Weltweit)	ISO	ICE	ITU

Tabelle 2.2: Zuständigkeiten der Normungsinstitute

Kapitel 3

Standardisierung im Internet

Im folgenden wird die Standardisierung im Internet beschrieben, beginnend mit einem Abschnitt über die Geschichte des Internet (3.1), gefolgt von einem Abschnitt über die Organisation des Internet (3.2), worauf dann der eigentliche Standardisierungsprozeß folgt (Abschnitt 3.2.5).

3.1 Die Geschichte des Internet

Im folgenden wird kurz die Geschichte des Internet vom ARPANET (Abschnitt 3.1.1) über das NSFNET (Abschnitt 3.1.2) zum heutigen Internet (Abschnitt 3.1.3) beschrieben, sofern sie für das Verständnis der Organisation des Internet und damit auch des Standardisierungsprozesses notwendig ist.

3.1.1 ARPANET

Die *Advanced Research Projects Agency* (ARPA), ein Forschungsbereich des US-Amerikanischen Verteidigungsministeriums, wurde 1957 mit der Aufgabe ins Leben gerufen, ausgefeilte Technologien zu entwickeln, die für das Militär von Nutzen sind [Tane_97]. Mitte der sechziger Jahre wurde die ARPA damit beauftragt, ein Kommando- und Steuernetz zu entwickeln, das einen Atomkrieg zu überstehen in der Lage ist. Im Rahmen dieser Forschungen, die nicht von der ARPA selbst, sondern von von ihr beauftragten Unternehmen und Universitäten durchgeführt wurden, entstand ab 1968 das ARPANET, ein Vorgänger des heutigen Internet mit nur wenigen Knoten. Im Zuge der Forschung entstand schließlich 1974 das TCP/IP-Protokoll, mit dem das ARPANET durch den Anschluß immer weiterer Universitäten weiter anwuchs. 1983 war ARPANET stabil und erfolgreich und die ARPA übergab das Management des Netzes der *Defence Communication Agency* (DCA), die es als funktionierendes Netz führen sollte. Als erstes trennte die DCA den militärischen Teil des Netzes in ein separates Teilnetz, genannt MILNET, ab. In den achtziger Jahren wurden weitere Netze, vor allem LANs, an das ARPANET angeschlossen. Durch das ständige Wachstum wurde es immer schwieriger, Hosts zu finden. Daher wurde das *Domain Name System* (DNS) entwickelt, womit sich die Maschinen in Domains organisieren und Hostnamen in IP-Adressen umwandeln lassen. 1990 wurde das ARPANET von neueren Netzen, die aus ihm selbst hervorgingen, überrannt. Es wurde daher geschlossen und demontiert. Das MILNET ist noch heute in Betrieb [Tane_97].

3.1.2 NSFNET

Gegen Ende der siebziger Jahre erkannte die *US National Science Foundation* (NSF) die enorme Wirkung des ARPANET auf die Forschung an den Universitäten. Da jedoch nur Universitäten am ARPANET teilnehmen konnten, die einen Forschungsvertrag mit dem US-Verteidigungsministerium hatten, begann die NSF, ein virtuelles Netz einzurichten. Dieses CSNET genannte Netz, welches sich auf eine einzelne Maschine bei einer Beraterfirma in Cambridge befand, verband das ARPANET als eine Art „Router“ mit den anderen Netzen. 1984 begann die NSF dann, einen schnelleren Nachfolger des ARPANET zu entwickeln. Der erste Schritt war dabei der Aufbau eines Backbone-Netzes, welches die 6 Superrechenzentren der USA miteinander verband. Außerdem bezuschußte das NSF einige (zum Schluß 20) regionale Netze, die an das Backbone angeschlossen wurden und die Benutzer von Tausenden von Universitäten, Forschungslaboren, Bibliotheken und Museen miteinander verbanden. Das komplette Netz - einschließlich Backbone und regionaler Netze - wurde NSFNET genannt und besaß auch einen Zugang zum ARPANET [Tane_97].
Bald wurde ein Nachfolger entwickelt, und das weitere Wachstum machte es erforderlich, die Finanzierung des Netzes nicht allein durch die US-Regierung zu regeln. Außerdem wollten Privatfirmen das Netz mit benutzen, weshalb auf dem Weg zur Kommerzialisierung das ANS (*Advanced Networks and Services*) gegründet wurde, an dem die Unternehmen MERIT, MCI und IBM beteiligt waren. 1990 übernahm ANS das NFSNET, das daraufhin in ANSNET umbenannt wurde.

3.1.3 Internet

Die an das ARPANET angeschlossenen Netze, Maschinen und Benutzer nahmen nach der vollständigen Umstellung auf TCP/IP am 1.1.1983 ständig zu. Nachdem NFSNET und ARPANET zusammengeschlossen wurden, nahm der Umfang exponentiell zu. Ebenso kamen viele regionale Netze dazu und es wurden Verbindungen zu Netzen in Kanada, Europa und im pazifischen Raum hergestellt.
Etwa Mitte der achtziger Jahre wurde dieser Zusammenschluß von Netzen als **ein** Netzverbund betrachtet, später dann als *das Internet*.

3.2 Die Organisation des Internet

Die Organisation des Internet besteht aus

- Internet Society (ISOC) (Abschnitt 3.2.1)
  - Internet Architecture Board (IAB) (Abschnitt 3.2.2)
    - Internet Research Task Force (IRTF) (Abschnitt 3.2.2.1)
    - Internet Engineering Task Force (IETF) (Abschnitt 3.2.2.2)
      - Federal Networking Council (FNC) (Abschnitt 3.2.2.3)
  - Internet Engineering Steering Group (IESG) (Abschnitt 3.2.3)
  - Internet Assigned Numbers Authority (IANA) (Abschnitt 3.2.4)

Abbildung 3.1 zeigt die Organe des Internet.
Als das ARPANET eingerichtet wurde, gründete das US-Verteidigungsministerium einen informellen Ausschuß zur Überwachung. Dieser wurde 1983 in *Internet Activities Board* (IAB) umbenannt und erhielt eine breitere Mission: Die Beaufsichtigung der an ARPANET und Internet beteiligten Forscher. Die Bedeutung von IAB wurde später in *Internet Architecture Board* abgeändert (siehe Abschnitt 3.2.2).
Wurde ein Standard benötigt, entwickelten die IAB-Mitglieder, meist ungefähr 10 Personen, etwas passendes und veröffentlichten ihre Arbeit, damit die neue Technik

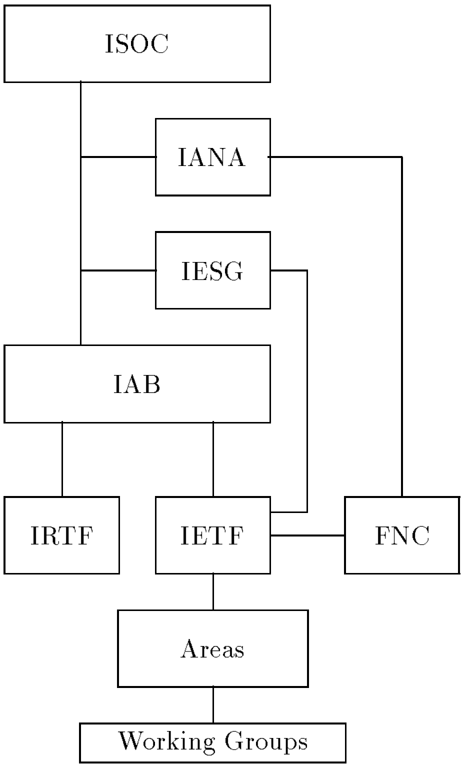

Abbildung 3.1: Die Struktur des Internet nach [http://www.isoc.org]

implementiert werden konnte. Bei der Entwicklung kommunizierten die Mitglieder über die sogenannten „Requests for Comment“ (RFCs).

Bis 1989 nahm der Umfang des Internet soweit zu, daß dieser informelle Stil nicht mehr beibehalten werden konnte. Viele Anbieter von TCP/IP-Produkten sahen nicht ein, wieso sie ihre Produkte ändern sollten, weil 10 Entwicklern etwas Besseres eingefallen war. Im Sommer 1989 wurde das IAB erneut umorganisiert und die Entwickler wurden der *Internet Research Task Force* (IRTF) (siehe Abschnitt 3.2.2.1) als Teil des IAB eingegliedert, ebenso wie die *Internet Engineering Task Force* (IETF) (siehe Abschnitt 3.2.2.2). Das IAB setzte sich aus Mitgliedern der Forschungsgemeinde und anderer Organisationen zusammen. Anfangs war dies eine rotierende Gruppe, deren Mitglieder alle 2 Jahre wechselten. Später wurde die *Internet Society* (ISOC) (siehe Abschnitt 3.2.1) gegründet, die aus am Internet interessierten Personen besteht und damit in gewissem Sinn mit ACM oder IEEE zu vergleichen ist [Tane_97]. Sie wird von gewählten Treuhändern, dem *Board of Trustees*, beaufsichtigt, die die IAB-Mitglieder benennen.

Ziel dieser Neueinteilung war es, daß die IRTF sich auf langfristige Forschungsprojekte konzentriert, während die IETF sich mit kurzfristigen technischen Fragen beschäftigen soll. Darüber hinaus wurde ein formelles Standardisierungsverfahren nach dem ISO-Muster umgesetzt (siehe Abschnitt 3.2.5).

Die Internet-Standards, genannt *„Request for Comment“* (RFC), werden heute von der Internet Engineering Task Force (IETF) entwickelt, von der Internet Engineering Steering Group (IESG) begutachtet und von der Internet Society (ISOC) als internationaler Standard veröffentlicht.

3.2.1 Internet Society ISOC

Die im Januar 1992 gegründete *Internet Society* (ISOC) ist eine Organisation von Internetexperten, sowohl Individuen als auch Unternehmen, Non-Profit Organisationen und Regierungsbehörden, die sich mit dem Wachstum und der Weiterentwicklung des Internets, seiner jetzigen und zukünftigen Nutzung und den sich daraus ergebenden politischen, sozialen und technischen Aspekte befassen. Sie wird vom *ISOC Board of Trustees* geleitet, das von den ISOC-Mitglieder gewählt wird und unter anderem für die Berufung der durch das IETF Nominierungskomitee benannten Kandidaten zum IAB verantwortlich ist.

3.2.2 Internet Architecture Board IAB

Das *Internet Architecture Board* (IAB) ist eine technische Beratergruppe der Internet Society und dafür zuständig, einen Überblick über Architektur und Protokolle des Internets zu erhalten. Es ist für die Definition des generellen Aufbaus des Internets und die weitläufige Leitung der IETF verantwortlich.
Als das ARPANET eingerichtet wurde, gründete das US-Verteidigungsministerium einen informellen Ausschuß zur Überwachung, das *Internet Configuration Control Board* (ICCB). 1984 wurde das ICCB in *Internet Activities Board* (IAB) umbenannt, dies wurde im Juni 1992 mit der Verantwortung für „... oversight of the architecture of the worldwide multi-protocol Internet“ [Cro_93] der ISOC unterstellt und in *Internet* ***Architecture*** *Board* umbenannt, da das IAB tatsächlich nicht an operationalen Aktivitäten irgendeiner Internet-Organisation beteiligt ist. Die Charta des IAB ist RFC 1601.
Es dient im Rahmen des Internet Standardisierungsprozesses als das Gremium, bei dem Einsprüche gegen Entscheidungen der IESG eingelegt werden können, und fungiert als Herausgeber der RFCs.
Das IAB ist für die Berufung der durch das IETF Nominierungskomitee benannten Kandidaten zur IESG und dem IETF-Vorsitzenden verantwortlich.

3.2.2.1 Internet Research Task Force IRTF

Die 1989 von der IAB gegründete *Internet Research Task Force* (IRTF) befaßt sich mit den Themen, die einen langen Zeitraum betreffen und mit gewissen technischen Risiken verbunden sind [Cro_93]. Sie besteht aus einer Anzahl von langfristig arbeitenden, kleinen Forschungsgruppen, deren Arbeitsgebiete z.B. die Internetprotokolle, Anwendungen, Architektur und Technologie sind [http://www.irtf.org].
Die IRTF wird vom IRTF-Vorsitzenden geleitet, der vom IAB berufen wird. Neue Mitglieder werden vom Vorsitzenden und den Mitgliedern unter Mitbestimmung des IAB gewählt.
Zusätzlich zur Verwaltung der Forschungsgruppen werden von der IRTF von Zeit zu Zeit Workshops zu bestimmten Themen einberufen.
Das Verhalten der IRTF Forschungsgruppen wird in RFC 2014 (BCP 8), „IRTF Research Group Guidelines and Procedures“, beschrieben.

3.2.2.2 Internet Engineering Task Force IETF

Die *Internet Engineering Task Force* (IETF) ist der Zweig des Internet Architecture Board (IAB), der für die Entwicklung von Protokollen, deren Implementierung und Standardisierung verantwortlich ist. Sie wurde nach [http://www.dfn-cert.de] 1986

und nach [Cro_93] 1989 als Forum für die technische Koordinierung der Gruppen gegründet, die an den Arbeiten zum ARPANET, zum US Defense Data Network (DDN) und dem Kern des Internet-Gateway-Systems beteiligt waren. Seitdem hat sie sich zu einer großen, offenen, internationalen Gemeinschaft von Entwicklern, Administratoren, Herstellern und Forschern entwickelt, die sich mit der Weiterentwicklung der Internet-Architektur und ihrem einwandfreien Funktionieren in der Praxis beschäftigen [http://www.dfn-cert.de]. Sie ist für jedes daran interessierte Individuum offen [http://www.ietf.org].
Als Aufgaben der IETF werden in [RFC_1718] genannt:

- Lösung operationaler und technischer Probleme
- Spezifikation von Entwicklung und Anwendung der Protokolle und der damit verbundenen Architektur
- Beratung der IESG bei Fragen der Standardisierung und Anwendung von Protokollen
- Technologietransfer von der IRTF zur "Internet-Gemeinde"
- Bereitstellung eines Forums für den Informationsaustausch zwischen Betreibern, Benutzern, Entwicklern und Netzwerkverwaltern.

Der Großteil der Arbeit erfolgt über Mailinglisten, dreimal jährlich werden Versammlungen der IETF abgehalten. Diese Versammlungen werden von einem kleinen IETF Sekretariat organisiert, das auch sonstige Unterstützung für die IETF-Aktivitäten leistet. Das Sekretariat wird laut [Cro_93] zur Zeit von der Corporation for National Research Initiatives verwaltet, unterstützt von mehreren Behörden der US-Regierung und der ISOC.
Die IETF ist in 8 funktionale Bereiche, die Areas, unterteilt. Diese ändern sich von Zeit zu Zeit, in [http://www.ietf.org, Juli 1997] werden genannt:

- Application Area,
- General Area,
- Internet Area,
- Operations and Management Area,
- Routing Area,
- Security Area,
- Transport Area und
- User Services Area.

Für die Areas sind jeweils ein bis zwei Area Direktoren (AD) verantwortlich, die zusammen mit dem Chairman der IETF die Internet Engineering Steering Group (IESG) bilden. Der Chairman der IETF ist gleichzeitig der Chairman der IESG.
Jede Area besteht aus verschiedene Arbeitsgruppen, in denen die Mitglieder unter einer Charter am Erreichen eines bestimmten Zieles zusammenarbeiten. Dies Ziel kann z.B. die Erstellung eines informationellen Dokuments, die Entwicklung einer Protokollspezifikation oder die Lösung eines Problems des Internets sein. Die meisten dieser Arbeitsgruppen haben eine begrenzte Lebensdauer von in der Regel 9-18 Monaten [Cro_93]; wird das Ziel erreicht, wird die Arbeitsgruppe aufgelöst. Arbeitsgruppen werden in RFC 1603, „IETF Working Group Guidelines and Procedures" beschrieben, dieses RFC ist „Informational" und kein Internetstandard.
Hier interessieren besonders die Arbeitsgruppen der Security Area, diese sind nach [http://www.ietf.org] zur Zeit

- Authenticated Firewall Traversal (aft),
- Common Authentication Technology (cat),
- Domain Name System Security (dnssec),
- IP Security Protocol (ipsec),
- One Time Password Authentication (otp),
- Public-Key Infrastructure (X.509) (pkix),
- Secure Shell (secsh),
- Simple Public Key Infrastructure (spki),
- Transport Layer Security (tls) und
- Web Transaction Security (wts).

Sie werden in Kapitel 4 näher beschrieben.

3.2.2.3 Federal Networking Council FNC

Das *Federal Networking Council* (FNC) besteht aus 18 Mitgliedern, von denen einige das National Institute of Health, das Department of Energy und die National Science Foundation sowie einige andere staatliche (US-amerikanische) Einrichtungen vertreten. Es arbeitet als Forum für die Zusammenarbeit von Netzwerken und ist der IANA und der IETF angegliedert.

3.2.3 Internet Engineering Steering Group IESG

Die *Internet Engineering Steering Group* (IESG) ist für das technische Management der IETF-Aktivitäten und die Standardentwicklung im Internet verantwortlich. Als Teil der ISOC verwaltet es die Standardentwicklung im Rahmen der Regeln und Prozeduren, die für diesen Zweck von den ISOC Trustees ratifiziert wurden. Die IESG ist direkt für die Entwicklung der Standards verantwortlich, die eigentliche Standardisierungsarbeit findet in Arbeitsgruppen statt..

3.2.4 Internet Assigned Numbers Authority IANA

Die *Internet Assigned Numbers Authority* (IANA) verwaltet alle „unique parameter values“ des Internet, einschließlich der Internet Protokoll (IP) Adressen. Sie wurde von der ISOC und dem FNC als Clearingstelle gegründet.

3.2.5 Die Entwicklung eins Internetstandards (RFC)

3.2.5.1 RFCs und Internet-Drafts

Ursprünglich waren RFCs genau das, was ihr Name besagt: *Requests for comments*, auf Deutsch etwa „Aufforderungen zum Kommentieren“. Die ersten RFCs, die 1969 erschienen, waren Arbeitspapiere, die zwischen den ARPANET-Entwicklern ausgetauscht wurden, um Lösungen bestimmter Problem zu entwickeln. Im Laufe der Jahre wurden die RFCs immer mehr formalisiert, bis sie als Standards zitiert wurden, auch wenn sie eigentlich keine sind.
Innerhalb der RFCs gibt es zwei Untergruppen, *For Your Information* (FYI) und *Standard* (STD). Die FYI-Gruppe wurde gebildet, um Übersichten und Einführungen in einzelne Gebiete zu dokumentieren. Die STD-Gruppe dient der Identifikation derjenigen RFCs, die tatsächlich Internetstandards spezifizieren.

Jedes RFC, einschließlich FYI und STD, hat eine eindeutige RFC-Nummer, über die es indexziert ist und über die es identifiziert werden kann. FYIs und STDs haben zusätzlich FYI- und STD-Nummern, so daß bei Bedarf nach allen FYIs oder STDs gesucht werden kann. Wird ein RFC überarbeitet, ändert sich seine RFC-Nummer. Die FYI- und STD-Nummern bleiben dabei zur einfachen Referenzierung unverändert.
Es existiert eine weitere Untergruppe für *Reseaux Associes pur la Recherche Europeenne (RARE) Technical Reports* (RTR), die technische Berichte enthält, die im Rahmen der RARE-Gruppe erarbeitet wurden und die als RFCs veröffentlicht wurden, um sie auf einfachem Weg für die Internetgemeinschaft verfügbar zu machen.
Außerdem können RFCs als *Best Current Practice RFCs* (BCP) gekennzeichnet sein. Dies sind RFCs, die die Sicht- oder Arbeitsweise der IETF wiedergeben. Zum Beispiel ist RFC 2026, Internet Standards Process, auch gleichzeitig BCP 9. Die BCPs werden wie Proposed Standards herausgegeben.
Internet-Drafts sind Arbeitspapiere der IETF, die von jeder Gruppe oder Person ausgegeben werden können. Sie werden im „Internet-Drafts" Directory der IETF gespeichert und sind für 6 Monate gültig. Sie können jeder Zeit ergänzt, ersetzt oder zurückgezogen werden. Wird ein Internet-Draft durch eine neue Version ersetzt, beginnt die Laufzeit der 6-Monatsfrist von neuem. Werden sie innerhalb dieser 6 Monate nicht verändert und nicht von der IESG als RFC veröffentlicht, so werden sie nach Ablauf der Frist gelöscht.
Eine Liste der Internet-Drafts findet man unter
<http://www.ietf.org/1id-abstracts.html>,
die eigentlichen Texte befinden sich im Verzeichnis
<ftp://ietf.org/internet-drafts>.
Weitere Informationen über RFCs und Internet-Drafts finden sich nach [RFC_1718] in

- Request for Comments on Request for Comments (RFC 1111)
- F.Y.I. on F.Y.I.: Introduction to the F.Y.I. notes (FYI 1)
- Introduction to the STD Notes (RFC 1311)
- Guidelines to Authors of Internet-Drafts (GAID)
- The Internet Activities Board (RFC 1160)
- The Internet Standards Process (RFC 2026)
- Internet Official Protocol Standards (STD 1)

Nach [Cro_93] durchläuft ein Dokument auf dem Weg zum Internet-Standard die folgenden 4 Stufen:

1. Grundlagenforschung (*Basic development*),
   wobei die Spezifikation keinen formalen Status besitzt und die Entwicklung nicht zum Einleiten eines Standardprozeß führen muß.

2. *Proposed Standard*,
   wenn die Spezifikation stabil ist, eine ausreichende Zustimmung erhält und keine bekannten Lücken oder Probleme enthält.

   Generell ist das Testen vor der Standardisierung ein wichtiges Prinzip des Internet-Prozeßes, und oft werden Spezifikationen getestet, bevor sie in den Standardisierungsprozeß eingehen.

3. *Draft Standard* (Internet Draft),
wenn eine Spezifikation in mindestens zwei voneinander unabhängigen Implementationen existiert, die miteinander interoperiert haben, um alle Funktionen zu testen, und die Spezifikation seit mindestens 6 Monaten ein Proposed Standard ist.

4. *Internet Standard* (RFC oder auch STD),
wenn für einen Draft Standard signifikante Felderfahrungen gemacht wurden, ein klares Interesse der Öffentlichkeit an der Nutzung der Spezifikation besteht und die Spezifikation mindestens 4 weitere Monate ihren Status behalten hat.

Dokumente anderer Standardisierungsorganisationen, anderer Organisationen oder Individuen, die von ihrem Herausgeber dem Internet verfügbar gemacht werden sollen, können von diesen als RFC mit dem Zusatz *Informational* veröffentlicht werden. Sie werden damit kein Internetstandard und müssen nicht das direkte Ergebnis von Arbeiten des Internet sein. Für Spezifikationen, die nicht in den Standardprozeß eingebunden sind, für die der Autor aber die Erfahrung der Internet-Teilnehmer mit dieser Spezifikation erfahren möchte, können als *Experimental* veröffentlicht werden. Diese Spezifikationen können noch geändert werden, unvollständig oder fehlerhaft sein, aber der Autor erwartet technische Reviews und Erfahrungen, z.B. um die Spezifikation für eine Veröffentlichung im Rahmen des Standardprozesses zu überarbeiten.
Der größte Teil der Arbeit besteht in der Produktion von *Technical Specifications* (TS), als Dokumenten, die Formate und Prozeduren beschreiben. Zusätzlich können separate *Applicability Statements* (AS) existieren, die die Umstände beschreiben, unter denen ein oder mehrere TSs angewendet werden.
Für die Akzeptanz einer Spezifikation durch die IETF gelten folgende Kriterien [Cro_93]:

Kompetenz Die Spezifikation ist technisch geschrieben und stimmt mit der Internetarchitektur überein.

Unterstützung Es muß eine signifikante Menge von potentiellen Anbietern und potentiellen Benutzern existieren, sowie ein Nachweis dafür, daß diese tatsächlich den durch die Spezifikation definierten Service benutzen werden.

Kohärenz Die Spezifikation muß klar und sauber geschrieben sein.

Konsens Die Spezifikation muß einen adäquaten Konsens der technischen Gemeinschaft reflektieren.

3.2.5.2 Der Internet-Standardisierungsprozeß

Die Ziele des Internet-Standardisierungsprozeß sind nach [RFC_2026]:

- Technische „Exzellenz“
- Vorherige Implementierung und Tests
- Klare, präzise und leicht verständliche Dokumentation
- Offenheit und Fairness
- Zeitlosigkeit

Die Prozedur für die Entwicklung eines Internetstandards ist relativ einfach, obwohl sie im Laufe der Zeit mehr formalisiert wurde. Eine Arbeitsgruppe wird gebildet und ein Vorsitzender von der IESG bestimmt. Sie bekommt eine Charta, in der

unter anderem das Ziel der Arbeitsgruppe beschrieben wird. Die Arbeitsgruppe nimmt ihre Tätigkeit online und auf IETF-Treffen auf, wobei zusätzliche Treffen der Arbeitsgruppe möglich sind, was aber sehr selten vorkommt. Jede Arbeitsgruppe bestimmt ihre eigenen Arbeitsregeln, deren Art von einem sehr formlosen Stil bis zu einer sehr formalen Struktur reichen kann.
Grundlage der Arbeit in einer Arbeitsgruppe ist die grobe Übereinstimmung über Entscheidungen und das Fällen von Entscheidungen in einer Weise, die eine Fortentwicklung in Richtung auf das in der Charta genannte Ziel garantiert. Stimmt die Arbeitsgruppe darin überein, eine stabile Spezifikation gefunden zu haben, welche die gegebenen technischen Bedingungen erfüllt, wird sie zur Stellungnahme an die IESG weitergeleitet. Ein kurzer, öffentlicher Review erlaubt die Abgabe von Kommentaren zum technischen Inhalt oder dem Fortschritt der Arbeitsgruppe.
Da es keine formale Mitgliedschaft in einer Arbeitsgruppe gibt, finden auch keine Abstimmungen statt. Daher kann es vorkommen, daß ein Teil der Arbeitsgruppe, der in mehreren Diskussionen unterliegt, sich unterdrückt fühlt oder meint, daß der Konsens innerhalb der Arbeitsgruppe nicht erreichbar ist. Diese Fälle werden vom IETF-Management sehr ernst genommen. Die sich durch eventuelle Wiederholungen von Schritten oder zusätzliche Stellungnahmen ergebenden Verzögerungen werden in Kauf genommen, da ein breiter Konsens bei der Entwicklung erwünscht ist und das System der IETF auf dem guten Willen und der Integrität der Teilnehmenden basiert.
Die Schritte des Internet Standardisierungsprozeß werden in [RFC_2026, Abschnitt 6] beschrieben und sind im folgenden aufgeführt:

1. Standardisierungsaktionen
   Eine Standardisierungsaktion (*Standards Action*) - die Einfügung in, der Aufstieg innerhalb oder die Entfernung einer Spezifikation aus dem Standardisierungsverfahren (*Standards Track*) - muß von der IESG durchgeführt werden.

   (a) Einleitung einer Aktion
   Eine Spezifikation, die in das Standardisierungsverfahren eingefügt werden oder darin aufsteigen soll, muß zuerst als Internet-Draft veröffentlicht werden, sofern sie nicht seit ihrer Veröffentlichung als RFC unverändert geblieben ist. Sie soll für einen Zeitraum von mindestens zwei Wochen als Internet-Draft bestehen bleiben, um einen nutzbaren Review zu erlauben. Danach kann eine Empfehlung für eine Aktion ausgesprochen werden.
   Eine Standardisierungsaktion wird durch eine Empfehlung durch die zuständige IETF Arbeitsgruppe oder, sofern es sich um ein Dokument handelt, welches nicht von einer Arbeitsgruppe stammt, die Empfehlung eines einzelnen Individuums an die IESG eingeleitet.

   (b) IESG Review und Genehmigung
   Die IESG stellt fest, ob eine Spezifikation die an sie gestellten Anforderungen erfüllt oder nicht. Gegebenenfalls kann die IESG einen zusätzlichen Review veranlassen.
   Danach informiert die IESG die IETF über den der Spezifikation von ihr zugeteilten Status und stellt die Spezifikation der Internetgemeinde für einen letzten Review vor. Diese letzte, „Last-Call“ genannte Periode soll nicht kürzer als 4 Wochen sein.
   Nach Ablauf der Last-Call Periode trifft die IESG eine Entscheidung darüber, ob die Standardisierungsaktion genehmigt wird oder nicht. Diese Entscheidung wird der IETF mitgeteilt.

   (c) Veröffentlichung
   Wurde eine Standardisierungsaktion genehmigt, wird die Spezifikation an

den RFC-Editor weitergeleitet und die IETF angewiesen, die Spezifikation als RFC zu veröffentlichen. Zu diesem Zeitpunkt wird die Spezifikation aus dem Internet-Drafts Directory gelöscht.

Eine offizielle Zusammenfassung aller durchgeführten und geplanten Standardisierungsaktionen wird in jeder Ausgabe des Internet Society Newsletters veröffentlicht.

2. Aufsteigen im Standardisierungsverfahren
   Die in 1. beschriebene Prozedur wird für jede Aktion während des Aufsteigens einer Spezifikation im Standardisierungsverfahren durchgeführt.

   Eine Spezifikation soll für mindestens 6 Monate den Status eines *Proposed Standard* behalten und für mindestens 4 Monate oder bis zur Durchführung eines IETF-Treffens, je nachdem was später eintrifft, den Status eines *Draft Standard* behalten. Diese Zeiträume wurden gewählt, um ausreichend Zeit für die Begutachtung durch die Internetgemeinde zu haben. Die Frist wird ab dem Zeitpunkt gerechnet, zu dem das entsprechende RFC veröffentlicht wird oder, wenn kein RFC veröffentlicht wird, ab dem Zeitpunkt der Ankündigung der Genehmigung der Aktion durch die IESG.

   Eine Spezifikation kann während ihres Aufsteigens im Standardisierungsverfahren überarbeitet werden. In jeder Stufe soll die IESG die Änderungen der überarbeiteten Spezifikation gegenüber der aktuellen Version bestimmen und die Standardisierungsaktion gegebenenfalls entsprechend abändern. Geringfügige Änderungen sind ohne Änderung der Aktion möglich, bei signifikanten Änderungen kann es jedoch notwendig sein, auf der aktuellen Stufe weitere Erfahrungen zu sammeln, bevor im Standardisierungsverfahren fortgefahren wird. Wurde die Spezifikation grundlegend geändert, kann es notwendig sein, sie als neues Dokument zu betrachten und das Standardisierungsverfahren wieder am Anfang zu beginnen. Bei jeder Änderung des Status soll die Spezifikation erneut als RFC veröffentlicht werden.

   Erreicht eine Spezifikation nicht die Stufe eines Internet-Standards, verbleibt aber für 24 Monate oder, nach einer Änderung, für 12 Monate auf einer Stufe, soll die IESG die Spezifikation auf ihre Brauchbarkeit hin überprüfen und daraufhin über die Fortführung oder Einstellung der Entwicklung entscheiden.

3. Überarbeitung eines Standards
   Eine neue Version eines eingeführten Internetstandards muß genauso wie eine komplett neue Version den gesamten Standardisierungsprozeß durchlaufen. Erreicht die neue Version den Status eines Internet Standards, ersetzt sie die alte Version, die daraufhin den „Historic“ Status erhält. In einigen Fällen kann es notwendig sein, beide Versionen als Internet Standard bestehen zu lassen, z.B. um eine installierte Basis zu unterstützen. In diesem Fall muß in der neuen Version oder in einem extra Dokument auf die Beziehungen zwischen den Dokumenten hingewiesen werden.

4. Zurückziehen eines Standards
   Im Zuge der technologischen Entwicklung kann es vorkommen, daß eine neue Standardspezifikation das Zurückziehen einer oder mehrerer anderer Standardspezifikationen erfordert. In diesem Fall, oder wenn es aus anderen Gründen notwendig erscheint, kann die IESG eine Änderung des Status einer alten Spezifikation zu Historic veranlassen. Dabei wird wie bei jeder anderen Standardisierungsaktion vorgegangen und insbesondere die Last-Call Periode eingehalten.

Eine Anforderung zum Zurückziehen eines existierenden Standards kann von einer Arbeitsgruppe, einem Area Direktor oder jeder anderen interessierten Partei ausgehen.

5. Konfliktlösung und Einsprüche
Kontroversen können auf jeder Stufe während des IESG-Prozesses vorkommen. Soweit möglich wurde der Prozeß so angelegt, daß Kompromisse möglich sind und eine übergreifende Zustimmung erreicht werden kann. Trotzdem kann es vorkommen, daß Personen nicht zustimmen können. Um die Ziele der Offenheit und Fairness zu erhalten, muß in einem solchen Fall eine Lösung im Rahmen eines offenen Reviews und einer offenen Diskussion gefunden werden. Im folgenden werden die dabei verwendeten Verfahren beschrieben:

   (a) Kontroversen in Arbeitsgruppen
   Ein Individuum (Mitglied der entsprechenden Arbeitsgruppe oder nicht) kann mit der Empfehlung der Arbeitsgruppe nicht einverstanden sein, wenn er oder sie meint, daß (a) seine oder ihre Sichtweise nicht ausreichend von der Arbeitsgruppe beachtet wurde oder (b) die Arbeitsgruppe eine falsche technische Wahl getroffen hat, wodurch die Qualität oder Integrität der Lösung gefährdet wird. Der erste Fall ist ein Problem im Arbeitsablauf von Arbeitsgruppen, der zweite die Behauptung eines technischen Fehlers. Obwohl beide Fälle grundverschieden sind, werden beide durch dieselbe Vorgehensweise behandelt.

   Eine Person, die mit der Empfehlung einer Arbeitsgruppe nicht einverstanden ist, soll das Problem zuerst mit dem Vorsitzenden der Gruppe besprechen, der weitere Mitglieder oder die gesamte Gruppe hinzuziehen kann. Wird dabei keine Lösung gefunden, kann jede beteiligte Partei den Area Direktor der für die Arbeitsgruppe zuständigen Area hinzuziehen. Dieser versucht dann, den Konflikt zu schlichten. Schlägt dies fehl, kann jede beteiligte Partei die IESG im ganzen anrufen. Diese wird dann versuchen, das Problem im Rahmen ihrer eigenen Möglichkeiten zu lösen. Ist auch auf Stufe der IESG keine Lösung möglich, kann von jeder Partei das IAB angerufen werden, dessen Entscheidung endgültig ist.

   (b) Fehlschläge im Prozeß
   Der in [RFC_2026] beschriebene Prozeß geht von einem stetigen Fortschreiten aus, wobei die IESG für die korrekte Durchführung verantwortlich ist.

   Ist ein Individuum mit einer Aktion der IESG nicht einverstanden, soll dieses Individuum das Thema zuerst mit dem Vorsitzenden der IESG diskutieren. Kann dabei keine Lösung gefunden werden, wird die IESG als ganzes damit beauftragt, die Aktion unter Berücksichtigung der Einwände neu zu bewerten. Ein Bericht über diese Arbeit wird an die IETF gesendet.

   Ist innerhalb der IESG keine Lösung möglich, wird das IAB eingeschaltet, dessen Entscheidung endgültig ist.

   (c) Fragen der Anwendungsprozedur
   Weitere Schritte sind nur möglich, wenn eine Prozedur selbst (z.B. die in RFC 2026 beschriebenen Prozeduren) für unpassend oder unzureichend für den Schutz der Rechte aller Teilnehmer in einem fairen und offenen Internet Standardisierungsprozeß gehalten wird. In diesem Fall wird das Board of Trustees der Internet Society mit der Lösung des Problems beauftragt.

(d) Einsprüche
Alle Einsprüche müssen eine detaillierte und spezifische Beschreibung der Tatsachen des Konflikts beinhalten und innerhalb von zwei Monaten nach der öffentlichen Bekanntmachung der Aktion oder Entscheidung eingereicht werden.

Auf jeder Stufe des Entscheidungsprozesses können die Personen oder Einrichtungen, die die Entscheidungen treffen, selber die dabei befolgte Vorgehensweise bestimmen.

Alle Entscheidungen müssen in einer angemessenen Zeit getroffen werden, wobei kein Zeitrahmen angegeben wird, da der Standardisierungsprozeß im Internet auf Konsens beruht und deshalb keine Zeitlimits vorgegeben werden sollen.

Kapitel 4

Arbeitsgruppen der Security Area der IETF

Im folgenden werden die Arbeitsgruppen der Security Area der IETF, ihre Ziele und die bisher von ihnen geleistete Arbeit genauer beschrieben.

4.1 Authenticated Firewall Traversal (aft)

Ziel der Arbeitsgruppe „Authenticated Firewall Traversal“ ist die Entwicklung eines Protokolls für das Passieren eines Firewalls durch Programme der Anwendungsschicht. Sie wird ein Durchgangsprotokoll (traversal protocol) sowohl für TCP- als auch UDP-Anwendungen entwickeln, welches ein Framework für die Authentikation des Firewall-Durchgangs umfaßt. Um Interoperabilität zu fördern, werden ebenso grundlegende Authentikationstechniken für die Benutzung in einem generellen Authentikations-Framework entwickelt.
Ergebnis der Arbeit soll ein RFC sein, welches eine Beschreibung des Durchgangsprotokolls und der grundlegenden Authentifikationsmethoden sowie eine Referenzimplementierung des Protokolls und der Authentifikationsmethoden enthält. Grundlage der Arbeit ist das SOCKS-System, das David Koblas 1992 auf dem Usenix Security Symposium veröffentlicht hat.
Es existieren bisher (Juli 1997, [http://www.ietf.org]) die RFCs

- RFC 1928, SOCKS Protocol Version 5
- RFC 1929, Username/Password Authentication for SOCKS V5
- RFC 1961, GSS-API Authentication Method for SOCKS Version 5

und die Internet-Drafts

- Challenge-Handshake Authentication Protocol for SOCKS V5
- Challenge-Response Authentication Method for SOCKS V5
- Secure Sockets Layer for SOCKS Version 5
- SOCKS Protocol Version 5.

4.2 Common Authentication Technology (cat)

Ziel der „Common Authentication Technology"-Arbeitsgruppe ist die Entwicklung eines Verteilten Sicherheitsservices (distributed security services), einschließlich Authentikation, Integrität und Vertraulichkeit, für eine Vielzahl von Protokoll-Aufrufern, wobei diese Aufrufer von der Spezifikation der tieferliegenden Sicherheitsmechanismen isoliert werden.
Zum Erreichen dieses Ziels werden Aufgaben auf allen Ebenen verfolgt, es werden sowohl Schnittstellen zwischen den Ebenen als auch die tieferliegenden Sicherheitsfunktionen entwickelt.
Es existieren bisher (Juli 1997, [http://www.ietf.org]) die RFCs

- RFC 1507, DASS - Distributed Authentication Security Services
- RFC 1508, Generity Security Service Application Program Interface
- RFC 1509, Generic Security Service API: C-bindings
- RFC 1510, The Kerberos Network Authentication Service
- RFC 1511, Common Authentication Technology Overview
- RFC 1964, The Kerberos Version 5 GSS-API Mechanism
- RFC 2025, The Simple Public-Key GSS-API Mechanism

und die Internet-Drafts

- FTP Security Extensions
- Independent Data Unit Protection Generic Security Service Application Programm Interface (IDUP-GSS-API)
- Public Key Cryptography for Initial Authentication in Kerberos
- Generic Security Service API Version 2: C-bindings
- Independent Data Unit Protection Generic Security Service Application Programm Interface: C-bindings
- The Simple and Protected GSS-API Negotiation Mechanism
- The SESAME V5 GSS-API Mechanism
- Extended Generic Security Service APIs: XGSS-APIs Access control and delegation extensions
- Public Key Cryptography for Cross-Realm Authentication in Kerberos
- Key Derivation for Kerberos V5
- Triple DES with HMAC-SHA1 Kerberos Encryption Type
- Public Key Utilizing Tickets for Application Servers (PKTAPP)
- Kerberos Change Password Protocol
- Integrity Protection for the Kerberos Error Message

Zur GSS-API siehe auch Abschnitt 6.4, zusätzlich zu den oben genannten RFCs existiert zumindest noch RFC 2078, Generity Security Service Application Program Interface Version 2.

4.3 Domain Name System Security (dnssec)

Die Arbeitsgruppe „Domain Name System Security“ arbeitet an der Erweiterung des DNS-Protokolls um Fähigkeiten zum Schutz der dynamischen Update-Operationen des DNS. Speziell soll erreicht werden, daß ein Replay von Update-Transaktionen erkannt wird und daß Update-Transaktionen geordnet werden können.
Bisher (Juli 1997, [http://www.ietf.org]) existieren die RFCs

- RFC 2065, Domain Name System Security Extensions
- RFC 2137, Secure Domain Name System Dynamic Update

und die Internet-Drafts

- Mapping Autonomous Systems Number into the Domain Name System
- Detached Domain Name Systems Information
- The DNS Inverse Key Domain

4.4 IP Security Protocol (ipsec)

Die Aufgabe der „IP Security Protocol“-Arbeitsgruppe besteht in der Entwicklung von Mechanismen zum Schutz der Client-Protokolle des Internet-Protokolls IP. Ein Sicherheitsprotokoll in der Netzwerkschicht soll kryptographische Sicherheitsdienste bereitstellen, die flexible Kombinationen von Authentikation, Integrität, Zugriffskontrolle und Vertraulichkeit unterstützen.
Die Protokollformate des „IP Authentication Headers“ (AH) und des „IP Encapsulating Payload“ (ESP) werden unabhängig von den kryptographischen Algorithmen sein.
Es sollen Protokolle und kryptographische Techniken entwickelt werden, die die Anforderungen an die Schlüsselverwaltung der Sicherheit in der Netzwerkschicht erfüllen. Das „Internet Key Management Protocol“ (IKMP) soll ein Protokoll für die Anwendungsschicht definieren, das unabhängig von den tieferliegenden Sicherheitsschichten ist.
Es gibt bisher (Juli 1997, [http://www.ietf.org]) die RFCs

- RFC 1825, Security Architecture for the Internet Protocol
- RFC 1826, IP Authentication Header
- RFC 1827, IP Encapsulating Security Payload (ESP)
- RFC 1828, IP Authentication using Keyed MD5
- RFC 1829, The ESP DES-CBC Transform
- RFC 2085, HMAC-MD5 IP Authentication using Replay Prevention
- RFC 2104, HMAC: Keyed-Hashing for Message Authentication

und die Internet-Drafts

- Internet Security Association and Key Management Protocol (ISAKMP)
- SKIP Extensions for IP Multicast
- Combined DES-CBC, HMAC and Replay Preventation Security Transform
- HMAC-SHA IP Authentication with Replay Prevention

- Security Architecture for the Internet Protocol
- The resolution of ISAKMP with Oakley
- Combined 3DES-CBC, HMAC and Replay Preventation Security Transform
- The Internet IP Security Domain of Interpretation for ISAKMP
- Inline Keying within the ISAKMP Framework
- Implementation of Virtual Private Networks (VPNs) with IP Security
- HMAC-SHA-1-96 IP Authentication with Replay Prevention
- HMAC-MD5-96 IP Authentication with Replay Prevention
- IP Encapsulating Security Payload (ESP)
- IP Authentication Header
- The ESP RC5-CBC Algorithm
- The ESP CAST-128-CBC Algorithm
- A revised encryption mode for ISAKMP/Oakley

4.5 One Time Password Authentication (otp)

Eine Angriffsmöglichkeit auf Computersysteme mit Anschluß an das Internet besteht im Ausspähen von Benutzerkennungen und zugehörigem Passwords legitimer Benutzer. Durch ein One-Time Passwordsystem können diese Replay-Attacken genannten Angriffe abgewehrt werden.
In der Arbeitsgruppe „One Time Password Authentication" soll ein RFC-Standard für die One-Time Password-Technologie entwickelt werden.
Bisher (Juli 1997, [http://www.ietf.org]) existieren der RFC

- RFC 1938, A One-Time Password System

und die Internet-Drafts

- OTP Extended Response
- OTP Verification Examples
- A One-Time Password System

4.6 Public-Key Infrastructure (X.509) (pkix)

Viele Internetprotokolle und Anwendungen, die die asymmetrische Public-Key Technologie verwenden, benötigen eine Public-Key Infrastruktur (PKI) zur sicheren Verwaltung der Schlüssel der weit verteilten Benutzer und Systeme. Der Standard CCITT X.509 der ITU bildet eine weit akzeptierte Basis eines solchen Systems, indem er Datenformate und Prozeduren zur Verteilung von öffentlichen Schlüsseln (Public-Keys) mit von Zertifizierungsstellen (Certification Authorities, CAs) digital signierten Zertifikaten definiert. RFC 1422 spezifiziert die Basis einer X.509-basierten Public-Key Infrastruktur, die primär für die Verwendung für Internet Privacy Enhanced Mail (PEM) gedacht ist. Seit der Veröffentlichung von RFC 1422 haben sich die Anforderungen gewandelt und die Fähigkeiten von X.509 wurden

durch die Entwicklung der Standards X.509 Version 3 für Zertifikate und Version 2 für das Widerrufen von Zertifikaten erweitert.
Im Rahmen der Arbeitsgruppe Public-Key Infrastructure (X.509) sollen die Internetstandards entwickelt werden, die für eine auf X.509 basierende Public-Key Infrastruktur für mehrere Anwendungen und verschiedene Implementationen notwendig sind. Die sich ergebende Public-Key Infrastruktur soll ein Framework liefern, das es ermöglicht, mehrere Vertrauenshierarchien und Benutzerumgebungen zu definieren. Mögliche Systeme, die diese Public-Key Infrastruktur verwenden können, sind z.B. GSS-API Mechanismen, ipsec-Protokolle, Zahlungssysteme und WWW-Protokolle. Bisher (Juli 1997, [http://www.ietf.org]) existieren keine RFCs und die Internet-Drafts

- Internet Public Key Infrastructure Part I: X.509 Certificate and CRL Profile
- Internet Public Key Infrastructure Part II: Operational Protocols
- Internet Public Key Infrastructure Part III: Certificate Management Protocols
- Internet Public Key Infrastructure Part IV: Certificate Policy and Certification Practices Framework
- Architecture for Public Key Infrastructure

4.7 Secure Shell (secsh)

Die Arbeitsgruppe „Secure Shell“ arbeitet an einem Update und der Standardisierung des populären SSH-Protokols, welches Unterstützung z.B. für sicheres Remote-Login und sicheren Filetransfer bietet. SSH kann automatisch verschlüsseln, authentifizieren und übertragene Daten komprimieren.
Die Arbeitsgruppe versucht sicherzustellen, daß das SSH-Protokoll

- starke Sicherheit gegen kryptoanalytische und Protokoll-Angriffe bietet,
- auch ohne globales Key-Management oder globale Zertifizierungs-Infrastruktur zufriedenstellend arbeitet,
- existierende Zertifizierungs-Infrastrukturen (z.B. SPKI, X.509) benutzen kann, sofern sie vorhanden sind.

Das resultierende Protokoll arbeitet über TCP/IP oder andere zuverlässige, aber unsichere Transportprotokolle und soll auf der Anwendungsebene implementiert werden.
Es existieren bisher (Juli 1997, [http://www.ietf.org]) keine RFCs und die Internet-Drafts

- SSH Transport Layer Protocol
- SSH Authentication Protocol
- Connect

4.8 Simple Public Key Infrastructure (spki)

Viele Internetprotokolle benötigen eine Public-Key Infrastruktur, wie schon oben bei „Public-Key Infrastructure (X.509)“ beschrieben. Die Arbeitsgruppe „Simple Public Key Infrastructure“ entwickelt einen Internetstandard für ein von der IETF unterstütztes Public-Key-Zertifikat Format, dazugehörige Signaturen und andere

Formate sowie Schlüsselerwerbsprotokolle. Die Formate und Protokolle sollen einfach zu verstehen, zu implementieren und zu benutzen sein und als „Simple Public Key Infrastructure“ SPKI bezeichnet werden. Nach Abschluß der Arbeit wird damit ein Alternativsystem zu X.509 zur Verfügung stehen.
Es existieren bisher (Juli 1997, [http://www.ietf.org]) keine RFCs und die Internet-Drafts

- Simple Public Key Certificate
- SPKI Requirements

4.9 Transport Layer Security (tls)

(Diese Arbeitsgruppe wurde in Gemeinschaft mit der Transport Area gegründet.)
Es existieren verschiedene Methoden zum Aufbau eines sicheren und authentischen Kanals zwischen Internet-Hosts auf Ebene der Transportschicht. Die Arbeitsgruppe „Transport Layer Security“ soll Standards für Protokolle herausgeben, die auf den existierenden Internetdrafts basieren.
Die sich ergebende Protokollspezifikation wird Methoden zur Implementierung von Vertraulichkeit, Authentikation und Integrität auf der Transportschicht umfassen.
Es existieren bisher (Juli 1997, [http://www.ietf.org]) keine RFCs und die Internet-Drafts

- The SSL Protocol Version 3.0
- SSH Transport Layer Protocol
- Addition of Kerberos Cipher Suites to Transport Layer Security (TLS)
- Addition of Shared Key Authentikation to Transport Layer Security (TLS)
- Modification of the SSL protocol for TLS
- The TLS Protocol Version 1.0

4.10 Web Transaction Security (wts)

Die Arbeitsgruppe „Web Transaction Security“ entwickelt Protokolle für die Sicherheit in WWW-Transaktionen, z.B. Transaktionen über das HyperText Transfer Protokoll HTTP. Die Arbeit läuft parallel zur und ist unabhängig von der Weiterentwicklung der Nicht-Sicherheitsfeatures in der HTTP-Arbeitsgruppe. Es werden zwei RFCs vorbereitet, eine Spezifikation für HTTP-Sicherheitsanforderungen (HTTP Security Requirements Specification) und eine Spezifikation für das HTTP Sicherheitsprotokoll (HTTP Security Protokoll Specification).
Es existieren bisher (Juli 1997, [http://www.ietf.org]) die RFCs

- RFC 2048, Considerations for Web Transaction Security

und die Internet-Drafts

- The Secure HyperText Transfer Protokoll
- Security Extensions for HTML

Kapitel 5

Standardisierung durch die Industrie

Im folgenden erfolgt eine kurze Beschreibung weiterer Organisationen, die in den anderen Kapiteln noch nicht erwähnt wurden und von denen teilweise Standards im Kapitel 6 beschrieben werden.

5.1 European Computer Manufacturers Association (ECMA)

Die im Mai 1991 gegründete *European Computer Manufacturers Association* (ECMA) ist eine nichtkommerzielle Organisation derjenigen europäischen Unternehmen, die sich mit Entwicklung, Herstellung und Vertrieb von Hard- und Software sowie Dienstleistungen im Bereich Informationstechnologie und Telekommunikation beschäftigen [Ford_94]. Die Tätigkeiten der ECMA umfassen die Entwicklung von ECMA-Standards und Technischen Reports, welche regelmäßig als Ausgangspunkt für die Arbeit von ISO/IEC und ITU verwendet wurden. ECMA hat formal den Status einer „Liaison Organization" zum ISO/IEC Subkomitee JTC1.
Die Zwecke der ECMA sind nach [ECMA_96]:

- Die Entwicklung von Standards und Technischen Berichten in Zusammenarbeit mit den entsprechenden nationalen, europäischen und internationalen Organisationen.
- Die Anregung zur korrekten Benutzung der Standards durch Beeinflussung der Umgebung, in der diese angewendet werden.
- Die Verbreitung von Standards aus den Bereichen Informationsverarbeitung und Telekommunikation.

Die ECMA besteht aus ordentlichen und assoziierten Mitgliedern sowie den Klassen von Mitgliedern, die durch die ordentlichen Mitglieder bei einer Generalversammlung gegründet werden. Eine derartige Klasse (die einzige bisher) sind die SME-Mitglieder (Small and Medium sized Enterprises), dies sind Unternehmen mit einem Jahresumsatz von weniger als 100.000.000 Schweizer Franken.
Ordentliche Mitglieder sind Unternehmen, die in Europa Hard- oder Software oder Dienstleistungen aus den Bereichen Informationsverarbeitung oder Telekommunikation entwickeln, produzieren oder vertreiben, die für geschäftliche, wissenschaftliche, Verwaltungs- oder ähnliche Zwecke genutzt werden. Produkte oder Dienstleistungen, die ausschließlich für militärische Zwecke genutzt werden, sollen dabei nicht

berücksichtigt werden [ECMA_96]. Der Repräsentant jedes ordentlichen Mitglieds hat eine Stimme in der Generalversammlung.
Assoziierte Mitglieder können alle Unternehmen werden, die Interesse und Erfahrung in den Angelegenheiten eines oder mehrerer Technischer Komitees der ECMA haben. Unternehmen, die die Anforderungen an ein ordentliches Mitglied erfüllen, können nicht assoziiertes Mitglied werden. Assoziierte Mitglieder haben kein Stimmrecht in der Generalversammlung.
SME-Mitglieder können diejenigen Unternehmen sein, die auch als ordentliches oder assoziiertes Mitglied in Frage kommen und einen Jahresumsatz von weniger als 100.000.000 Schweizer Franken haben. SME-Mitglieder haben kein Stimmrecht in der Generalversammlung.
Die Organe der ECMA sind nach [ECMA_96, ECMA - By laws]:

- Die Generalversammlung
  der ordentlichen Mitglieder. Sie ist die höchste Autorität der ECMA und kontrolliert die ECMA und ernennt und kontrolliert das Management. Sie tritt zweimal jährlich zusammen.

- Das Management,
  bestehend aus dem Präsidenten, dem Vizepräsidenten und dem Schatzmeister. Präsident und Vizepräsident werden für jeweils ein Jahr von der Generalversammlung gewählt. Kandidaten können nur die Vertreter ordentlicher Mitglieder sein. Der Schatzmeister wird von der Generalversammlung bestimmt und muß ebenfalls Vertreter eines ordentlichen Mitglieds sein.

  Der Präsident vertritt die ECMA nach außen.

- Das Koordinierungskomitee,
  das aus 6 Mitgliedern besteht und der Generalversammlung Empfehlungen für die Bildung, Aktivitäten, Reorganisation oder Auflösung der Technischen Komitees gibt.

- Das Sekretariat,
  das gegenüber der Generalversammlung verantwortlich ist und dessen Vorsitzender der von der Generalversammlung ernannte Generalsekretär ist. Dieser gründet auf Grundlage eines Beschlusses der Generalversammlung die Technischen Komitees.

- Die Technischen Komitees,
  in denen die eigentliche Standardisierungsarbeit geleistet wird. Mitglied eines Technischen Komitees können die Vertreter von ECMA-Mitgliedern oder andere vom Generalsekretär auf Anforderung des Technischen Komitees oder Managements eingeladene Teilnehmer sein.

  Hier interessiert besonders TC 36 - IT Security

Der Schwerpunkt der ECMA-Arbeit liegt auf dem Bereich OSI und andere Offene Systeme, einschließlich der Sicherheit offener Systeme.

5.2 X/Open und Open Software Foundation OSF - The Open Group

Die *Open Group* entstand im Februar 1996 aus dem Zusammenschluß von *X/Open Company Ltd.* und der *Open Software Foundation* (OSF). Die 1984 gegründete X/Open Company Ltd. arbeitet auf dem Gebiet der Produktspezifikation und -verifikation für offene Systeme, die 1988 gegründete OSF ist auf das Gebiet der

Technologieentwicklung und unternehmensübergreifende Entwicklungsprojekte für offene Systeme spezialisiert. Zusammen unter dem Namen Open Group werden technologische Innovationen und großmaßstäbliche Anpassungen von Spezifikationen für offene Systeme bearbeitet [http://www.open-group.com].
Die Arbeitsschwerpunkte der Open Group sind nach [Open_96]:

- Sicherheit
- Interoperabilität
- Management Verteilter Systeme
- Architektur
- Internet

Die Organisationen der Open Group sind unter anderem:

- Der Open Group Customer Council (OGCC),
  in dem die Benutzergruppen von X/Open und OSF zusammengefaßt sind.

  Er versorgt die Hersteller mit dem Blickpunkt der Anwender, ihren Anforderungen und Problemen.

- Die Technologieentwicklungsgruppen der OSF,
  - das OSF Research Institute,
    das zusammen mit Wissenschaft, Industrie und Regierung an der Entwicklung zukünftiger offener Systeme arbeitet,
  - der Pre-Structured Technology process (PST),
    der effektiv an existierender Technologie für den Markt arbeitet,
  - der Request For Technology process (RFT),
    der Probleme offener Systeme identifiziert und mit weltweiter Hilfe der Computerindustrie, der Bildungsinstitute, der Behörden und Benutzer zu lösen versucht.

- Der Standardisierungsprozeß von X/Open

5.3 Telecommunications Information Network Architecture Consortium (TINA-C)

Das *Telecommunications Information Network Architecture Consortium* (TINA-C), dessen Gründung auf der ISS92 im September 1992 verkündet wurde, beabsichtigt die Entwicklung eines Frameworks für den Bereich der Telekommunikation [http://www.tinac.com]. Dieses Framework beschreibt eine offene Architektur für Telekommunikationssysteme, welche die effiziente Einführung von Telekommunikationsdiensten und deren Management in zukünftigen, breitbandigen und multimedialen Telekommunikationsnetzen unterstützen soll [WSWZ_97].
Das TINA-Konsortium entwickelt nicht eine vollkommen neue Menge von Spezifikationen, sondern stützt sich auf die früheren Entwicklungen anderer Organisationen und Normungsinstituten. TINA-C kooperiert z.B. mit dem ATM Forum, DAVIC, der OMG und der ITU-T SG 10 und SG 11.
Das TINA-Konsortium besteht nach [http://www.tinac.com] aus den folgenden Komitees, Teams und Büros:

- Dem *Consortium Steering Board* (CSB)
  mit dem Präsidenten als Vorsitzenden, dem *Consortium Technical Leader* (TCL) als Führer des Core Team, verantwortlich für die Vertretung der technischen Ausrichtung von Projekten gegenüber dem CSB und CTC sowie dem *General Manager* als Kopf der Verwaltung.

  Seine Mitglieder sind Vertreter der Kernmitglieder und es ist für die Definition der allgemeinen Vorgehensweise des Konsortiums.

- Dem *Consortium Technical Committee* (CTC),
  bestehend aus Vertretern aller Mitglieder und verantwortlich für das Management aller Vorgänge, die dem Ziel des Konsortiums dienen.

- dem *Core Team* (CT),
  das aus Forschern der Mehrzahl der Mitglieder besteht und seinen Sitz in New Jersey, USA, hat. Es entwickelt und validiert die Architektur.

- der Verwaltung.

Die Arbeit des TINA-Konsortiums sollte bis Ende 1997 beendet sein. Im November 1997 wurde beschlossen, die Arbeit weitere 3 Jahre bis zum Jahr 2000 fortzuführen, um die bereits entwickelte Architektur weiter zu entwickeln und zu verfeinern. Für die Fortsetzung der Arbeit wurde die Organisation des Konsortiums geändert, siehe dazu die Homepage des TINA-Konsortiums unter <http://www.tinac.com>.

5.4 Object Management Group OMG

Die *Object Management Group* (OMG) wurde im Mai 1989 von 8 Unternehmen gegründet: 3Com Corporation, American Airlines, Canon Inc., Data General, Hewlett Packard, Philips Telecommunication N.V., Sun Microsystems und der Unisys Corporation. Im Oktober 1989 nahm die OMG ihre Tätigkeit als Non-Profit-Organisation auf. 1993 hatte die OMG bereist 300 Mitglieder, 1997 hat sie über 800 Mitglieder [http://www.omg.org]. Ihr Ziel ist „die netzwerktransparente Kommunikation heterogener Systeme auf der Basis objektorientierter Software-Komponenten zu ermöglichen.“ [Wagn_93]
Haupsitz der OMG ist Framingham, Massachusetts, USA und besitzt internationale Marketingpartner in Großbritannien, Deutschland, Japan, Indien und Australien.
Die OMG wurde gegründet, um einen Komponenten-basierten Softwaremarkt zu bilden, indem die Einführung standardisierter Objekt-Software beschleunigt wird. Die Charter der OMG umfaßt die Einführung von Industrierichtlinien und detaillierten Objekt-Management Spezifikationen für ein Framework für die Anwendungsentwicklung. Konform zu diesen Richtlinien erfolgt die Entwicklung einer heterogenen Umgebung über die Grenzen aller wichtigen Hardwareplattformen und Betriebssysteme hinweg. Heute existieren Implementationen von OMG-Spezifikationen für über 50 Betriebssysteme.
Zentrum der Arbeit der OMG ist die *Object Management Architecture* (OMA), dessen Referenzmodell die Ziele der OMG in Komponenten aufteilt, die durch die Technologien der Mitglieder abgedeckt sind. Es bildet den Plan (Roadmap) für die Kombination der sich ergebenden Technologien. Die OMA kann als drei Segmente mit fünf kritischen Komponenten betrachtet werden [http://www.omg.org]:

1. Anwendungsorientiert (Application Oriented)
   Die OMA charakterisiert Interfaces und Common Facilities als Lösungsspezifische Komponenten für die Anforderungen der Endbenutzer.

2. Systemorientiert (System Oriented)
   Object Request Broker und Object Services sind stark am System oder den Infrastruktur-Aspekten verteilter Objekte und deren Management orientiert.

3. Vertikal Marktorientiert (Vertical Market Oriented)
   Domain-Interfaces sind vertikale Anwendungen oder Domain-Spezifische Interfaces. Diese, verbunden mit Kombinationen inheriter Common Facilities- und Betriebssysteminterfaces bilden Anwendungs-Frameworks für viele industriebereiche.

5.4.1 Die Organisation der OMG

Die Organisation der OMG ähnelt denen der meisten anderen Organisationen, so besitzt sie ein Direktorium mit einem Präsidenten als Vorsitzenden. Das im Januar 1996 gegründete Architecture Board beaufsichtigt und leitet den technischen Prozeß der OMG, die technische Arbeit erfolgt in den Domain-Arbeitsgruppen (Domain Task Forces) und den Special Interest Groups (SIGs). Hier interessiert besonders die Security SIG, die ein Diskussionsforum für die Sicherheitsbelange der Endbenutzer bildet und mit den Arbeitsgruppen zusammenarbeitet. Sie berichtet dem OMG Architecture Board und hat die folgenden Aufgaben:

- Entwicklung von Sicherheitsanforderungen der Endbenutzer
- Dokumentieren, wie Sicherheit die Anforderungen der Wirtschaft unterstützen kann.
- Zusammenarbeit mit den OMG SIGs und Arbeitsgruppen, um eine generische Sicherheitsarchitektur zu entwickeln.

Kapitel 6

Vergleichende Übersicht über Standards zu Security Frameworks

Im folgenden wird erklärt, was ein Framework und eine API sind, danach werden eine Reihe von Framework-Standards, die Bereiche der Sicherheit und Kryptographie betreffen, genauer betrachtet.

6.1 Begriffe

6.1.1 Was ist ein Framework?

Floyd/Züllighoven definieren in [FlZü_97] Frameworks folgendermaßen: „**Rahmenwerk, Anwendungsrahmenwerk.** Sie sind Organisationsformen von Sammlungen objektorientierter Komponenten. Ein Rahmenwerk *(framework)* ist im Sinne von [Johnson 88] eine Konfiguration von Klassen, die ein Lösungsschema für eine Problemstellung vergegenständlichen. Ein Anwendungsrahmenwerk *(application framework)* ist eine spezielle Form eines Rahmenwerks, das die Grundstruktur und den Kontrollfluß einer vollständigen Anwendung enthält. Es liefert eine generische Lösung für eine Klasse von Anwendungsprogrammen; eine Lösung , die aber in den meisten Fällen noch anwendungsspezifisch durch Ableitung spezialisiert oder durch Parametrisierung ergänzt werden muß. Darüber hinaus bieten Anwendungsrahmenwerke oft eine einheitliche Benutzungsschnittstelle sowohl in Form von Präsentation als auch der Handhabung *(look and feel)*. Verglichen mit Klassenbibliotheken kommt hier der Gesichtspunkt hinzu, daß die anwendungsspezifischen Komponenten mit passenden Schnittstellen in ein Anwendungsrahmenwerk eingehängt werden. Der Kontrollfluß der Anwendung ist insgesamt bereits durch das Anwendungsrahmenwerk definiert und wird anwendungsspezifisch nur noch angepaßt.“
Ignoriert man in dieser Definition das „objektorientierte“, bekommt man eine allgemeine Definition für Frameworks: Es ist eine Sammlung von Funktionalitäten (Funktionen, Prozeduren, Methoden ...) für die Lösung bestimmter Aufgaben(bereiche), die zum Zweck einer einheitlichen Bedienung bzw. Anwendung zusammengefaßt werden. Oft sind sie in einem Schichtenmodell angeordnet, wobei die implementierten Funktionen von den im Schichtenmodell über ihnen stehenden Applikationen etc. benutzt werden. Dabei werden in den Frameworks oft generische Lösungen für bestimmten Problembereiche (hier im weitesten Sinne für den Bereich Sicherheit) zur Verfügung gestellt.

6.1.2 Was ist ein Application Programming Interface (API)?

Ein Application Programming Interface (API) ist nach [XOpe2_96, Glossar] das Interface zwischen der Anwendungssoftware und der Anwendungsplattform, durch welches alle von der Anwendungsplattform zur Verfügung gestellten Dienste unterstützt werden. Es dient primär der Portabilität der Anwendungsprogramme, doch kann auch die Zusammenarbeit von System und Anwendung durch eine Kommunikations-API unterstützt werden.

6.2 Überblick über betrachtete Frameworks

Im folgenden werden die Frameworks

- Secure Electronic Market Place for Europe (SEMPER) (6.3),
- Generic Security Service API (GSS-API) (6.4),
- Generic Cryptographic Service API (GCS-API) (6.5),
- Common Object Request Broker Architecture (CORBA) (6.6),
- Telecommunication Information Networking Architecture (TINA) (6.7),
- Intel Common Data Security Architecture (CDSA) (6.8),
- RSA Cryptographic Token Interface (Cryptoki) (6.9) und
- ISO/IEC 10181: Information technology - Open Systems Interconnection - Security frameworks for open systems (6.10)

betrachtet

6.3 SEMPER - Secure Electronic Market Place for Europe

Im Rahmen des EU-Projektes SEMPER (*Secure Electronic Market Place for Europe*) wird an der Entwicklung eines sicheren elektronischen Marktplatzes für Europa gearbeitet.
Die dafür entwickelte Architektur befaßt sich nach [SEMP1_96] mit folgenden typischen Situationen:

- Online-Handel (On-line purchase)
  Ein Händler akzeptiert elektronische Bestellungen und Zahlungen, die auf digitalen oder konventionellen Katalogen basieren und liefert physikalische oder digitale Güter.
- Subskription (Subscriptions)
  Eine Organisation liefert Dienste auf Subskriptionsbasis, z.B. Zeitungsnachrichten oder Datenbankenauskünfte.
- Elektronisches Einkaufszentrum (Electronic Mall)
  Eine Organisation bietet Dienste für verschiedene Service-Provider, von Verzeichnissen (directory services) über Inhalte (content hosting) zu Zahlungssystemen (payment services).
- Versteigerungen (Auctions)
  Benutzer können (evtl. anonym) an Versteigerungen teilnehmen, wobei die üblichen Fairnessregeln gelten.

- Sichere Kommunikation (Secure communication)
  Sichere Übertragung elektronischer Dokumente mit Sicherstellung von Vertraulichkeit, Nicht-Abstreitbarkeit (non-repudiation) etc.

- Vertragsunterzeichnungen (Contract signing)
  Zwei oder mehr Parteien tauschen signierte Kopien desselben Dokuments untereinander aus.

Für erste Versuche wurden die folgenden Basisdienste als notwendig erachtet: Authentifikation, Integrität, Signaturen, Zahlungssysteme und Vertraulichkeit.

6.3.1 Architektur

Im folgenden wird die grundlegende Architektur des SEMPER-Frameworks erläutert, wie sie in [SEMP1_96] beschrieben wird.

6.3.1.1 Dienste, Schnittstellen und Protokolle

SEMPER definiert eine Servicearchitektur mit mehreren *Schichten* (Layers, entsprechend dem ISO OSI-Referenzmodell (ISO 7498)).
Die aktiven Elemente einer derartigen Architektur werden als *Instanzen* (Entities) bezeichnet. Jede dieser Instanzen existiert in einem *Gerät* (Device), wobei damit ein physikalisches Objekt wie z.B. ein PC gemeint ist. Der Term *lokal* (local) bedeutet dabei „im selben Device".
Eine *Schicht* (layer) ist eine (virtuelle) Sammlung von Instanzen in allen Devices, die Funktionen auf dem gleichen Abstraktionsgrad ausführen. Grundlegende Funktionen werden in den niedrigeren Schichten zusammengefaßt, während die höheren Schichten komplexere Funktionen ausführen, die auf den niedrigeren Schichten aufbauen. Die Schnittstelle zwischen zwei Schichten wird als *Schichten-Interface* (layer interface) bezeichnet. Es ist die Gesamtheit aller Schnittstellen aller Instanzen dieser Schicht. Instanzen in derselben Schicht, die dieselben Dienste auf verschiedenen Devices anbieten, also gleichrangige Instanzen, werden als *Peer Instanzen* (Peer-Entities) bezeichnet.
Die Funktionalitäten, die eine Schicht an ihrem oberen Interface, d.h. für höhere Schichten anbietet, werden die *Dienste* (services) dieser Schicht genannt. Eine Schicht kann mehrere Dienste zur Verfügung stellen.
Eine Instanz kann auf die Dienste jeder niedrigeren Schicht an einem *Servicepunkt* (Service access point, SAP), siehe Abbildung 6.1, zugreifen. Ein *Dienst-Interface* eines Dienstes ist eine Teilmenge des Schichten-Interfaces, welches aus einem Servicepunkt und einer syntaktischen Definition der *Dienst-Primitiven* (Service primitives), die über diesen Servicepunkt ausgetauscht werden können, besteht. Eine Instanz, die einen Dienst in Anspruch nimmt, wird als *aufrufende Instanz* (invoking entity) bezeichnet.
Ein *Dienst* (Service) wird beschrieben, indem das mögliche Verhalten der gesamten Dienst-Interfaces angegeben wird, d.h. wie die Ein- und Ausgaben an den verschiedenen Servicepunkten voneinander abhängig sind, jedoch ohne zu beschreiben, wie diese Abhängigkeiten implementiert sind.
Ein *Protokoll* (protocol) beschreibt, wie ein Dienst aus Interaktionen von Peer-Instanzen unter Benutzung tieferer Schichten aufgebaut ist.

6.3.1.2 Serviceblöcke

Generische Dienst werden durch *Service-Manager* und mehrere *Service-Module* zur Verfügung gestellt, siehe Abbildung 6.2. (Das letzte Modul wurde speziell für Semper geschrieben und besitzt daher keinen Adapter.)

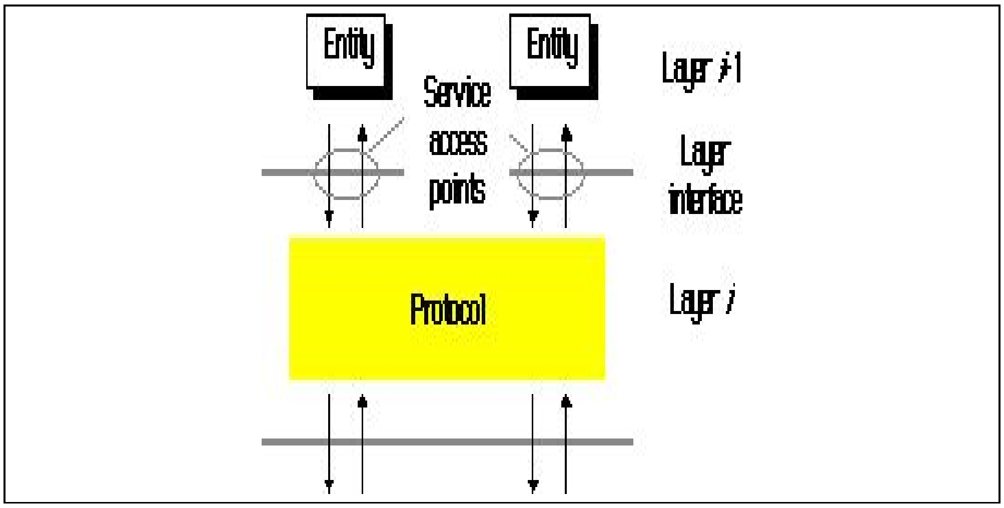

Abbildung 6.1: Schichten der Servicearchitektur (aus [SEMP1_96])

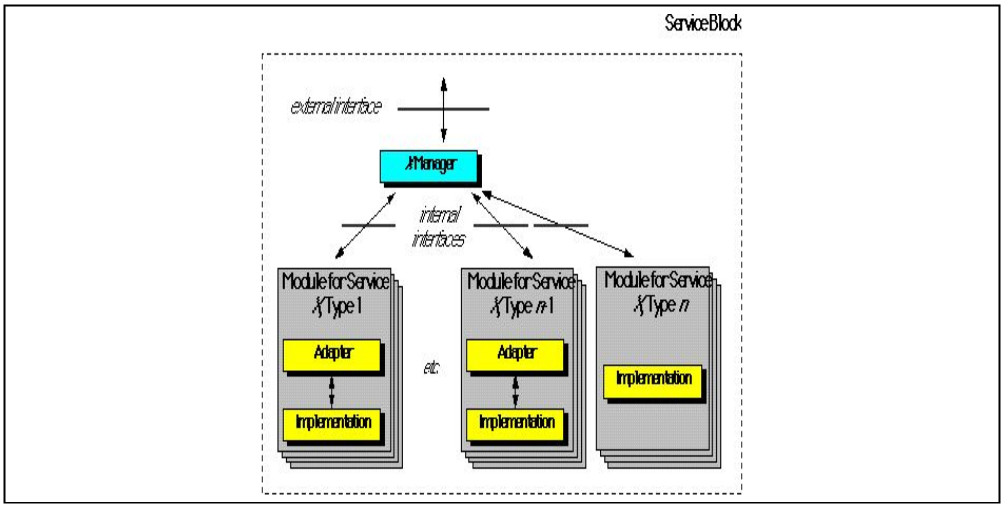

Abbildung 6.2: Manager, Module und Adapter (aus [SEMP1_96])

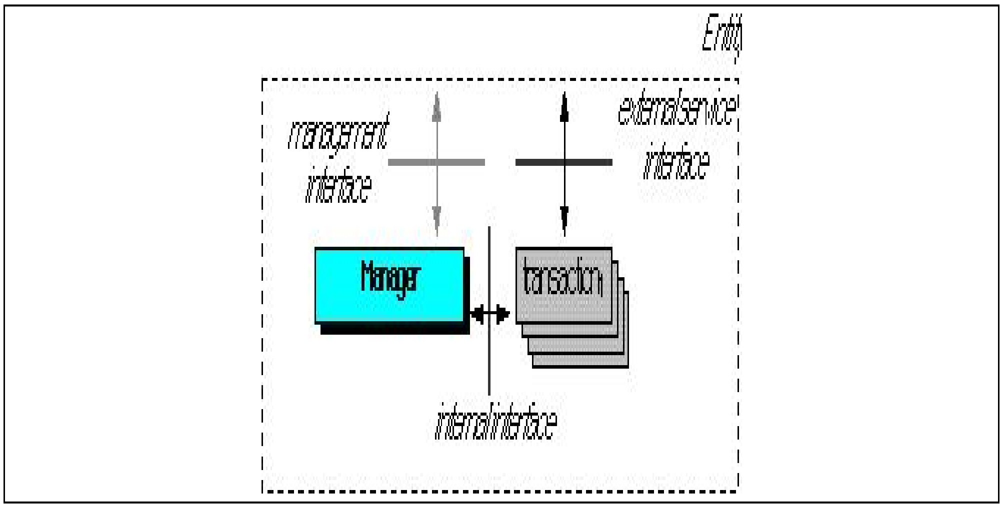

Abbildung 6.3: Instanzen (Manager oder Module) und ihre Transaktionen (aus [SEMP1_96])

Die Vereinigung aus einem Manager und seinen Modulen wird als *Service-Block* bezeichnet. Der Service-Block liefert generische, vereinheitlichte Dienste, z.B. Dienst = „Zahlung“. Das Interface, welches von den Instanzen des Blocks gebildet wird, als *Externes Interface* (External interface). Diese externen Interfaces liefern einen generischen Dienst, basierend auf einer Reihe verschiedener Protokolle für diesen Dienst.
Ein *Dienst-Manager* (Service-Manager) liefert ein einheitliches Interface für mehrere Module in Verbindung mit Methoden zur *Negotiation* (dabei handelt es sich um die Aushandlung der verwendeten Verfahren) und Auswahl einer geeigneten Methode.
Ein *Service-Modul* korrespondiert zur Implementierung eines Protokolls für den Dienst. Sein Interface zum Service-Manager wird als *Internes Interface* (internal interface) dieses Dienstes bezeichnet. Jedes generische Servicemodell kann mehrere verschiedene interne Interfaces definieren, die auf dem *Typ* der erwarteten Services seiner Module basieren.
Um auf existierende Produkte aufzubauen, die nicht zum Internen Interface kompatibel sind, werden die Interfaces existierender Implementierungen um *Serviceadapter* (service adapter) erweitert, so daß die daraus resultierenden Module die benötigten Services liefern.

6.3.1.3 Transaktionsobjekte und Kontext

Für die Ausführung eines Protokolls kann es notwendig sein, daß die beteiligten Instanzen sich auf bestimmte Parameter wie den Typ und die Qualität des zu benutzenden Services einigen. Das Sub-Protokoll für diese Verhandlungen wird *Negotiation* genannt. Das Ergebnis der Negotiation wird im sogenannten *Kontext* (context) gespeichert, einer für jede Instanz lokalen Datenstruktur, die das Ergebnis der Benutzerdefinierten Präferenzen, Konfigurationen und der Negotiation enthält.
Die Funktionen eines Serviceblocks können entweder direkt oder durch ein sogenanntes *Transaktionsobjekt* benutzt werden, siehe Abbildung 6.3.

6.3.1.4 Transfer, Austausch und Container

Beim Ausführen von Wirtschaftsaktionen treten zwei Arten von Übertragungen auf:

Party A sends → Party B sends ↓	Money	Signed document	Information
nothing	Payment	Certificate transfer etc.	Information transfer
Money	Fair money exchange	Fair payment with receipt	Fair purchase
Signed document		Fair Contract Signing	Fair conditional access
Information			Fair information exchange

Abbildung 6.4: Transfer (erste Zeile) und Austausch primitiver Typen (aus [SEMP1_96])

- Der *Transfer*,
  bei dem eine Partei eine Container genannte Datenstruktur an eine oder mehrere andere Parteien sendet. Die sendende Partei kann verschiedene Sicherheitsanforderungen an den Transfer stellen.

- Der *Austausch* (Exchange),
  der aus mehreren kombinierten Transfers besteht. Zwei oder mehr Parteien haben die Sicherheit, daß sie, wenn sie etwas spezifisches an die anderen übertragen, von diesen ebenso etwas spezifisches zurückerhalten.

Ein *Container* ist eine allgemeine Datenstruktur, für das was transferiert und ausgetauscht werden kann. Er kann mehrere *primitive Typen* (primitive types) enthalten, wie z.B.

- Signierte Dokumente,
  wie z.B. Zertifikate, Quittungen, signierte Stellungnahmen.

- Informationen,
  wie z.B. digitale Güter, Zugangsinformationen für einen Dienst (z.B. eine Adresse und Passwort, einen kryptographischen Schlüssel zum Entschlüsseln verschlüsselt gelieferter Daten) oder Informationen, die für die Nutzung physikalischer Güter notwendig sind.

- Elektronisches Geld

Information ist dabei etwas, das nicht für die Zwecke eines spezifischen Transfers oder Austauschs interpretiert wird, sondern einfach als Bit-String übertragen wird. Abbildung 6.4 listet die primitive Typen auf, die transferiert oder ausgetauscht werden können, wobei es evtl. weitere, detailliertere Sicherheitsattribute geben kann. Alle Services müssen definieren, was passieren soll, wenn eine der Parteien mit dem Ergebnis nicht einverstanden ist, d.h. wenn in einer bestimmten Stufe eine *Exception* ausgelöst wird. Dies kann geschehen, wenn

- eine Partei ungenügende Rechte besitzt,

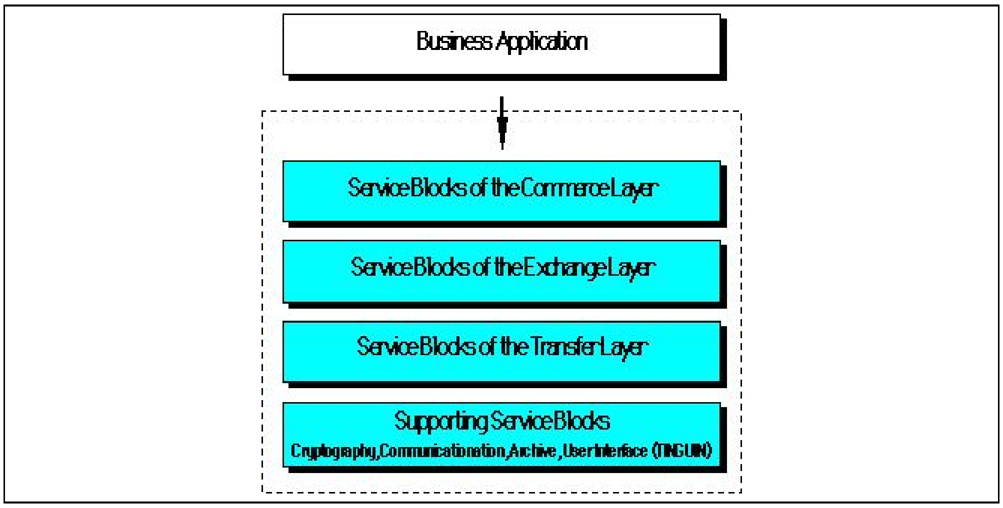

Abbildung 6.5: Übersicht über die Architektur von SEMPER (aus [SEMP1_96])

- ein unbeabsichtigter Fehler auftritt, z.B. wenn eine Nachricht verlorengeht, Softwareversionen inkompatibel sind etc., oder
- bei Fehlverhalten anderer, z.B. der Mißbrauch der Kreditkartennummer eines Unbeteiligten.

Falls eine Exception ausgelöst wurde, wird mit ihrer Behandlung durch einen *Exception Handler* begonnen, wobei zuerst davon ausgegangen wird, daß sich alle Parteien ehrenhaft verhalten haben. Schlägt dieser optimistische Ansatz fehl, befinden sich die Parteien in einem realen Disput, und pessimistischere Ansätze müssen verwendet werden, wobei ein Schlichter (Arbiter) und letztendlich ein Gericht hinzugezogen werden können. Für die Behandlung der Exception ist es notwendig, genau zu protokollieren ,was bisher geschehen ist, so daß sich die Parteien auf einen vorher bestehenden, unangefochtenen Zustand einigen können. Für die Disputbehandlung müssen unanfechtbare Beweise vorhanden sein. Für die Exceptionbehandlung kann ein Wechsel des Kommunikationsprotokolls notwendig sein, z.B. von http zu asynchroner E-Mail, jedoch soll sie soweit möglich im digitalen System stattfinden. Der Wechsel zu Aktionen außerhalb des digitalen Systems, z.B. Telefonanrufe oder Briefe mit handschriftlicher Signatur (also der üblichen Unterschrift), sollte minimiert werden, kann aber als letzter Ausweg notwendig sein.

6.3.1.5 Überblick über die Service-Architektur

Die SEMEPR-Architektur besteht aus 4 Schichten, siehe Abbildung 6.5.

6.3.1.5.1 Business Application

Die *Business Application* ist eine Instanz der Schicht, die die SEMPER-Library benutzt. Eine Business Application benutzt die Dienste der unter ihr liegenden Schichten, primär die des Commerce Layers.

6.3.1.5.2 Commerce Layer

Im *Commerce Layer* werden die Protokolle für Geschäftsaktionen implementiert, z.B. wie bestimmte Händler die Registrierung von Kunden, deren Bestellungen, Zahlungen und Belieferung organisieren. Außerdem sind hier Services genereller Art implementiert, wie z.B. für die Anzeige und das Ausfüllen von Formularen.

6.3.1.5.3 Exchange Layer

Im *Exchange Layer* werden Services für den fairen Austausch von Gütern implementiert.

6.3.1.5.4 Transfer Layer

Im *Transfer Layer* werden Funktionen zum Senden, Empfangen und Konstruieren von Containern implementiert, um Informationen zwischen Kommunikationspartnern unter Beachtung vorgegebener Sicherheitsattribute auszutauschen.
Alle Daten, die mit dem Transfer Layer übertragen werden, werden in einem Container (s.o.) gespeichert. Der Transfer oder der Container besitzen *Sicherheitsattribute* (security attributes), z.B. Nichtabstreitbarkeit des Absenders.
Diese Schicht umfaßt den *Transfer Manager*, den *Payment Service Block*, den *Statement Service Block* und den *Certificate Service Block*.

6.3.1.5.5 Supporting Services

Die *Supporting Services* implementieren Funktionen, die von allen über ihnen liegenden Schichten benutzt werden. Im einzelnen sind dies

- die *Cryptographic Services*,
  z.B. für Ver- und Entschlüsselung, Hashfunktionen, Message Authentication Codes, digitale Signaturen und die Schlüsselgenerierung.

- die *Communication Services*
  für die Kommunikation zwischen verschiedenen Instanzen. Diese Funktionen sind unabhängig vom benutzten Netzwerk und Protokollen. Die Communication Services trennen die anderen Schichten von Details des Netzwerks. Die grundlegenden Kommunikationsdienste werden durch die sogenannten *ComPoints* realisiert, die wie Sockets den Zugriff zu darunterliegenden Kommunikationsprotokollen ermöglichen. Für jedes unterstützte Protokoll existiert eine Klasse, die die ComPoints für dieses Protokoll implementiert. Die ComPoints werden durch *Channels* verfeinert, die es ermöglichen, daß mehr als ein Paar von Modulen eine spezifische Portnummer zwischen zwei Hosts benutzen. Dieses geschieht durch die Einrichtung eines Kanals (Channels) zwischen Initiator und Responder.

- die *Archive Services*
  für die Speicherung und Archivierung aller persistenten Daten.

- die *Trusted Interactive Graphical User Interface Services* (TINGUIN),
  die die Benutzerschnittstelle bilden.

- die *Preference Service*,
  zuständig für die Verwaltung der Präferenzen.

- die *Access Control Services*,
  mit denen die Zugriffskontrolle auf die verschiedenen Blöcke von SEMPER realisiert wird, die verhindert, daß potentiell gefährliche oder ungewünschte Aktionen von nicht autorisierten Benutzern oder ohne ausdrückliche Zustimmung des Benutzers stattfinden.

Vergleich:
Hier ergibt sich der erste Unterschied zwischen SEMPER und anderen APIs und Frameworks: Während letztere allgemein von Anwendungsprogrammen verwendet werden, die mit Hilfe der APIs z.B. ihre Kommunikation schützen, ist diese Anwendung bei SEMPER in Form der Business Application enthalten. Andererseits kann man SEMPER

auch als eine Kombination von Anwendung (d.h. Business Application) und API (d.h. alle anderen Teile von SEMPER) auffassen.
Allgemein besteht SEMPER aus vielen verschiedenen APIs: Einzelnen Blöcken und den Vereinigungen aus ihnen.
Im folgenden werden diejenigen Blöcke der SEMPER-Software beschrieben, die für diese Arbeit von besonderem Interesse sind, und sie werden mit anderen Frameworks in Beziehung gesetzt.

6.3.2 Sichere Kanäle

6.3.2.1 Überblick

Die *Secure Communication Channels* der SEMPER-Software werden in [BrSc_97] beschrieben. Es handelt sich dabei um einen Block, der sichere Kanäle für die übertragenen Daten zur Verfügung stellt (also Vertraulichkeit und Authentizität) sowie eine anonyme Kommunikation ermöglicht. Dabei wird allein die Übertragung betrachtet - weitere Folgen außerhalb der Kommunikationsverbindung werden nicht berücksichtigt, etwa Nichtabstreitbarkeit oder Fairneß.
Der *Secure Communication Block* (SecCom-Block) dient dem Austausch von Objekten zwischen zwei Partnern. Er umfaßt die folgenden fünf Elemente: Die

1. Objekte,
   die über die sichere Verbindung übertragen werden, die

2. Adressen,
   die die an der Kommunikation Beteiligten bezeichnen, die

3. Verbindungen,
   über die die Kommunikation abläuft, in der Regel ComPoints oder Channels, den

4. Verbindungsaufbau,
   der unter Berücksichtigung der gewünschten Sicherheitsattribute (z.B. Vertraulichkeit, Anonymität, ...) erfolgt und die

5. Sicherheitsattribute,
   die für eine Verbindung die dabei geforderten Sicherheitsfunktionen festlegen.

Der SecCom-Block besteht aus dem Secure Communication Manager, zuständig für den Verbindungsaufbau, und verschiedenen Servicemodulen, die Sicherheitsfeatures bereitstellen und die aktuelle Kommunikation durchführen (siehe Abbildung 6.6).

6.3.2.2 Secure Communication Manager

Der *Secure Communication Manager* selbst beinhaltet keine Sicherheitsmechanismen, er ermittelt aus den Anforderungen des die Verbindung eröffnenden Teilnehmers die benötigten Sicherheitsfunktionen und wählt daraufhin das Servicemodul aus, das diese Anforderungen am besten erfüllt. Die Servicemodule können auf den Communication Block zurückgreifen, der zur Zeit die Protokolle TCP, HTTP und Mail unterstützt.
Die gewünschten Sicherheitsfunktionen werden dem SecCom-Block über das Setzen von *Sicherheitsattributen* mitgeteilt, woraufhin ein geeignetes Servicemodul ausgewählt wird. Der Secure Communication Manager besitzt eine Matrix, die die Zuordnung von Sicherheitsattributen (und ihren Kombinationen) zu den Servicemodulen enthält.

Die Adressierung erfolgt durch die Servicemodule, da es verschiedene Adressierungsarten (z.B. für anonyme Kommunikation) gibt. Der SecCom-Block besitzt ein Interface, das die Ermittlung der Adressen, ihre Veröffentlichung und ihre Wiederbenutzung ermöglicht.
Die Kommunikation erfolgt zwischen einem Initiator-Objekt und einem Responder-Objekt, eventuell über eine oder mehrere Dritte Parteien, um Anonymität sicherzustellen. Der Responder muß einige Vorbereitungen treffen, bevor der Initiator die Kommunikation tatsächlich starten kann. Nachdem eine Verbindung aufgebaut wurde, kann die Kommunikation in beide Richtungen erfolgen. Die gesamte Kommunikation erfolgt synchron, d.h. daß eine Schreiboperation bei einem Teilnehmer von einer Leseoperation beim anderen Teilnehmer begleitet wird.

6.3.2.3 Sicherheitsattribute

Die *Sicherheitsattribute* gelten nur für die Richtung vom sie bestimmenden Teilnehmer zum anderen Teilnehmer.
Mögliche Sicherheitsattribute sind für Daten Vertraulichkeit und Authentizität, für das Wissen über die Identität der Teilnehmer Anonymität (wenn sich beide Teilnehmer nur unter einem Pseudonym kennen) und schwache Anonymität (wenn sich die Teilnehmer zwar kennen, aber die Kommunikation zwischen ihnen von Außenstehenden nicht beobachtet werden kann).

6.3.2.4 Servicemodule

Die *Servicemodule* implementieren ein Kommunikationsinterface und sind für die Durchführung der zugeordneten Sicherheitsmechanismen zuständig. Das Kommunikationsinterface ist annähernd dasselbe wie die ComPoints und Channels des Communication Blocks (siehe oben). In den meisten Fällen können die Servicemodule auf die existierenden Funktionen im Communication Block zurückgreifen, für anonyme Verbindungen gilt dies jedoch nicht, so daß ein spezieller Block für anonyme Kommunikation notwendig ist. Alle Servicemodule müssen auch das Interface für die Adressierung implementieren.

6.3.2.5 Adressierung

Die Adressierung im SecCom-Block erfolgt für jedes Servicemodul anders, je nach den Erfordernissen dieses Moduls, z.B. wenn die Adressen auch Portnummern, Hostnamen oder MIX-Namen enthalten. Der Secure Communication Manager ruft das entsprechende Servicemodul für die Adreßgenerierung auf, das Ergebnis ist eine Kombination der Sicherheitsattribute und einer für das Servicemodul spezifischen Adresse. Für die Adreßgenerierung gibt es drei Möglichkeiten:

1. Direkt durch die Instantiierung eines Servicemodul-Adreßobjektes, wobei alle notwendigen Datenfelder ausgefüllt und die benötigten Sicherheitsattribute gesetzt werden

2. Bildung eines Adreßobjektes aufgrund einer von anderer Stelle erhaltenen Adresse (z.B. von einer Webseite, aus einer E-Mail, Eingabe des Benutzers).

3. Öffnen eines Responder-Objekts mit den benötigten Sicherheitsattributen und Abfragen der Adresse aus diesem Objekt.

Die Öffnung eines anonymen Responders erfolgt einfach durch das Abfragen seiner anonymen Adresse.

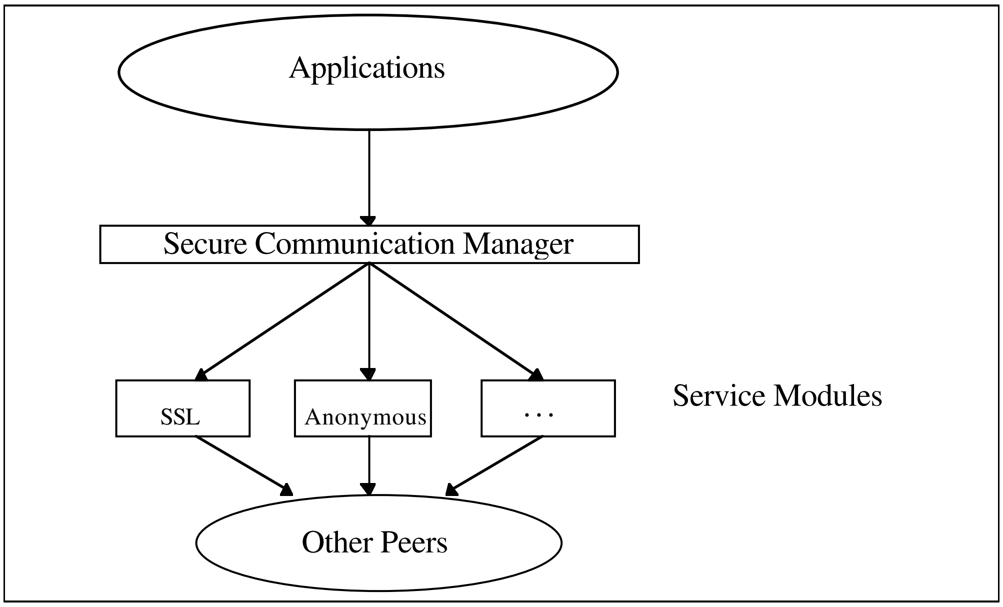

Abbildung 6.6: Der Aufbau des SecCom-Block (aus [BrSc_97])

6.3.2.6 Anonymität

Anonyme Verbindungen können aufgebaut werden, wenn der Initiator ein Pseudonym des Responders kennt. In der obigen Schreibweise handelt es sich dabei um die Adresse des anonymen Responders. Die Übertragung des Pseudonyms muß außerhalb des SecCom-Blocks erfolgen, z.B. über eine Webseite. Eine Möglichkeit zum Bilden eines Pseudonyms besteht im Aufbauen einer anonymen Verbindung als Responder und die Abfrage der Adresse des Verbindungsobjektes.

6.3.2.7 Design

Die gesamte SEMPER-Software wird in Java entwickelt. Im folgenden werden die für den SecCom-Block notwendigen Klassen beschrieben.

SecComPointAdress
: SecComPointAdress bildet ein Interface für die Spezifikation der Sicherheitsattribute in Verbindung mit den (evtl. von der Servicemodulen abhängigen) Adressen. Die Servicemodule müssen Unterklassen von SecComPointAdress zum Bilden ihrer spezifischen Adressen enthalten. Außerdem müssen die Servicemodule eine Methode zur Adreßgenerierung ohne Vorlagen enthalten.

SecComManager Interface
: Der SecComManager enthält Methoden zum Generieren und Öffnen von ComPoints.

SecComPoint Interface
: Alle Servicemodule müssen das SecComPoint Interface implementieren. Es erweitert das ComPoint Interface, um eine einfachere Integration in den existierenden Code zu ermöglichen. Es umfaßt unter anderem Methoden zum Lesen, Schreiben, Schließen und Akzeptieren von ComPoints sowie zum Ermitteln der Sicherheitsattribute und Adressen.

SecChannel Interface
SecChannel stellt Methoden für das Öffnen sicherer Kanäle zur Verfügung, analog zum existierenden Communication Block.

Sicherheitsattribute für SecComPoints und SecChannels
Die Sicherheitsattribute werden dem Packet semper.txlayer.attribute entnommen. Es handelt sich um die folgenden Attribute:

- Confidentiality
  für die Sicherstellung der Vertraulichkeit, üblicherweise durch Verschlüsselung der übertragenen Daten,
- Authenticity
  zum Sicherstellen der Authentizität,
- Anonymity
  für die Wahrung der Anonymität sowie
- WeakAnonymity
  um die eigene Identität gegenüber Außenstehenden zu verbergen.

Die Attribute werden in Attributmengen zusammengefaßt. Alle Methoden und Konstruktoren innerhalb des SecCom Blocks, die sich mit Attributen befassen, erwarten diese Attributmengen als Parameter.

Servicemodul BasicServices
Das BasicServices Modul implementiert die Sicherheitsattribute Vertraulichkeit (Confidentiality) und Authentizität (Authenticity) und benutzt die ComPoints und Channels des Communication-Managers mit dem TCP-, Mail- und HTTP-Protokoll. Vertraulichkeit wird durch die Verschlüsselung der gesendeten Daten erreicht, die Authentizität wird durch das Anhängen eines Message Authentication Codes (MAC) erreicht. Zusätzlich wird jeder Datenblock mit einer verschlüsselten Sequenznummer versehen, um sicherzustellen, daß alle Blöcke in der gleichen Reihenfolge entschlüsselt wurden, in der sie gesendet wurden.

6.3.3 Kommunikation mittels des SecCom-Blocks

Sehr vereinfacht funktioniert die Kommunikation mit Hilfe des SecCom-Blocks wie in Abbildung 6.7 gezeigt: Der Aufrufer (Caller) des Senders kommuniziert mit seinem SecCom-Manager, der die Servicemodule entsprechend steuert. Dabei beginnt die Kommunikation mit einer Eingabe beider Aufrufer an den SecCom-Manager, mit der die gemeinsame Kommunikation eingeleitet wird. Die (gegebenenfalls geschützte) Nachricht wird mit Hilfe der Servicemodule über ein im Allgemeinen ungesichertes Netz an den Kommunikationspartner, d.h. hier den Empfänger, übertragen, dessen Servicemodule die Nachricht empfangen und entsprechend bearbeitet an ihren SecCom Manager weiterleiten. Dieser übermittelt sie dann an seinen Aufrufer (Caller). Bei dieser Betrachtung wurden einige Tätigkeiten und Funktionen, wie z.B. die Festlegung der Schutzfunktionen, nicht betrachtet. Die Aushandlung der zu verwendenden Funktionen erfolgt zwischen den SecCom-Manager in Verbindung mit ihren Servicemodulen ohne Zutun des Aufrufers, der nur die gewünschten Sicherheitsattribute angibt.
Die Kommunikationspfeile in Abbildung 6.7 zeigen jeweils in beide Richtungen, da auch ein Empfänger die Kommunikation starten kann, etwa wenn er explizit ein Empfangen einleitet, indem er eine Nachricht vom Sender anfordert.

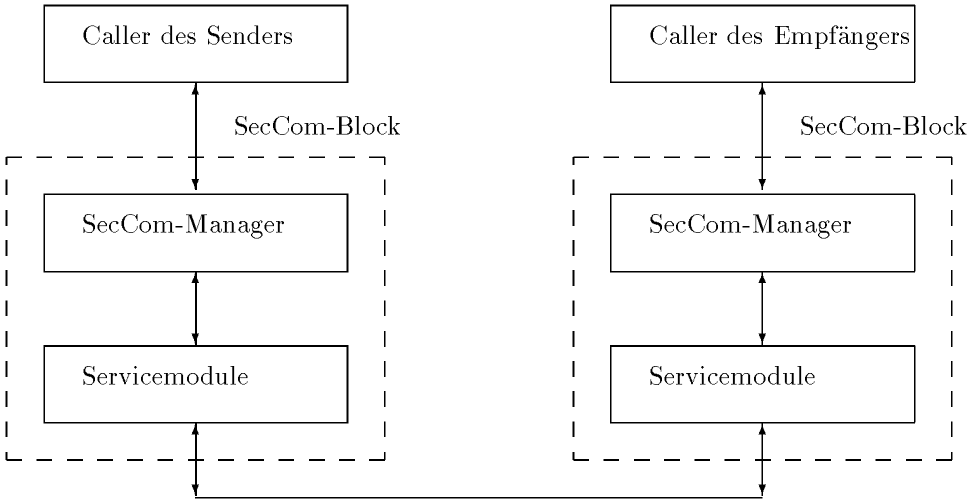

Abbildung 6.7: Kommunikation über den SEMPER SecCom-Block

6.4 Generic Security Service API (GSS-API)

Wie bereits in Abschnitt 4.2 zu lesen war, beschäftigt sich die Arbeitsgruppe „Common Authentication Technology (cat)“ der IETF mit der Entwicklung eines Verteilten Sicherheitsservices (distributed security services), einschließlich Authentikation, Integrität und Vertraulichkeit, für eine Vielzahl von Protokoll-Aufrufern, wobei diese Aufrufer von der Spezifikation der tieferliegenden Sicherheitsmechanismen isoliert werden.
Ein Ergebnis dieser Arbeitsgruppe ist die *Generic Security Service Application Program Interface* (GSS-API), die erstmals in RFC 1508 definiert und in [RFC_2078] überarbeitet wurde. Die GSS-API liefert Sicherheitsdienste für Aufrufer in einer generischen Art, wobei sie auf eine Reihe von darunter liegenden Mechanismen und Technologien aufsetzt und dadurch die Portabilität von Anwendungen zwischen verschiedenen Systemen auf Quelltextebene ermöglicht. [RFC_2078] definiert die GSS-API Dienste auf einer von den darunterliegenden Schichten und Programmiersprachen unabhängige Weise. Andere Spezifikationen z.B. für spezielle Programmiersprachen und Protokolle sind die Aufgabe anderer Dokumente, z.B. sind in RFC 1509, „Generic Security Service API: C-bindings“ die Bindings für C beschrieben.

6.4.1 Überblick

Die GSS-API arbeitet folgendermaßen: Ein Typischer GSS-API-Aufrufer ist selbst ein Kommunikationsprotokoll, welches die GSS-API aufruft, um seine Kommunikation mit Authentikations-, Integritäts- und / oder Vertraulichkeitsmechanismen zu schützen. Ein GSS-API-Aufrufer akzeptiert Token (dies sind die Datenelemente, die zwischen den GSS-API Aufrufern übertragen werden), die er von seiner lokalen GSS-API-Implementierung erhält und überträgt sie an seinen Kommunikationspartner auf einem anderen System, der Kommunikationspartner übergibt die Token zur Weiterverarbeitung an seine lokale GSS-API-Implementierung. Die durch die GSS-API verfügbaren Sicherheitsmechanismen werden durch eine Reihe von unter ihr liegenden Mechanismen implementiert, die sowohl auf Secret Key als auch auf Public Key Verfahren basieren können.

Vergleich:

Die Sicherheitsmechanismen entsprechen den Servicemodulen im SEMPER SecCom-Block, mit dem Unterschied, daß sie bei SEMPER Teil des SecCom-Blocks sind, während sie bei der GSS-API nicht Teil der API sind, sondern nur von ihr benutzt werden. Bei beiden müssen die oberen Schichten wissen, welche Module vorhanden sind (SEMPER) bzw. welche Mechanismen vorhanden und adaptiert sind (GCS), um dann ein geeignetes Modul, das bei beiden Kommunikationspartnern vorhanden ist, auswählen zu können. Die in der GSS-API definierten Parameter und Nachrichtennamen müssen in die Sprache und Abläufe der spezifischen Implementierung übersetzt werden, während dies bei SEMPER durch eine einheitliche Implementierung entfällt - wenn in verschiedenen Implementierungen die gleichen Module vorhanden sind, sind sie auch identisch implementiert.

Die GSS-API verfolgt mehrere Ziele, wie z.B. die Unabhängigkeit von den unter ihr liegenden Mechanismen sowie vom verwendeten Protokoll.

6.4.2 Aufbau der GSS-API

Referenzen (Credentials)

Referenzen beschreiben die Voraussetzungen, die für den Aufbau eines Sicherheitskontextes notwendig sind. Der Aufrufer kann bestimmte Referenzen als Defaultwert festlegen, oder für einzelne Verbindungen gezielt einzelne Referenzen auswählen.

Eine einzelne Referenz kann gleichzeitig sowohl für eingehende wie auch für ausgehende Verbindungen benutzt werden.

Eine Referenzstruktur kann mehrere Referenzelemente enthalten, die jeweils die Informationen für eine spezifische Funktion der unterhalb der GSS-API liegenden Schichten enthält, aber jede dieser Referenzenmengen innerhalb einer bestimmten Referenzstruktur ist eine Einheit. Der Inhalt einer Referenzstruktur einer bestimmten GSS-API-Implementierung kann in Abhängigkeit von der Implementierung der tieferen Schichten sehr unterschiedlich ausfallen, da jedes Element der Referenzstruktur die Daten enthält, die für den Aufbau eines Kontextes durch den dazugehörenden Mechanismus notwendig sind.

Vergleich:

Generell entsprechen die Referenzen teilweise dem, was allgemein als Zertifikat bezeichnet wird. Sie entsprechen auch etwas den Adressen in SEMPER.

Die tieferliegenden, systemspezifischen Schichten sind dafür zuständig, daß Referenzen benutzt werden können und die damit spezifizierten Funktionen zur Verfügung stehen. Wurden Referenzen einmal eingerichtet, ist die Übertragung dieser Referenzen zu anderen Prozessen oder dazu analogen Konstrukten innerhalb des Systems nicht mehr Aufgabe der GSS-API, sondern muß lokal geleistet werden. Ein Beispiel dafür ist die Übertragung von Rechten, die sich nach einem Login für einen Account ergeben, auf andere Prozesse, die unter diesem Account laufen.

Tokens

Als Token werden die Datenelemente bezeichnet, die zwischen den GSS-API Aufrufern übertragen werden. Sie werden in zwei Klassen unterteilt, einmal die Kontext-Token (Context-level token), die für den Aufbau und die Verwaltung eines Sicherheitskontextes zwischen den Teilnehmern benötigt werden, und die Nachrichten-Token (peer-message token), die einem eingerichteten

Kontext zugeordnet sind und ausgetauscht werden, um die gewünschten Sicherheitsfunktionen für die dazugehörenden Daten zu erhalten.

Das erste ausgetauschte Kontext-Token erlaubt eine globale Identifikation des benutzten Sicherheitssystems und umfaßt einen gegebenenfalls erforderlichen Schlüssel, alle danach ausgetauschten Token beziehen sich auf dieses System.

Die Tokens sind für die Aufrufer undurchsichtig, sie werden von der GSS-API des einen Teilnehmers erzeugt und ausgegeben, von Aufrufenden an den anderen Teilnehmer übermittelt und von diesem an seine lokale GSS-API zur Auswertung übergeben.

Vergleich:
Für Tokens gibt es nichts vergleichbares im SEMPER SecCom Block, sie entsprechen den Dingen, die ein SecCom-Modul intern an den CommBlock übergibt.

Die Token enthalten in der Regel mechanismenspezifische Informationen, um den Mechanismen den Umgang mit dem Token für verschiedene Zwecke zu erlauben. Dies erlaubt es z.B. auch, festzustellen, ob ein Token vom Aufrufer an einen nicht dafür zuständigen Mechanismus übergeben wurde.

Die Tatsache, daß eine bestimmte Funktion durch ein bestimmtes kryptographisches Protokoll oder eine bestimmte kryptographische Technik als tieferliegende Schicht ausgeführt wird, bedeutet nicht, daß die davon erzeugten Token von diesem Protokoll oder dieser Technik außerhalb des Zusammenhangs der GSS-API verarbeitet werden können. Daraus folgt, daß Benutzer der GSS-API nicht notwendigerweise mit Teilnehmern, die dieselben Protokolle und Techniken ohne GSS-API benutzen oder deren GSS-API dieselben Protokolle und Techniken in einer anderen Implementierung benutzt, kommunizieren können.

Sicherheitskontext (Security Context)

Ein Sicherheitskontext wird zwischen zwei Teilnehmern durch Referenzen festgelegt. Er beschreibt, welche Sicherheitsfunktionen und zugehörige Schlüssel bei der Kommunikation zwischen diesen beiden Teilnehmern verwendet werden sollen. Multiple Sicherheitskontexte können zwischen Gruppen von Teilnehmern eingerichtet werden.

Da die GSS-API unabhängig von den in den tiefer liegenden Schichten implementierten Protokollen und Adressierungsarten ist, ist es Aufgabe der Aufrufer, die von der GSS-API gelieferten Datenelemente zu übertragen. Daraus ergibt sich, daß der Aufrufer dafür verantwortlich ist, die empfangenen Daten zu parsen und die die GSS-API betreffenden Datenelemente von den den Aufrufer betreffenden Daten zu trennen. Dies macht die GSS-API unabhängig davon, ob die tieferliegenden Schichten auf eine bestehende Verbindung zum anderen Teilnehmer angewiesen sind oder verbindungslos arbeiten.

Vergleich:
Ein GSS-API Kontext entspricht einem SEMPER-Kanal.

Mechanismentypen (Mechanism Types)

Die Mechanismentypen dienen dazu, die benutzten Mechanismen der tiefer liegenden Schichten zu bestimmen, da sowohl Initiator als auch Responder denselben Mechanismus benutzen müssen. Sie definieren nicht nur das verwendete kryptographische Protokoll, sondern auch die Syntax und Semantik der ausgetauschten Datenelemente, die für die Benutzung der Sicherheitsfunktionen notwendig sind.

Der Aufrufer kann in seinem Sicherheitskontext „Default“ wählen, woraufhin durch die GSS-API mittels systemspezifischer Funktionen der benötigte

Mechanismus festgelegt wird, er kann aber auch direkt einen bestimmten Mechanismus angeben.

Bei der Übertragung zwischen den Teilnehmern werden die Mechanismentypen, repräsentiert durch Object Identifiers (OIDs), benutzt, um die Interpretation der zugehörigen Token zu ermöglichen. Die OIDs werden nur im ersten Token eines Kontext benötigt, für den Rest der Kommunikation in diesem Kontext liegt der Mechanismus damit fest.

Vergleich:
Hierzu gibt es bei SEMPER nichts vergleichbares.

Namen

Die Namen dienen in der GSS-API als Bezeichner der zu adressierenden Personen, Rechner oder was immer als Kommunikationspartner verwendet wird. Sie werden verwendet, um von den evtl. unterschiedlichen Adressierungsarten der tieferen Schichten unabhängig zu sein.

Übersetzungsfunktionen für die Verwendung der Namen in verschiedenen Adressierungssystemen sind nicht Teil der GSS-API und müssen lokal zu Verfügung gestellt werden.

Vergleich:
Namen entsprechen in SEMPER den Adressen. Beide sind mechanismen- bzw. modul-spezifisch.

Kanalanbindung (Channel Bindings)

Die GSS-API unterstützt das Konzept der Kanalanbindung durch den Aufrufer (caller-provided channel binding). Die Kanalanbindungen werden genutzt, um die Qualität der Authentikation während des Aufbaus des Sicherheitskontextes zu erhöhen, während gleichzeitig die Wiederbenutzung eines bereits benutzten Kontext-Tokens durch einen Angreifer erschwert wird.

Vergleich:
Hierzu gibt es bei SEMPER nichts vergleichbares.

Statusmeldungen

Jeder GSS-API-Aufruf liefert zwei Rückgabewerte für den Status, den Major_status, der einen vom verwendeten Mechanismus unabhängigen Wert zurückliefert, und den Minor_status, der detailliertere Statusinformation liefert, die aber spezifische Statusinformationen der Mechanismen in den tieferliegenden Schichten enthalten kann. Die Major_status-Codes werden in [RFC_2078] spezifiziert, während die Minor_status-Codes nicht spezifiziert werden und damit von der Implementierung abhängig sind.

Es gibt z.B. Codes für die in einem Sicherheitskontext verwendeten Sicherheitsdienste, für das Erkennen von Replays und für die Qualität des Schutzes.

Vergleich:
Hierzu gibt es beim SEMPER SecCom-Block nichts vergleichbares, es ist aber mit den Fehlermeldungen (Exceptions) von SEMPER vergleichbar.

Anonymität

Es können Situationen oder Umstände auftreten, in denen eine Anwendung einen Kommunikationspartner authentisieren und / oder Kommunikation mit der GSS-API schützen möchte, ohne seine eigene Identität preiszugeben.

Bei der üblichen Benutzung der GSS-API wird die Identität des Initiators eines Kontextes während des Aufbaus dieses Kontextes dem Kommunikationspartner mitgeteilt. Um Anonymität zu ermöglichen, ist es notwendig, diese Information während des Aufbaus zu verbergen. Dafür sind keine spezielle

Mechanismen notwendig, es wird lediglich über ein Flag angegeben, daß die Identität des Aufbauenden nicht an den Kommunikationspartner weitergeleitet wird, und über einen Rückgabewert wird dem Aufrufer signalisiert, ob seinem Wunsch nach Anonymität entsprochen wurde oder nicht.

Vergleich:
Hier wird Anonymität erreicht, indem die Identität des den Kontext aufbauenden Kommunikationspartners nicht übertragen wird. Dadurch kann es nur Anonymität in eine Richtung geben (ähnlich einem anonymen Telefonanruf: Der Angerufene kennt die Identität des Anrufers nicht, dieser aber die des Angerufenen) während bei SEMPER auch Anonymität in beide Richtungen möglich ist (keiner von beiden kennt die Identität des anderen).

Nicht betrachtet wird hierbei die Anonymität gegenüber Dritten, es werden keine Angaben oder Anforderungen bezüglich der Unbeobachtbarkeit etc. gemacht, während bei SEMPER auch Anonymität gegenüber Dritten vorgesehen ist. Dies könnte man mit anonymen Briefen vergleichen: Bei der GSS-API wird ein nicht mit Absender versehener Brief, der direkt an den Empfänger adressiert ist, einem Postboten übergeben, während bei SEMPER z.B. beim optimalen Einsatz von MIXen kein Dritter Informationen über Absender und Empfänger enthält.

Initialisierung
In der GSS-API gibt es keine Initialisierungsaufrufe, die vor der Benutzung von Funktionen der API aufgerufen werden müssen. Daher müssen die Implementierungen selbstinitialisierend sein.

Vergleich:
Im Gegensatz hierzu gibt es bei SEMPER für jeden Block Initialisierungsmethoden, die auch verwendet werden müssen.

6.4.3 Design

Die GSS-API-Aufrufe werden in vier Klassen unterteilt:

1. Referenzen-Management-Aufrufe (credential management calls)
   für das Einrichten und Verwalten von Referenzen durch den Benutzer,

2. Kontext-Ebenen-Aufrufe (context-level calls)
   für die Verwaltung der Sicherheitskontexte zwischen den Benutzern,

3. Benutzernachrichten-Aufrufe (peer-message calls)
   für den Schutz der individuellen Nachrichten innerhalb eines eingerichteten Sicherheitskontextes und

4. Support-Aufrufe (support calls)
   für Hilfsfunktionen der API-Aufrufe.

6.4.4 Kommunikation mittels der GSS-API

Etwas vereinfacht funktioniert die Kommunikation mit Hilfe der GSS-API folgendermaßen (Abbildung 6.8): Der Sender gibt die Nachricht an seinen Caller, dieser übermittelt seine Referenzen und die Nachricht an seine GSS-API. Die GSS-API gibt die Nachricht an den ausgewählten Sicherheitsmechanismus weiter. Dieser schützt die Nachricht entsprechend den Vorgaben und liefert das Token, d.h. die Nachricht geschützt durch die Sicherungsfunktion, an die GSS-API zurück. Die GSS-API leitet das Token an den Caller weiter, der es an den Caller des Empfängers übermittelt (üblicherweise über einen unsicheren Kanal). Auf Empfängerseite laufen jetzt die gleichen Aktionen wie auf der Senderseite in umgekehrter Reihenfolge ab: Der Caller

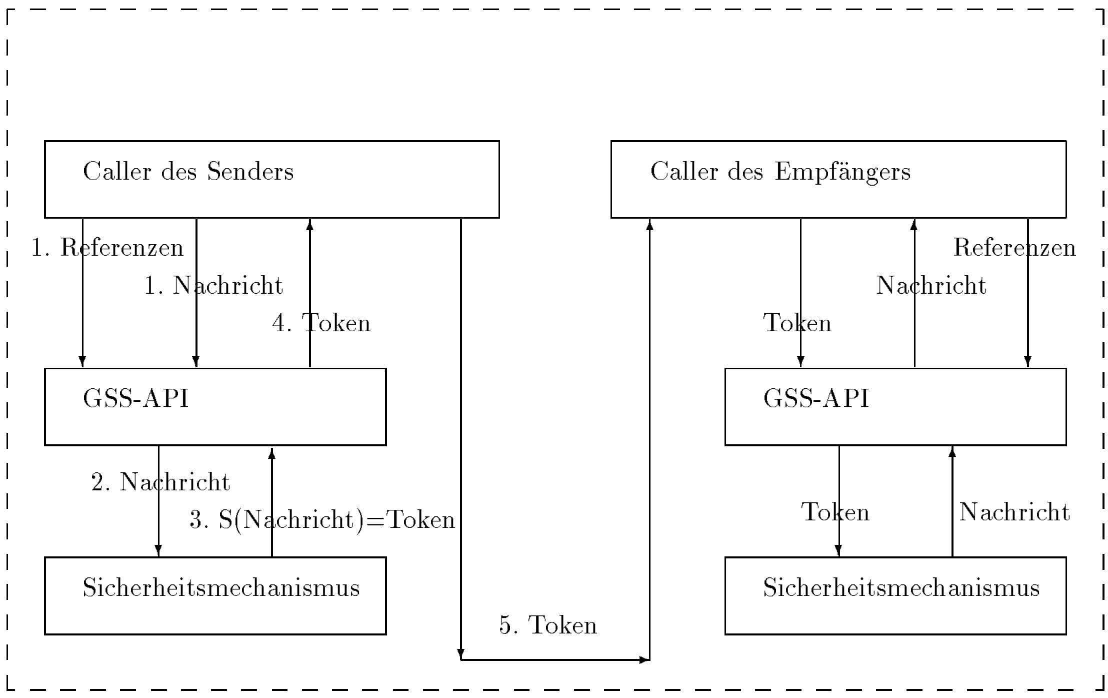

Abbildung 6.8: Kommunikation über die GSS API

leitet das Token an die GSS-API weiter, ebenso wie seine Referenzen. Die GSS-API übermittelt das Token an den entsprechenden Sicherheitsmechanismus und erhält die Nachricht von ihr zurück. Die GSS-API leitet sie an den Caller weiter, der sie dann an den Empfänger ausgibt. Die gesamte Kommunikation findet innerhalb des Sicherheitskontext statt (gestrichelter Kasten, siehe Bild), dessen Aufbau mit Hilfe der Referenzen hier als bereits durchgeführt angenommen wurde. Zu beachten ist, daß die GSS-API keinen Sicherheitsmanager vorschreibt, daher ist der Kasten „GSS-API" in Bild 6.8 nicht als Manager zu verstehen, sondern eher als eine Art Schnittstelle, über die der Aufrufer seiner Daten an die Mechanismen übermittelt und die Ausgaben der Mechanismen entgegennimmt. Mit den Referenzen werden die gewünschten Mechanismen ausgewählt.

6.4.5 Weitere Spezifikationen

Es existiert eine Beschreibung für das mechanismusunabhängige Token-Format und die Name Type Definitions für die Vergabe von Namen innerhalb der API. Außerdem gibt es noch Beispielszenarien für Kerberos V5 und das X.509 Authentication Framework.

6.4.6 Weitere vergleichende Bemerkungen

Vergleich:
Im Vergleich zu SEMPER, wo die kryptographischen Funktionen Teil des Frameworks sind, fehlen in der GSS-API sämtliche kryptographischen Funktionen, diese müssen von den unter der GSS-API liegenden Schicht zur Verfügung gestellt werden. Daraus ergibt

sich aber auch der Vorteil, das die GSS-API von den zur Verfügung stehenden Funktionen weitgehend unabhängig ist, d.h. sie kann bei der Implementierung an vorhandene Funktionen angepaßt werden, während bei SEMPER vorhandene Funktionen entweder direkt angepaßt oder über eine Zwischenschicht an die entsprechenden SEMPER-Schichten angekoppelt werden müssen. Der Unterschied liegt also hauptsächlich darin, was angepaßt werden muß: Bei SEMPER müssen die Funktionen angepaßt werden bzw. eine Zwischenschicht muß zwischen den Funktionen und den darüberliegenden Schichten vermitteln, bei der GSS-API werden bei der Implementierung die mechanismenspezifischen Schnittstellen der API an die Mechanismen angepaßt. Welche dieser Vorgehensweise vorteilhafter ist, oder ob beide gleichwertig sind, ist schwer zu beurteilen.
Im Vergleich zum SEMPER SecCom-Block fällt auf, das die GSS-API keinen Manager für die Funktionen vorschreibt. Zwar wird aus Vereinfachungsgründen ein solcher wahrscheinlich bei der Implementierung mit implementiert, es ist jedoch nicht Teil der GSS-API.
In der GSS-API gibt es keine Signaturen, während bei SEMPER Signaturen (im Statement-Manager) vorhanden sind.
Ungewöhnlich ist noch, daß trotz des eingerichteten Sicherheitskontextes bei jeder Nachricht einzeln angegeben wird, ob sie verschlüsselt werden soll oder nicht.
Ein Disput ist bei der GSS-API unmöglich, da im Zweifelsfall auch der Kontext nicht mehr vorhanden ist und ohne nachprüfbare Signatur keine Disputbehandlung erfolgen kann.

6.5 Generic Cryptographic Service API (GCS-API)

Die *Generic Cryptographic Service API* (GCS-API) wird von der Open Group (siehe Abschnitt 5.2) entwickelt. Sie dient dem Zugriff auf kryptographische Algorithmen sowohl durch Programme, die direkt Algorithmen benutzen als auch solche, die Algorithmen nur indirekt, z.B. bei der Benutzung von Protokollen, benutzen [Adam_96].
Die Forderungen an die API werden von der Open Group in funktionale und nichtfunktionale Forderungen unterschieden. [Adam_96] nennt für die funktionalen Forderungen zum einen die sogenannten *General Application Cryptographic Services*,

- Datenver- und entschlüsselung,
- Checksummenberechnung und -überprüfung zur Integritätsprüfung,
- Berechnung von Einweg-Hashfunktionen,
- Generierung von Zufallszahlen,

zum anderen zusätzliche Funktionen für das Schlüsselmanagement:

- zur Generierung, Ableitung (Derivation) und Löschung von Schlüsseln sowie
- den Im- und Export von Schlüsseln.

Die nichtfunktionalen Forderungen sind (ebenfalls nach [Adam_96]) die folgenden Anforderungen, die dafür sorgen, daß die API generisch ist:

- Die API soll unabhängig von kryptographischen Algorithmen sein.
- Die API soll unabhängig von Anwendungen sein.

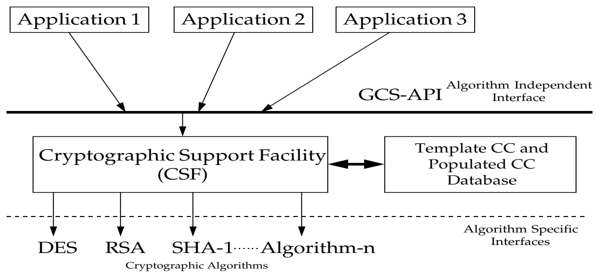

Abbildung 6.9: Basismodell der CSF (aus [XOpe2_96])

- Die API soll von kryptographischen Subsystemen unabhängig sein (womit gemeint ist, daß sie unabhängig davon ist, ob es eine Hard- oder Softwareimplementierung ist).
- Die API soll nicht voraussetzen, daß die Zugangskontrolle für kryptographische Dienste ganz oder teilweise im Betriebssystemkern angeordnet ist.
- Die API soll zukünftige Erweiterungen nicht erschweren.

Die Funktionen der GCS-API werden mit Beispielen in der Programmiersprache C erläutert, in der Spezifikation [XOpe2_96] wird aber keine bestimmte Implementierungssprache vorgeschrieben. In [XOpe2_96, Kapitel 4], Basic CSF Application Programming Interface (API), und in [XOpe2_96, Kapitel 10], Advanced CSF Application Programming Interface (API), werden die Funktionen detailliert beschrieben, wobei nach folgendem Muster vorgegangen wird: Name, Synopsis (Kopf der Funktion mit den Parametern), Beschreibung, Rückgabewerte, Fehlermeldungen.
Die Spezifikation der GCS-API, [XOpe2_96], ist in zwei Teile gegliedert: Der erste Teil, die *Basic section*, enthält einen einfachen Überblick über die Typen kryptographischer Funktionen, ein vereinfachtes Modell der GCS-API-Architektur und die minimale Menge an generischer Kryptographiefunktionalität, die für die Unterstützung der Anforderungen allgemeiner Applikationen an kryptographische Funktionen nötig ist. Der zweite Teil, die *Advanced section*, liefert eine detailliertere Beschreibung der Konzepte und Datenstrukturen sowie zusätzliche Funktionen für Applikationen mit höheren Ansprüchen an die API, wie z.B. für das Management von kryptographischen Politiken sowie die Unterstützung langfristiger Schlüsselverwaltung.

6.5.1 Das GCS-API Programmiermodell

Die GCS-API ist eine Schnittstelle zu einer sogenannten *Cryptographic Support Facility* (CSF), die abhängig von der Implementierung eine Anzahl verschiedener kryptographischer Algorithmen unterstützt. Sie bietet ebenso Unterstützung für das Schlüsselmanagement durch individuelle Applikationen und gemeinsames Schlüsselmanagement mehrere Applikationen. Das Basismodell der CSF ist in Abbildung 6.9 zu sehen.

Das durch die GCS-API gebildete Interface unterstützt die Entwicklung portabler Applikationen, indem sie unabhängig von Algorithmen und Implementationen ist. Die API ist unabhängig von den verwendeten Algorithmen, da sie das Konzept der sogenannten *kryptographische Kontexte* (Cryptographic Context, CC) benutzt. Ein kryptographischer Kontext ist ein geschütztes Objekt, welches für die Aufrufer der GCS-API undurchsichtig ist und alle Informationen einschließt, die für den Kontext der durchzuführenden kryptographischen Operation notwendig sind. Ein CC beinhaltet die Identität des Algorithmus, algorithmenspezifische Parameter, schlüsselspezifische Parameter und optional einen Schlüssel. Der genaue Aufbau des Inhalts eines CC wird in der Advanced section beschrieben, Benutzer der Basic-API benötigen diese Informationen nicht. Die kryptographischen Kontexte werden in einer Datenbank, der CC-Datenbank, gespeichert.
Vergleich:
Der kryptographische Kontext der GCS-API entspricht von der Funktion her dem Kontext in SEMPER, während es bei der GSS-API etwas mit den Referenzen vergleichbar ist, die aber etwas weiter gehen als die GCS-Kontexte. Nicht zu vergleichen sind sie mit den Kontexten der GSS-API, auch wenn sie den gleichen Namen haben.
Eine Cryptographic Support Facility besitzt eine Datenbank mit CCs, die von Aufrufern über Namen ausgewählt werden können. Dabei werden die CCs in zwei Klassen eingeteilt, einmal die, in denen ein Schlüssel abgespeichert ist und einmal die, in denen kein Schlüssel gespeichert ist.
Die CCs, die keinen Schlüssel enthalten, werden als *Template CCs* bezeichnet. Sie können nicht direkt für kryptographische Operationen verwendet werden, sondern dienen als Template für die Algorithmen, die von der jeweiligen CSF unterstützt werden und konfigurieren die kryptographische Systeme entsprechend der lokalen Sicherheitspolitik.
Die CCs, welche einen Schlüssel enthalten, werden als *Populated CCs* bezeichnet. Sie können direkt in kryptographischen Operationen verwendet werden. Bei Implementationen für Multi-User-Umgebungen ist für die Populated CCs eine Zugangskontrolle erforderlich.
Ein CC wird von einer Schlüsselverwaltung folgendermaßen verwendet:

- Entsprechend den zu benutzenden Funktionen wird ein entsprechendes Template CC bestimmt,
- danach wird die entsprechende Cryptographic Support Facility aufgerufen, um einen Schlüssel zu generieren,
- dann wird das entstandene Populated CC entweder direkt in Folgeaufrufen für kryptographische Operationen benutzt oder
- für die Benutzung durch andere Aufrufe unter einem entsprechenden Namen abgespeichert.

Vergleich:
Eine Schlüsselverwaltung ist in der GSS-API nicht vorgesehen, d.h. dort muß die Schlüsselverwaltung ohne Unterstützung der API erfolgen. Bei SEMPER erfolgt die Schlüsselverwaltung durch Funktionen der Cryptographic Services, Archive Services und Preference Services im Rahmen der Supporting Services.

6.5.2 Basic GCS-API Services

Die Dienste (Service) der CSF sind in die folgenden vier Kategorien eingeteilt:

- Generelle kryptographische Funktionen (Teil der API)
- Geschützte Funktionen zur Schlüsselverwaltung (ebenfalls Teil der API)

- Clear Key Schlüsselverwaltung (Teil des System Programming Interface (SPI), siehe Seite 86ff)

  Ein Clear Key ist dabei ein Schlüssel, der weder in einem kryptographischen Kontext verborgen noch durch einen anderen Schlüssel (also durch Verschlüsselung) geschützt ist. (Dies steht nirgends direkt in der Spezifikation, sondern ergibt sich aus den Funktionen des SPI und der sonstigen Verwendung des Begriffes „Clear Key“ in der Spezifikation.)

- Initialisierungs- und Konfigurationsfunktionen (zur Zeit noch nicht in der Spezifikation enthalten)

Für die Einteilung der Aufrufer siehe Seite 84.
Die Basic-Services befassen sich mit den generellen kryptographischen Funktionen und einem Teil der geschützten Schlüsselverwaltung. Entsprechend befassen sich die Advanced-Services mit den restlichen Funktionen zur Schlüsselverwaltung.
Im folgenden werden die in Blöcke aufgeteilten Funktionen der Basic GCS-API zusammen mit einer kurzen Erklärung aufgeführt.

6.5.2.1 Session-Verwaltung

Die Verwaltungsfunktionen bestehen aus je einer Funktion zur Initialisierung und Terminierung einer Sitzung. Sie dienen zum Aufbauen bzw. Beenden einer Verbindung zur CSF und bewirken unter anderem eine Authentikation des Aufrufenden und die Einrichtung eines Sicherheitskontextes zwischen Aufrufer und CSF für die Sitzung.
Der Sicherheitskontext wird durch ein geschütztes, undurchsichtiges Objekt dargestellt, auf das? ein Handle an den die Sitzung initialisierenden Aufrufer zurückgegeben wird. Dieser session_context wird als Parameter an jeden Aufruf der GCS-API weitergegeben und dient als Methode zur ständigen Authentikation sowie um eine zustandslose Implementierung der CSF zu ermöglichen. Der Sicherheitskontext enthält alle notwendigen Informationen zur Authentikation und Autorisation.
Vergleich:
Das Session-Management wird in der GSS-API nicht durch die API, sondern durch den Aufrufer geleistet, unterstützt durch das Referenzen-Management. In SEMPER wird es durch die Business Application durchgeführt.
Eine Initialisierung ist in der GSS-API nicht vorgesehen, in SEMPER erfolgt sie in jedem Block für diesen Block einzeln.

6.5.2.2 Kryptographischer Kontext (CC)

Es existieren Funktionen zum Löschen, Auflisten und Abfragen eines Kryptographischen Kontext aus der CC-Datenbank, in der die Kryptographischen Kontexte gespeichert werden. Das Erzeugen eines Kryptographischen Kontexts ist nur mit den Advanced Services möglich, siehe Abschnitt 6.5.3.4.1 auf Seite 90.
Um die Verwendung der kryptographischen Schlüssel und aller damit verbundenen Informationen zu vereinfachen, werden diese in einer *Kryptographischer Kontext* (Cryptographic Context, CC) genannten, geschützten Struktur gespeichert, siehe oben, Seite 79.
Abbildung 6.10 und 6.11 zeigen das Abfragen und die Benutzung eines Kryptographischen Kontextes, einmal für den Fall des Populated CC 6.10 und einmal für einen Template CC 6.11.
Vergleich:
Für den CC siehe oben, Seite 79. Die Funktionen für die Verwaltung sind für die hierzu analogen Kontexte in SEMPER ebenso vorhanden. In der GSS-API stehen eben-

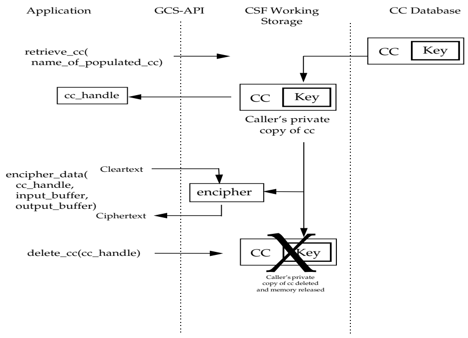

Abbildung 6.10: Auslesen und Benutzen eines CC mit Schlüssel (aus [XOpe2_96])

falls Funktionen für die Verwaltung der mit den CCs vergleichbaren Referenzen zur Verfügung.

6.5.2.3 Schlüsselgenerierung

Bevor ein CC benutzt werden kann, muß er mit einem Schlüssel versehen werden. Dafür existieren zwei Funktionen, eine zum internen Generieren und eine zum Einfügen eines Schlüssels aus einer externen Eingabe.

6.5.2.4 CC-Speicherfunktionen

Diese Funktionen dienen der Speicherung und Löschung der Kryptographischen Kontexte unter Kontrolle der CSF.
Es gibt Funktionen zum Speichern eines CC sowie die Zuordnung eines vom Aufrufer vergebenen Namens für den gespeicherten CC, sowie für das entfernen der zuvor gespeicherten CCs. Die Funktionen und ihre Wirkungsweise sind in Abbildung 6.12 zu sehen.

6.5.2.5 Schlüsselaustausch-Funktionen

Diese Funktionen ermöglichen das Einkapseln eines Schlüssels in ein Objekt, welches durch einen *Key Exchange Key* (KEK) geschützt wird. Dieses Objekt ermöglicht den Austausch des Schlüssels mit einem anderen CSF oder es kann mit einem Objekt, welches mit diesem Schlüssel geschützt wurde, zum Zwecke der Übertragung oder Speicherung verbunden werden. Für den Aufruf einiger dieser Funktionen ist eine Autorisation notwendig. Der Export eines Schlüssels ist in Abbildung 6.13 zu sehen.

6.5.2.6 Hash- und Signaturfunktionen

Es stehen grundlegenden Funktionen zur Sicherstellung von Integrität und für Digitale Signaturen zur Verfügung, die in jeder CSF-Implementierung vorhanden sind. Es handelt sich um Funktionen zum Generieren und Verifizieren kryptographisch geschützter Hashwerte.
Es handelt sich im einzelnen um Funktionen, die einen kryptographisch geschützten Hashwert erzeugen, der z.B. als digitale Signatur verwendet werden kann. Eine

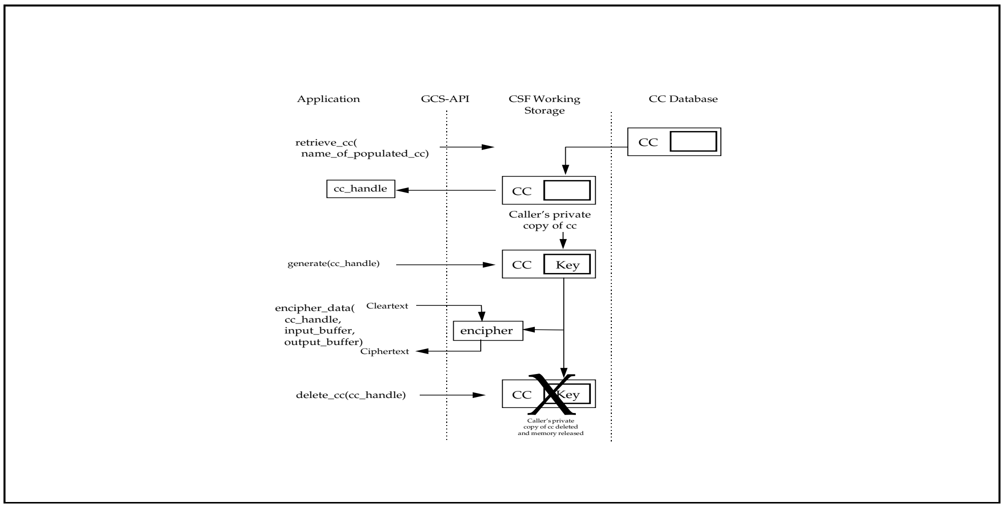

Abbildung 6.11: Auslesen und Benutzen eines Template-CC (aus [XOpe2_96])

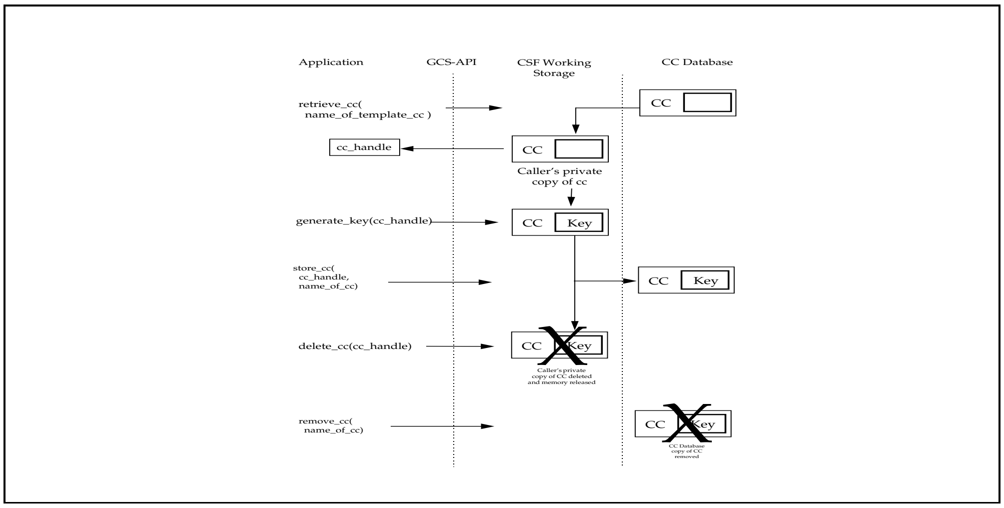

Abbildung 6.12: CC-Speicherverwaltungsfunktionen (aus [XOpe2_96])

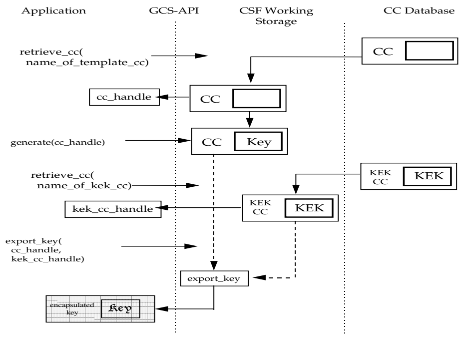

Abbildung 6.13: Schlüsselexport (aus [XOpe2_96])

weitere Funktion erzeugt einen Hashwert aus den Eingabedaten und es existiert eine Funktion für das Erzeugen kryptographisch starker Zufallszahlen [XOpe2_96].

Vergleich:

Die Funktionen des Typs „checkvalue" sind Funktionen für digitale Signaturen, für die Funktion zum Erzeugen eines Hashwertes wird kein Verwendungszweck angegeben - aufgrund der Konstruktion kann man das Ergebnis wahrscheinlich als MAC (Message Authentication Code), d.h. zur Integritätsprüfung, verwenden. Für die Verwendung des Zufallszahlengenerators werden ebenfalls keine Aussagen gemacht, hierzu ist aber festzustellen, daß es sich eigentlich nur um einen Generator von Pseudozufallszahlen handeln kann.

6.5.2.7 Datenverschlüsselung

Die Funktionen zur Datenverschlüsselung müssen nicht von allen CSF-Implementierungen unterstützt werden, oder es kann operationale Einschränkungen geben. Außerdem kann es Beschränkungen für den Zugriff auf die Funktionen geben, d.h. der Aufrufer muß speziell für den Zugriff autorisiert sein:

Es stehen außerdem Funktionen für die einfache Ver- und Entschlüsselung einer Datenmenge (d.h. genauer: eines Bytestrings) zur Verfügung, sowie eine Funktion für die gleichzeitige Verschlüsselung und Generierung eines Hashwertes bzw. einer digitalen Signatur über die gleichen Daten, wodurch gleichzeitig sowohl Vertraulichkeit und Integrität und evtl. Authentikation der Daten erfolgt. Ebenso steht eine entsprechende Test- und Entschlüsselungsfunktion zur Verfügung.

Bei gleichzeitiger Verschlüsselung und Integritätssicherung werden die verschlüsselten Eingabedaten und ein Checkwert für diese Eingabedaten ausgegeben [XOpe2_96, Kapitel 4, Abschnitt gcs_protect_data].

6.5.2.8 Hilfsfunktionen

Es existiert eine Hilfsfunktion zum Abfragen implementationsspezifischer Parameter, wie z.B. die maximale Größe eines Puffers und der Typ der Implementation (d.h. Hardware, Software etc.) sowie eine Funktion zum Freigeben aller durch einen Aufrufer veranlaßten Pufferbelegungen.

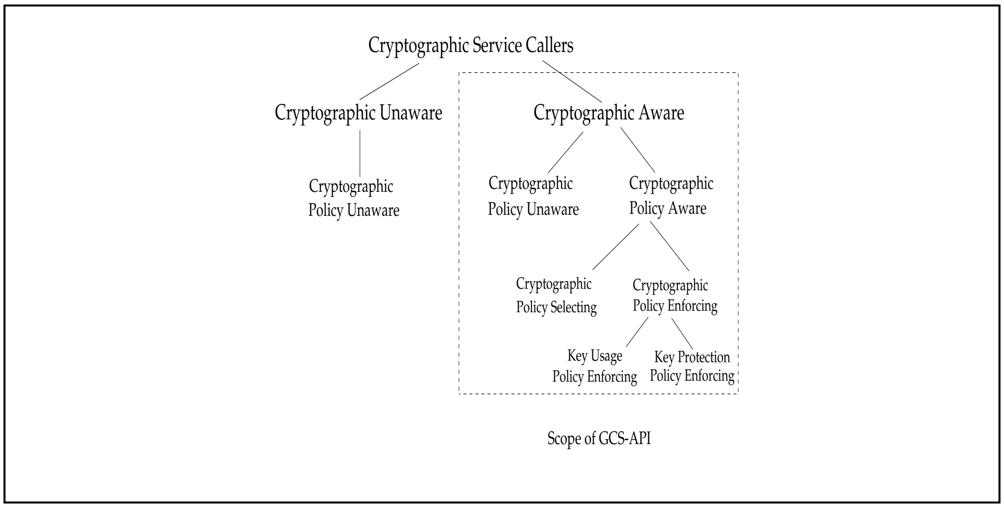

Abbildung 6.14: Typen der Aufrufer der kryptographischen Dienste (aus [XOpe2_96])

6.5.2.9 Weitere Spezifikationen

6.5.2.9.1 Parameter

In [XOpe2_96, Kapitel 3], Basic Parameter Passing Conventions, werden die von der C-Version der GCS-API verwendeten Datentypen und ihre Verwendung beschrieben. Dies umfaßt herkömmliche Datentypen wie Integer und Strings für Bits, Bytes und Charakters, die bereits oben erwähnten undurchsichtigen Datentypen (Opaque Data Types), einen Datentyp für Kontexte, Statuswerte (inklusive einer Liste von Fehlermeldungen mit Erklärung ihrer Bedeutung) sowie eine Auflistung der Konstanten.

Vergleich:

Auch in SEMPER werden Parameter und Variablen beschrieben, jedoch nicht zentral an einer Stelle innerhalb der Spezifikation, sondern für jeden Block getrennt in der Spezifikation des Blocks. Für die GSS-API existiert eine derartige Beschreibung innerhalb der Spezifikation.

6.5.3 Advanced Services der GCS-API

In [XOpe2_96, Kapitel 5], Advanced GCS-API Introduction, werden die erweiterten Funktionen der GCS-API beschrieben. Zuerst werden die potentiellen Aufrufer kryptographischer Dienste entsprechend ihrem Bewußtsein für die kryptographischen Dienste und Verantwortungen für die Sicherheitspolitik klassifiziert (siehe Abb. 6.14):

- Aufrufer werden als *Cryptographic Unaware Caller* bezeichnet, wenn sie die kryptographischen Dienste benutzen, ohne sich ihrer genauen Wirkungsweise bewußt zu sein (d.h. einem derartigen Benutzer ist es nicht bekannt, ob es sich um ein symmetrisches oder asymmetrisches System handelt, wie die geforderte Sicherheit erreicht wird etc.).

- Entsprechend werden Benutzer, die sich der zugrundeliegenden Techniken bewußt sind, als *Cryptographic Aware Caller* bezeichnet.

- Benutzt ein solcher Benutzer lediglich vorgegebene Kontexte, d.h. ist er zwar für die Benutzung der kryptographischen Systeme im Rahmen eines vorher de-

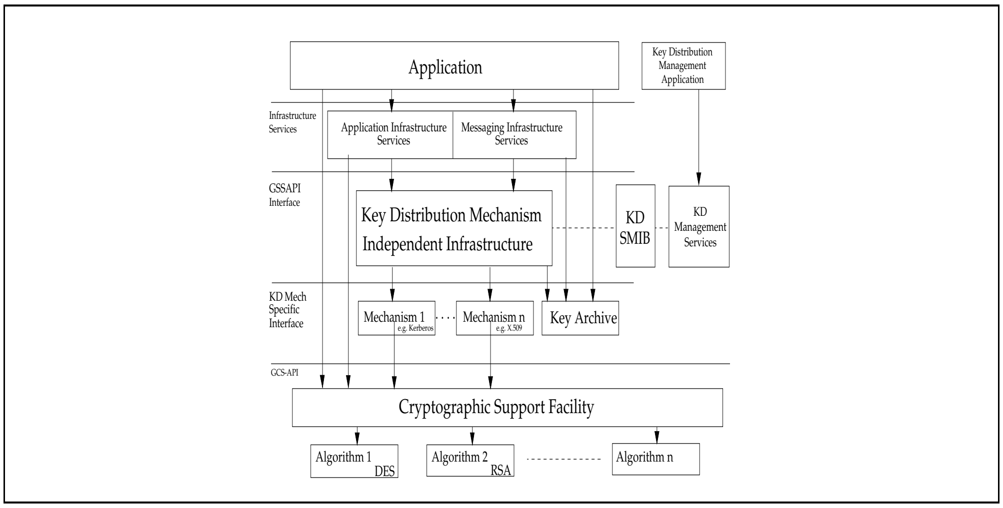

Abbildung 6.15: Schichten der kryptographischen Dienste (aus [XOpe2_96])

finierten Kontextes, nicht aber für die Bildung eines kryptographischen Kontextes verantwortlich, so wird er als *Cryptographic Policy Unaware* bezeichnet.

- Ein Benutzer, der auch für die Einrichtung eines Kryptographischen Kontextes verantwortlich ist, wird als *Cryptographic Policy Aware* bezeichnet.
  - Derartige Benutzer werden noch in *Cryptographic Policy Selecting Caller*, die aus einer Menge vorgegebener Kontexte einen geeigneten auswählen, und in
  - *Cryptographic Policy Enforcing Caller*, die für eine Sicherheitspolitik und damit die Konstruktion der Kryptographischen Kontexte verantwortlich sind, unterschieden.

In Abbildung 6.16 auf Seite 86 werden die verschiedenen Benutzer im Zusammenhang mit den von ihnen gemachten Aufrufen an die kryptographischen Dienste der CSF gezeigt.

Vergleich:

Eine derartige Einteilung gibt es weder in SEMPER noch in der GSS-API. Über ihren Sinn kann man streiten: Einerseits kann in der GCS-API durch diese Einteilung die Verwendung bestimmter Funktionen den dafür kompetenten Benutzern vorbehalten werden, wodurch Fehlbedienungen durch Unwissenheit vermieden werden, andererseits kann eben durch diese Einschränkung die Sicherheit auch eingeschränkt werden, wenn die Verwendung eigentlich gebotener Funktionen nicht möglich ist.

Abbildung 6.15 zeigt die Schichten der kryptographischen Dienste: Auf der obersten Schicht befinden sich die Applikationen, die Datenschutzmaßnahmen über die in der darunterliegenden Schicht angesiedelten Infrastruktur-Dienste in Anspruch nehmen. Sie sind generell Cryptographic Unaware. In der darunter liegenden Schicht befinden sich die Infrastruktur-Dienste, die für die Behandlung des Kontexts einer Operation unabhängig von mechanismenspezifischen Aspekten zuständig sind. Diese Funktionalität wird von Interfaces auf Basis der GSS-API (siehe Abschnitt 6.4 auf Seite 71) geleistet. Die tiefer liegenden Schichten sind für Details der kryptographischen Funktionen zuständig, wie z.B. den Aufbau eines Kryptographischen Kontexts. Dabei werden sowohl mechanismenunabhängige Funktionen wie Schlüsselverteilungen als auch mechanismenspezifische Funktionen wie spezielle Algorithmen verwendet.

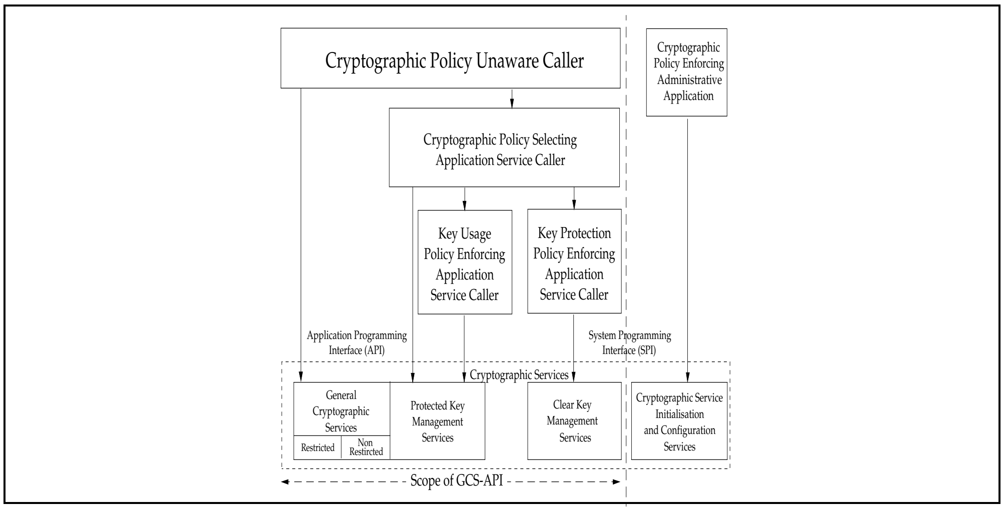

Abbildung 6.16: CSF-Aufrufer und -Dienste (aus [XOpe2_96])

Dabei wird die unterste Schicht im Rahmen dieser Spezifikation von der *Cryptographic Support Facility* (CSF) abgedeckt, die in [XOpe2_96, Kapitel 5] beschrieben wird und der im folgenden ein eigener Abschnitt gewidmet ist.
Vergleich:
Hier wird verdeutlicht, daß die GCS-API als ein Teil der unter der GSS-API liegenden, von dieser verwendeten Sicherheitsmechanismen verwendet werden kann (aber nicht muß - genauso kann eine beliebige andere Applikation die GCS-API direkt benutzen).

6.5.3.1 Cryptographic Support Facility (CSF)

Eine *Cryptographic Support Facility* (CSF) stellt eine Anzahl allgemeiner kryptographischer und Schlüsselverwaltungsinterfaces, die auf verschiedenen Algorithmen und Implementierungen dieser Algorithmen aufsetzen, zur Verfügung, siehe Abschnitt 6.5.2.
Die CSF der Advanced-Services unterstützt zusätzlich zu denen der Basic-Services Applikationen und Applikations-Infrastrukturen, die

- für eine gegebene Operation die Qualität des Schutzes angeben kann, aber nicht muß,

- für eine gegebene Operation den zu verwendenden Algorithmus angeben kann, aber nicht muß.

Wie in Abbildung 6.16 zu sehen ist, besitzt die CSF zwei Programmier-Interfaces, ein *Application Programming Interface* (API) und ein *System Programming Interface* (SPI). Das Application Programming Interface bildet das Interface zu den allgemeinen Kryptographischen Funktionen und den geschützten Schlüsselverwaltungsfunktionen, während das System Programming Interface für den Zugang zum sogenannten Clear Key Management zuständig ist.
Vergleich:
Die CSF entspricht in SEMPER den Supporting Services, insbesondere den Cryptographic Services. In der GSS-API gibt es nichts entsprechendes, dort wird dieser Teil durch die unterhalb der API liegenden Schichten geleistet, z.B. auch von den CSF der GCS-API, s.o..

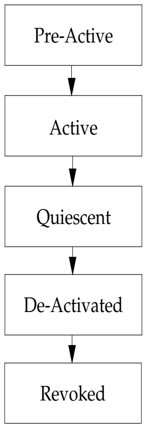

Abbildung 6.17: Übergänge im Schlüssellebenszyklus (aus [XOpe2_96])

6.5.3.1.1 Autorisationspolitik

Die in der GCS-API verwendete Autorisationspolitik ergibt sich aus den notwendigen Autorisationen, um die Funktionen der GCS-API aufzurufen bzw. auf spezifische Schlüssel zuzugreifen und sie zu benutzen.
Die Aufrufer der GCS-API sind autorisiert, auf jeden Schlüssel zuzugreifen, die der Benutzer des Aufrufers gebildet hat oder für die der Benutzer eine Zugriffsberechtigung besitzt. (Man beachte hier den Unterschied zwischen dem Benutzer, d.h. Menschen, und den von ihm gestarteten Programm(en) als Aufrufer der API.) Die dafür notwendige Sicherheitspolitik ist nicht Teil der Spezifikation der GCS-API. Es stehen jedoch Funktionen für die Initialisierung einer Sitzung zwischen Aufrufer und CSF und der damit verbundenen Authentikation der Identität des Aufrufers und seines Benutzers sowie der notwendigen Zugriffskontrolle zur Verfügung.
Die Funktionen, die ein Aufrufer auf Schlüssel anwenden kann, werden aufgrund einer Autorisationspolitik durchgeführt, die von einer Menge von Capabilities, die dem Aufrufer zugeordnet ist, abhängt. Diese Capabilities sind direkt dem Aufrufer zugeordnet, nicht dem Benutzer. Es werden dafür in [XOpe2_96] drei Capabilities definiert. Diese Capabilities beschränken nur den Zugriff auf die Schlüssel - alle Aufrufer dürfen die allgemeinen Kryptographischen Funktionen benutzen.
Vergleich:
Eine Zugriffskontrolle, um etwas derartiges handelt es sich hier letztendlich, wird in SEMPER durch den Access Control Service realisiert. In der GSS-API ist dafür nichts vorgesehen, d.h. es ist Aufgabe der die GSS-API benutzenden Applikationen.

6.5.3.2 Schlüssellebenszeit

Da ein Schlüssel immer gefährdeter wird, je länger er benutzt wird, ist es notwendig, den Schlüssel vor Kompromittierung zu schützen, indem er regelmäßig ersetzt wird. Daher wird ein Schlüssel betrachtet, als habe er einen Lebenszyklus: Er wird gebildet, benutzt und dann von der Benutzung zurückgezogen, bevor er effektiv gefährdet werden kann. Dafür werden eine Reihe von Zuständen im Lebenszyklus des Schlüssels definiert, siehe Abbildung 6.17.
Ein Schlüssel kann in mehreren Formaten existieren, z.B. kann ein Schlüssel, der benutzt wird, in einem anderen Format gespeichert sein als einer, der zurückgezogen wurde (siehe Abschnitt 6.5.3.2.2).

6.5.3.2.1 Schlüsselstatus

Die Basis des kryptographischen Schutzes ist die Benutzung eines *Schlüssels* als Eingabeparameter für einen kryptographischen Algorithmus, um die damit durchgeführte Aktion zu kontrollieren. Der damit erreichbare Schutz ist abhängig vom Schutz des Schlüssels. Daher wird für die Verwendung eines Schlüssels eine Art von Lebenszyklus zu Grunde gelegt, die in Abbildung 6.17 zu sehen ist.
Es gibt die folgenden Stufen:

- *Pre-Active*,
  für Schlüssel, die noch nicht verwendet werden,
- *Active*,
  für sich zur Zeit in Verwendung befindende Schlüssel,
- *Quiescent* (Ruhend),
  für Schlüssel, die nur eingeschränkt verwendet werden, z.B. zur Entschlüsselung, nicht aber zur Verschlüsselung,
- *De-Activated*,
  für Schlüssel, die nicht mehr für kryptographische Funktionen verwendet werden, sowie
- *Revoked* (Zurückgezogen),
  wenn bekannt ist bzw. vermutet wird, daß ein Schlüssel kompromittiert ist und er deshalb nicht mehr benutzt werden kann.

Die Basisfunktionen zum Ändern des Status eines Schlüssels sind

- **Advance Key State**,
  um den Schlüsselstatus eine Stufe höher zu setzen,
- **Revoke Key**,
  um einen Schlüssel zurückzuziehen sowie
- **Set Key Validity**
  für Security Aware Aufrufer, um einen Status entgegen der normalen Richtung in Lebenszyklus zu ändern, z.B. um den Status eines Schlüssels von Revoked oder De-Activated auf Quiescent zu setzen um eine historische Checksumme zu überprüfen.

Anschließend werden in [XOpe2_96, Abschnitt 6.1.3f] noch die Wechsel des Schlüsselstatus beschrieben.

6.5.3.2.2 Schlüsselformate

In der Spezifikation [XOpe2_96] werden drei mögliche Schlüsselformate beschrieben:

- das *Operational Format*
  für Schlüssel, die in kryptographischen Funktionen benutzt werden können und die sowohl direkt in der CSF als auch extern (dann geschützt durch eine Verschlüsselung mit dem Master Key der CSF) gespeichert werden können. Das Operational Format ist implementierungsabhängig.
- das *Exchange Format*
  für den Austausch von Schlüsseln zwischen verschiedenen CSFs (dafür werden die Schlüssel mit einem sogenannten Key-Encryption-Key (KEK) geschützt, siehe oben). Dieses Format ist vom Schlüsselverteilprotokoll abhängig, die Definition eines solchen Protokolls ist nicht Teil der Spezifikation der GCS-API.

- das *Archive Format*
  für die langfristige Speicherung eines Schlüssels unter der Kontrolle der CSF. Diese Schlüssel werden ebenfalls durch einen (Archiv-)KEK geschützt.

  Hier scheint sich ein Fehler in der Spezifikation [XOpe2_96, Abschnitt 6.3, S. 90] zu befinden: Laut Glossar gibt es auch einen KAK, Key-Archive-Key, der sicher hier verwendet werden sollte. Leider gibt es im Index keinen Verweis auf KEK und KAK außer denen in das Glossar.

Für die Arbeit mit den Schlüsseln in den verschiedenen Formaten stehen folgende Funktionen zur Verfügung:

- **Create**
  zur Generierung eines Schlüssels im Operational Format, dessen Status pre-active oder active ist,

- **Export**,
  um eine Kopie eines operationalen Schlüssels im Exchange Format zu erhalten, der dann für einen Schlüsselaustausch verwendet werden kann,

- **Import**,
  um einen Schlüssel vom Exchange Format ins Operational Format zu kopieren,

- **Archive**,
  um einen Operationalen Schlüssel zur langfristigen Speicherung in das Archive Format zu kopieren, sowie

- **Restore**,
  um einen im Archive Format gespeicherten Schlüssel in das Operational Format zu kopieren.

Beachtenswert ist dabei, das immer eine Kopie erstellt wird, d.h. es existieren nach dem Durchführen einer derartigen Operation zwei (oder mehr) Exemplare eines Schlüssels, jeweils in einem anderen Format.
Vergleich:
Über Schlüssellebenszeiten und -formate werden in der GSS-API Angaben gemacht, d.h. dort ist der Aufrufer selber dafür verantwortlich, und es stehen ihm auch keine unterstützenden Funktionen durch die API zur Verfügung.
In SEMPER ist der Crypto-Block für die Spezifikation der Schlüssel zuständig, dort gibt es einen kurzlebigen Session-Key, der jeweils nur für die Dauer einer Sitzung gültig ist und nach Beendigung der Sitzung verworfen wird, und die Schlüssel für kryptographische Operationen, die mit Hilfe des Archiv-Blocks gespeichert werden [ZaEh_96]. Zur Lebensdauer dieser Schlüssel wird keine Aussage gemacht.

6.5.3.3 Datenformate

In [XOpe2_96, Kapitel 7] werden die Datenformate der GCS-API beschrieben. Es handelt sich dabei um

- den Kryptographischen Kontext (Cryptographic Context), Abb. 6.18

- den Header des Kryptographischen Kontext (Cryptographic Context Header), Abb. 6.19

- den Algorithmen Kontext innerhalb des CC (Algorithm_Context), Abb. 6.20

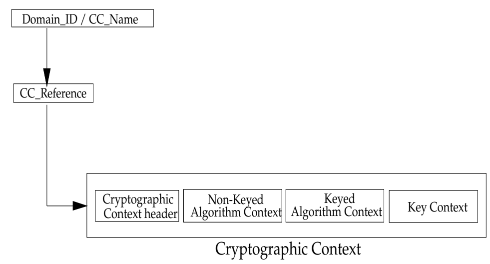

Abbildung 6.18: Struktur des CC (aus [XOpe2_96])

- den Schlüssel Kontext innerhalb des CC (Key_Context), Abb. 6.21
- Referenzen auf den CC
- CC Namen

Vergleich:
Datenformate werden sowohl in SEMPER (dort dezentral für jeden Block einzeln in dessen Spezifikation) als auch in der GSS-API beschrieben.
Ein kryptographischer Kontext ist für den Aufrufer undurchsichtig, d.h. er kennt den Inhalt der Datenstruktur nicht (auch wenn er ihren Aufbau kennen kann). Bei der GSS-API ist der Inhalt der mit den CCs vergleichbaren Referenzen für den Benutzer sichtbar. Für SEMPER fehlen die für einen Vergleich notwendigen Informationen.
Auffallend ist hier, daß die GCS-API keine Zertifikate oder damit vergleichbare Strukturen kennt.

6.5.3.4 Advanced GCS-API Services

In [XOpe2_96, Kapitel 8], Advanced GCS-API Services, werden analog zu [XOpe2_96, Kapitel 4] die Funktionen der Advanced GCS-API beschrieben. Analog zum Abschnitt 6.5.2 folgt nun eine kurze Beschreibung dieser Funktionen.

6.5.3.4.1 Bildung eines CC

Ein Kryptographischer Kontext (CC) darf nur von autorisierten Aufrufern gebildet werden. Derartige Aufrufer werden durch die Zuordnung einer Capability gekennzeichnet. Sie können einen CC erstellen und seine Komponenten Algorithm_Context und Key_Context bearbeiten.
Vergleich:
Hiermit wird die Basic GCS-API um für die Arbeit mit CCs notwendige Funktionen erweitert. Derartige Funktionen stehen auch in SEMPER und der GSS-API für die zu den CCs analogen Kontexte (SEMPER) bzw. Referenzen (GSS) zur Verfügung. Diese Aussage gilt auch für die Funktionen des folgenden Unterabschnitts.

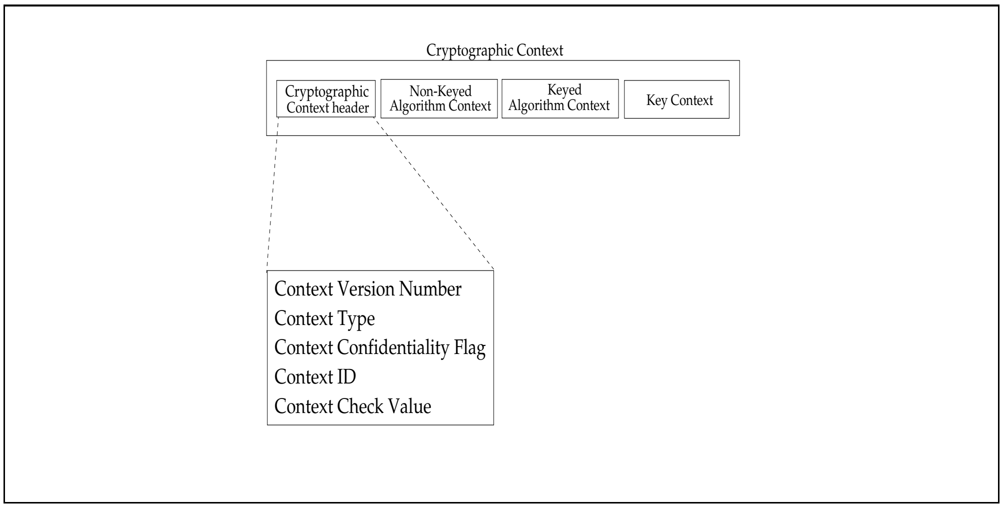

Abbildung 6.19: CC-Header (aus [XOpe2_96])

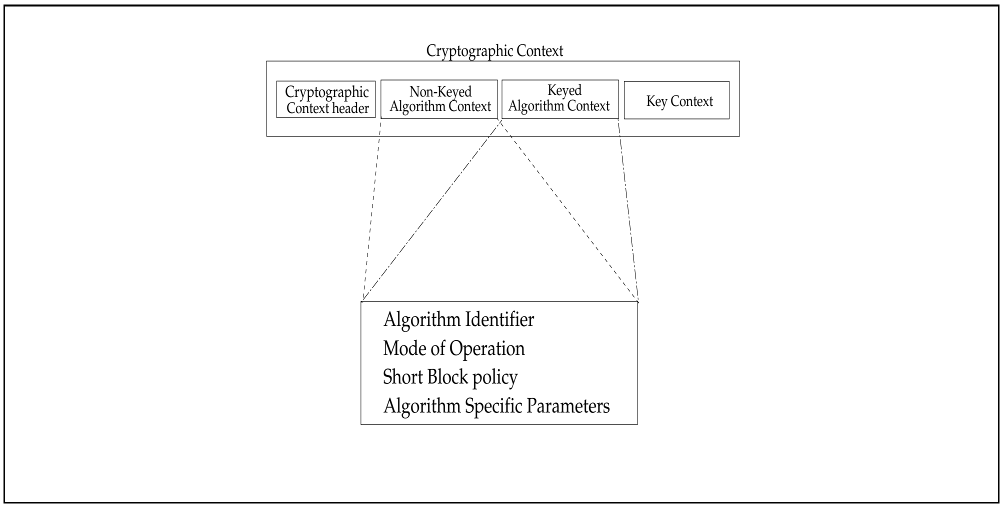

Abbildung 6.20: Algorithm_Context (aus [XOpe2_96])

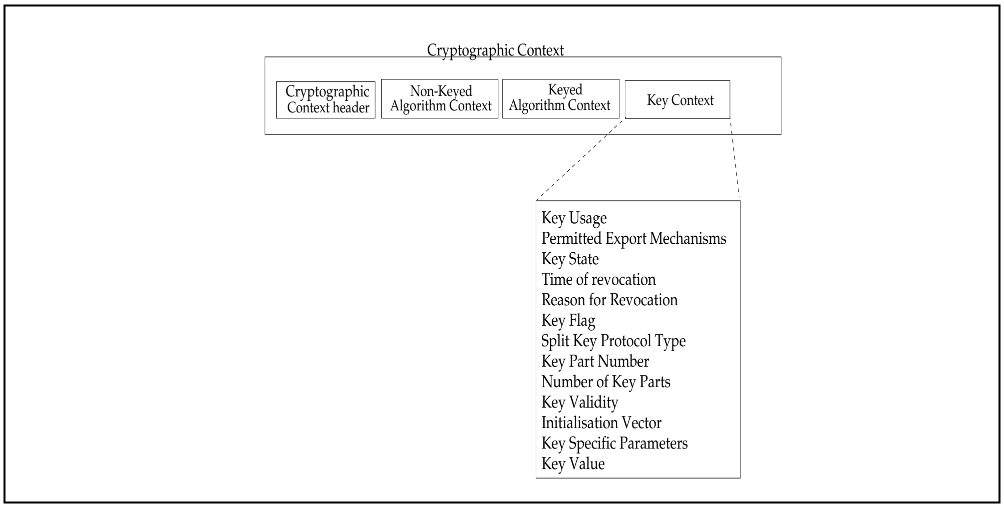

Abbildung 6.21: Key_Context (aus [XOpe2_96])

6.5.3.4.2 Modifikation eines CC

Es stehen Funktionen zur Verfügung, um den Inhalt eines CC zu lesen und zu schreiben sowie einen CC für Modifikationen vorzubereiten

6.5.3.4.3 Weitere Funktionen zur Schlüsselverwaltung

Es steht eine Funktion zur Verfügung, um Teile verschiedener Schlüssel, die in verschiedene CCs importiert wurden, zu einem einzigen zu kombinieren, sowie eine Funktion, um einen als Klartext empfangenen Public Key, der aufgrund seiner Verwendung nicht zur Erhaltung von Vertraulichkeit verschlüsselt werden muß, in einen CC zu laden. Außerdem existiert eine Funktion, um nicht speziell geschützte CCs zu kopieren, wobei die Kopie bis auf die ContextID identisch mit dem Original ist.

6.5.3.4.4 Verwaltung des Schlüsselstatus

Für die Verwaltung des Schlüsselstatus stehen Funktionen zur Verfügung, um den Status anzuheben, die Gültigkeit und Verwendbarkeit einzuschränken sowie einen Schlüssel zurückzuziehen.
Vergleich:
Da weder SEMPER noch die GSS-API einen Schlüsselstatus kennen, fehlen dort auch die entsprechenden Funktionen.

6.5.3.4.5 Weitere Funktionen zur Verwaltung des CC

Es stehen Funktionen zur langfristigen Speicherung der CCs zur Verfügung, sowie zur Überprüfung erhaltener Schlüssel.

6.5.3.4.6 System Programming Interface (SPI)

Das System Programming Interface (SPI) liefert Funktionen für die Manipulation von Clear Keys. Es gibt z.B. Funktionen, um einen Schlüssel aus einem CC in einem Clear Key umzuwandeln bzw. einen Clear Key direkt zu bilden, sowie einen Clear Key in einen CC einzufügen.
Für den Schutz der (ungeschützten) Clear Keys ist der Benutzer verantwortlich.

6.5.3.4.7 Parameter

In [XOpe2_96, Kapitel 9], Advanced GCS-API Parameter Passing Conventions, werden ergänzend zu [XOpe2_96, Kapitel 3] (siehe Abschnitt 6.5.2.9.1 auf Seite 84) weitere von der C-Version der GCS-API verwendeten Datentypen und ihre Verwendung beschrieben. Dabei handelt es sich um die Kontexte, Kryptographische Referenzen (dabei handelt es sich um C-Handles zu CCs) und weitere Konstanten.

6.5.3.4.8 Schlußbemerkungen in der Spezifikation

In [XOpe2_96, Kapitel 12], werden einige Anforderungen an verschiedene Implementierungsformen der API aufgeführt. In den Anhängen von [XOpe2_96] werden Hinweise zur Implementierung der CSF gegeben, einige Beispiele für Template CCs sowie Beispielanwendungen aufgeführt und einige Ausblicke auf zukünftige Erweiterungen gegeben. In weiteren Anhängen sind einige Beispiele für Tests zu finden sowie einige Bemerkungen über die Verwendung eines Paritätsbits in Schlüsseln. Die Spezifikation [XOpe2_96] wird danach mit einem Glossar abgeschlossen.
Vergleich:
Beispiele für die Implementierung bzw. Verwendung der API finden sich auch in der GSS-API. In SEMPER gibt es dafür die Referenzimplementierung.

6.5.4 Weitere vergleichende Bemerkungen

Vergleich:
Während bei der GSS-API keine kryptographischen Funktionen, d.h. Mechanismen vorhanden sind, sind sie hier Teil der Spezifikation. Wie schon oben geschrieben wurde, kann die GCS-API der GSS-API die notwendigen kryptographischen Mechanismen über ihre CSF zur Verfügung stellen.
In der GCS-API gibt es ebenso wie bei SEMPER Signaturen, die in der GSS-API fehlen. Spezielle Funktionen für die Behandlung eines Disputs fehlen hier ebenso wie bei der GSS-API, ein Disput ist hier im Gegensatz zur GSS-API jedoch (außerhalb der API) möglich, wenn ein Gericht denselben Public Key wie die sich im Disput befindenden Kommunikationspartner sowie die Signatur bekommt und das Ergebnis der Signaturfunktion mit der erhaltenen Signatur vergleichen kann. Da die API einen Disput nicht aktiv unterstützt, ist es den Benutzern überlassen, rechtlich verwertbare Beweise zu sammeln. Dies wird noch erschwert dadurch, daß die GCS-API auch keine Zertifikate kennt, mit denen die Echtheit eines Public Key bewiesen werden kann.
Gegenüber SEMPER und GSS gibt es bei der GCS-API das Konzept der Schlüssellebenszyklen und damit verbunden den Schlüsselstatus, wodurch eine Kompromittierung des Schlüssels oder zumindest die Verwendung eines bereits kompromittierten Schlüssels verhindert werden soll. Ob damit eine Kompromittierung verhindert werden kann, ist zu bezweifeln, zumindest gegen die Verwendung eines kompromittierten Schlüssels kann das Verfahren wirksam sein.
Ungünstig erscheint die Aufteilung in Basic- und Advanced-Services, da so in der Basic-Services API einige Funktionen vermißt werden, die erst in der Advanced-Services API quasi „nachgereicht“ werden - es wäre wahrscheinlich sinnvoller, alle Funktionen zusammen zu beschreiben und dabei diejenigen, die nur für qualifiziertere Benutzer zugänglich sind, zu kennzeichnen.

6.6 Common Object Request Broker Architecture (CORBA)

Die *Common Object Request Broker Architecture* (CORBA) wird von der Object Management Group (OMG) (siehe Abschnitt 5.4) entwickelt. Es handelt sich dabei um eine Architektur zur Konstruktion und Integration objektorientierter Client-Server-Applikationen in heterogenen Netzwerken. Ziel dabei ist es, die Verteilung

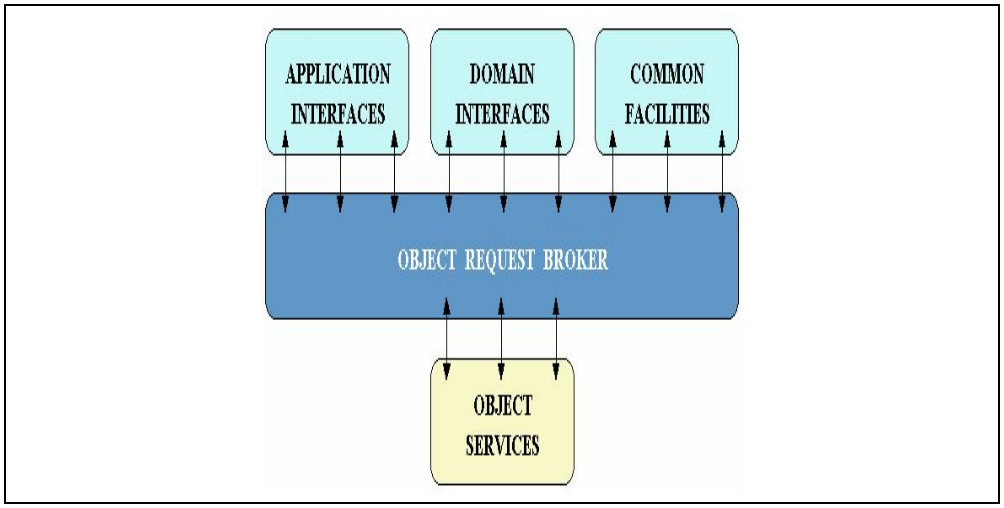

Abbildung 6.22: CORBA Architektur (von [http://www.omg.org])

und Kooperation von Software-Bausteinen auf verschiedenen Systemplattformen zu ermöglichen und dadurch die Portabilität, Interoperabilität und Wiederverwendbarkeit der Software zu verbessern. Für diesen Zweck wird eine Basisarchitektur für verteilte, objektorientierte Anwendungen definiert und standardisiert werden, genannt *Object Management Architecture* (OMA) [WSWZ_97], [http://www.omg.org].
Die OMG unterteilt die Architektur in fünf Bereiche [http://www.omg.org], siehe Abbildung 6.22:

- *Object Request Broker* (ORB),
  der Kern von CORBA.

- *Object Services*,
  die Basisfunktionen für das Funktionieren eines verteilten Systems (Name-Server, Ereignismanagement, Transaktionen etc.).

- *Common Facilities*,
  eine Sammlung generischer Objekte für sich wiederholende Aufgaben (Benutzerschnittstellen, Datenbankschnittstellen etc.).

- *Domain Interfaces*,
  für die Lösung spezieller Aufgaben (Telekommunikation, Finanzwesen etc.).

- *Application Interfaces*,
  spezialisierte Objekte, die die eigentlichen Anwendungen darstellen.

Zur Einordnung CORBAs in die Arbeit der OMG [Fait_94]: Die *Object Management Architecture* (OMA) ist die gesamte, von der OMG definierte Architektur. Der *Objekt Request Broker* (ORB) erlaubt Objekten das Senden und Empfangen von Anforderungen und Ausgaben in einer verteilten Umgebung. Die *Common Object Request Broker Architecture* (CORBA) definiert die Interfaces zum ORB. Die *Object Services* sind eine Sammlung von Diensten (Interfaces und Objekte), die Basisfunktionen für die Benutzung und Implementierung von Objekten zur Verfügung stellen. Die *Common Facilities* sind Dienste, die allgemein verwendbare Fähigkeiten (Capabilities) für die Verwendung in Applikationen liefern, und die *Application Interfaces* sind spezifische Objekte für Applikationen der Endbenutzer.

Ein wichtiges Ziel von CORBA ist die Austauschbarkeit und Kooperation von Objekten unabhängig vom Standort der Objekte im Netzwerk, verwendeter Hardware und Betriebssystem, benutzten Datenformaten, Implementierungssprachen und Netzwerkprotokollen. Dafür wird die Schnittstelle eines Objekts stärker von der Implementierung getrennt als in üblichen objektorientierten Systemen. Dies wird erreicht, indem die Schnittstelle nicht in der gleichen Programmiersprache implementiert wird wie das dazugehörende Objekt, sondern in einer eigenen, standardisierten *CORBA-IDL* (Interface Description Language), die von der eigentlichen Schnittstelle in der Implementierung abstrahiert. Dadurch kann das Verhalten und die Funktionalität des Objekts unabhängig von Implementierungssprache und -hardware definiert werden.
Ein Client kann auf diese IDL-Schnittstelle eines Servers entweder über einen IDL-Compiler zugreifen (statische Aufrufe), oder dynamische Aufrufe über die Schnittstellenverwaltung machen.

6.6.1 Die Bereiche von CORBA

6.6.1.1 Object Request Broker (ORB)

Der *Object Request Broker* (ORB) ist als zentrales Element der CORBA-Architektur dafür verantwortlich, den Clients die Lokalisierung von Objekten und Diensten zu ermöglichen, indem er sie entweder dabei unterstützt oder aber diese Aufgabe auch komplett übernimmt. Er ist außerdem für die Vermittlung von Objektaufrufen zuständig. Von CORBA werden alle Funktionalitäten und Schnittstellen definiert, die der ORB für diese Objektaufrufe zur Verfügung stellt.
Die Wahl eines Zielobjekts geschieht über eine Objektreferenz, die der Client entweder über einen Dienst wie den Name-Server, Broker oder Service Factory oder von einem anderen Objekt erhält. Die Referenz ist unabhängig vom Standort des Clients und bezeichnet das Zielobjekt (Server-Objekt), welches an einer beliebigen Stelle im CORBA-System angesiedelt sein kann, eindeutig. Der Client kann dann die im Zielobjekt in dessen IDL-Spezifikation definierten Methoden verwenden. Die Funktionen und externen Schnittstellen des Server-Objekts werden dem ORB bei der Registrierung mitgeteilt und im ORB gespeichert. Der ORB teilt dem Zielobjekt die anzuwendende Methode und die Parameter mit. Nach der Ausführung der Methode durch das Zielobjekt empfängt der ORB die Ergebnisse bzw. eine Exception und leitet sie an den Client weiter. Das Zielobjekt selber ist ein gekapseltes Objekt, das seine Dienste nur über die IDL-Schnittstelle zur Verfügung stellt.
Ein ORB kann Aufrufe auch an andere ORBs weiterleiten, falls ein vom Client angeforderter Dienst im lokalen ORB nicht verfügbar ist, da die Objektreferenz den Standort des Dienstes eindeutig bestimmt.
Da CORBA von Betriebssystemen, Implementierungssprachen und Hardware unabhängig ist und verschiedene ORBs zusammenarbeiten können, können Server-Objekte über Rechner-, Hardwarearchitektur- und Programmiersprachengrenzen hinweg genutzt werden. Damit kann ein hoher Grad an Wiederverwendung implementierter Objekte erreicht werden, und Produkte verschiedener Hersteller können miteinander kombiniert werden. Dies macht CORBA zu einer geeigneten Plattform für die Entwicklung verteilter Anwendungen z.B. im Bereich der Telekommunikation, wie z.B. in TINA (siehe Abschnitt 6.7).
Vergleich:
Da man bei CORBA Adapter für die an den ORB anzupassenden Objekte implementieren muß (die IDLs), kann man die Objekte etwas mit den Modulen von SEMPER und der GCS-API und den Mechanismen der GSS-API vergleichen, der ORB gleicht generell einem Manager.

6.6.1.2 Object Services

Die *Object Services* sind Domain-unabhängige Interfaces, die von vielen verteilten Objekten verwendet werden, z.B. die *Naming Services*, mit denen Clients Objekte anhand von Namen finden können, und die *Trading Services*, mit denen Objekte anhand ihrer Eigenschaften gefunden werden können [Ohne_97]. Weitere Spezifikationen für Object Services existieren z.B. für Lebenszyklenverwaltung, Sicherheit,Transaktionen und Ereignisverwaltung.

6.6.2 Sicherheit in CORBA

Die den Bereich Sicherheit betreffenden Spezifikationen finden sich in [OMG_97, Kapitel 15, Security Service Specification].
Hauptziel der Sicherheit in CORBA sind die üblichen Schutzziele [Fait_94]:

- Vertraulichkeit (Confidentiality),
- Integrität (Integrity),
- Verbindlichkeit (Accountability),
- Verfügbarkeit (Availability).

Diese werden jeweils für das verteilte System definiert, um Problemen wie dem Verlust von Daten, der Verfälschung von Daten oder der Aufdeckung von Daten gegenüber Unbefugten zu begegnen [WSWZ_97].
Die Sicherheitsziele werden durch die Verwendung von Sicherheitsfunktionen wie Authentikation, Zugriffskontrolle, Auditing, Verschlüsselung und dazugehörende Verwaltungsfunktionen verfolgt. Zusätzlich gibt es Voraussetzungen für die Konstruktion des Systems, um z.B. zu garantieren, daß eine adäquate Trennung von Daten und Funktionen erfolgt, so daß kein Objekt mit den anderen interferieren kann, sowie die Trennung der Benutzerdienste, so daß der Schaden, den ein einzelner Benutzer anrichten kann, begrenzt ist [Fait_94], [OMG_97].
Vergleich:
Ein detaillierter Vergleich für diesen Teil der Sicherheitsspezifikation erübrigt sich: Es handelt sich um die klassischen Schutzziele, wie sie für fast alle Systeme gestellt werden. Auch die vorhandenen Schutzfunktionen weichen nicht vom üblichen Rahmen ab. Nicht ganz so üblich ist einzig die Forderung nach einer adäquaten Trennung von Daten und Funktionen, was sich aber aus dem Verwendungszweck CORBAs für verteilte Systeme und den sich daraus ergebenden Anforderungen ergibt.
Neu im Vergleich zu den vorherigen Frameworks ist die Zugriffskontrolle, die hier ziwschen beliebigen Anwendungsobjekten betrachtet wird, während es sich bei den anderen bisher betrachteten Frameworks um konkrete Sicherheitsdienste handelt, die teilweise durch einen Zugriffsschutz geschützt sind

6.6.2.1 Die CORBA-Sicherheitsarchitektur

Einer der wichtigsten Grundsätze der CORBA-Sicherheitsarchitektur ist Flexibilität, sowohl bei der Implementierung als auch bei der Installation und bei der Benutzung. Daher gibt es keine verbindliche Sicherheitspolitik, sondern es wird ein Rahmenwerk für die Unterstützung unterschiedlicher Sicherheitspolitiken festgelegt [OMG_97]. Die Sicherheitsarchitektur ist generisch gestaltet, so daß sie für viele Anwendungen angepaßt werden kann, trotzdem sind die Schnittstellen und die dazugehörigen IDL-Konstrukte weitgehend definiert, um die Anwendung zu vereinheitlichen.

Die ORB-Anbieter können zwischen vielen verschiedenen Optionen für die Implementierung der Sicherheitsarchitektur wählen und auch Technologien anderer Anbieter in ihre ORBs integrieren, die Anwender der ORB können für sich geeignete Sicherheitspolitiken definieren und anwenden, und die Anwendungsprogrammierer können über ein Mindestmaß hinaus weitere Sicherheitsmaßnahmen implementieren [WSWZ_97].
Vergleich:
Dies trifft auch auf die GSS- und GCS-APIs zu, da beide generische Sicherheitslösungen zur Verfügung stellen. Bei SEMPER ist die Sachlage aufgrund der beabsichtigten Verwendungszwecke etwas anders, die SEMPER-APIs können jedoch ebenfalls generisch verwendet werden. Bei CORBA kommt wieder der etwas anders gelagerte Verwendungszweck zum Tragen: Es macht eben generell einen Unterschied, ob ein Framework für die Kommunikation verschiedener Systeme über evtl. unsichere Netze entworfen wird, oder ob es für die Benutzung in verteilten Systemen gedacht ist.

6.6.2.1.1 Principals

Die CORBA-Sicherheitsarchitektur beruht auf *Principals* genannten agierenden Subjekten, die bestimmte Rechte für den Zugriff auf Objekte besitzen, die vom System zur Laufzeit geprüft werden. Ein Principal kann dabei ein menschlicher Benutzer oder eine Systemeinheit sein, die innerhalb des Systems registriert und zu authentisieren ist. Ein Principal kann mehrere durch Attribute repräsentierte Identitäten haben, die für verschiedene Zwecke genutzt werden. Diese unterschiedlichen Identitäten sollen durch unterschiedliche Methoden geschützt werden. Durch sie kann auch eine gewisse Anonymität im System erreicht werden, da sie nicht explizit untereinander verknüpft werden können. Als Nachteil ergibt sich ein für den Nutzer komplexeres Gesamtsystem.
Die Attribute eines Principals werden in sicheren CORBA-Systemen in einer *Credential* genannten Datenstruktur gespeichert [OMG_97].
Sicherheitsattribute erhält ein Principal auf drei Wegen [WSWZ_97]:

- **Öffentliche** Attribute sind ohne Authentikation für alle Principals zugänglich,
- Mittels **Authentikation** erhalten sie z.B. Identitätsattribute und Zugriffsrechte,
- Attribute sind durch **Delegation** auf andere Principals übertragbar.

Die Gültigkeit eines Attributs kann zeitlich oder anderweitig begrenzt sein, um zu kontrollieren, wann und wo es benutzt werden darf.
Ein durch Delegation von einem anderen Principal erhaltenes Attribut kann für weitere Delegationen an Objekte benutzt werden, wodurch sogenannte *Aufrufketten* entstehen, in denen Zugriffsrechte auf unterschiedliche Art und Weise delegiert werden können. Bei einer einfachen Delegation erlaubt ein Client den dazwischenliegenden Objekten, seine Zugriffsrechte komplett zu übernehmen, wobei das Zielobjekt keine Informationen über dazwischenliegende Objekte erhält. Bei einer zusammengesetzten Delegation kann das Zielobjekt dagegen genau feststellen, welches Zugriffsrecht von welchem Objekt stammt. Andere, komplexere Schemata werden ebenfalls definiert [WSWZ_97].
Vergleich:
Das System der Principals gibt es so in keinem der bisher betrachteten Frameworks. Die Attribute als Beschreibung bestehender Rechte sind etwas vergleichbar mit der Funktionalität des Access Control Blocks und des Certificate Blocks in SEMPER sowie der Authorisationspolitik der GCS-API. Ein wichtiger Unterschied ist dabei der Geltungsbereich: Während SEMPER und die GCS-API die Authentikation lokal (für einen Rechner)

betrachten, gilt die Authentikation bei CORBA zusätzlich global, da ein auf einem Rechner authentisierter Principal auf Objekte auf allen anderen Rechnern im CORBA-System zugreifen kann.
Die Zugriffskontrolle in CORBA entspricht weitgehend der klassischen Zugriffskontrolle mit Subjekten, Operationen, Granulen und Erlaubnissen (grant), siehe z.B. [Brüg_94, Abschnitt A.2] und [Bisk1_93, Kapitel 3]

6.6.2.1.2 Sicherung von Objektaufrufen

Für Objektaufrufe existieren sowohl auf Sender- als auch auf Empfängerseite Sicherheitsmechanismen wie z.B. Zugriffskontrollen, Auditing und Verschlüsselung. Objekte müssen sich sowohl gegeneinander als auch gegenüber dem System authentisieren.
Ruft ein Client Funktionen auf einem Zielobjekt auf, wird jeweils eine neue Verbindung eingerichtet, wobei folgendermaßen vorgegangen wird [WSWZ_97], [OMG_97]:

1. Herstellung von Vertrauen in die Identität des Kommunikationspartners, wobei das Zielobjekt die Sicherheitsattribute des Clients überprüft.
2. Übermittlung der Legitimation einschließlich der Sicherheitsattribute des Clients an das Zielobjekt, Überprüfung der Sicherheitsattribute durch das Zielobjekt.
3. Einrichtung eines Sicherheitskontextes, der zum gewünschten Schutz der Kommunikation zwischen Client und Zielobjekt benutzt wird.

Die Art des Verbindungsaufbaus ist abhängig von den zugrundeliegenden Sicherheitspolitiken der Kommunikationspartner und den verwendeten Sicherheitsmechanismen. Jedes Objekt wird automatisch durch die in der zugehörigen Sicherheitspolitik definierten Schutzmaßnahmen geschützt, unabhängig davon, ob dies in der Implementierung des Objekts vorgesehen ist oder nicht. Dies erfolgt, indem jede Interaktion eines Objekts durch den CORBA-Kern geleitet wird. Dort wird die für das Objekt zuständige Sicherheitspolitik festgestellt und die entsprechenden Schutzmaßnahmen werden durchgeführt. Welche Mechanismen dafür verwendet werden, wird nicht in der CORBA-Sicherheitsarchitektur festgelegt, sondern in der ORB-Implementierung oder -Installation. Notwendige Initialisierungen werden automatisch vom ORB vorgenommen.
Vergleich:
Auch dieses Verfahren ist mit den anderen Frameworks nur bedingt vergleichbar. Es ähnelt etwas dem System von SEMPER, bei dem alle Nachrichten vom SecCom-Block unter Kontrolle des SecCom-Managers mit Hilfe der Serviceblocks transportiert werden. Bei der GSS-API erfolgt der Verbindungsaufbau im Rahmen der Sicherheitsreferenzen, in der GCS-API erfüllt die Session-Verwaltung einen ähnlichen Zweck.
Falls die Integrität einer Nachricht geschützt wird, müssen spezielle Sicherheits-Gateways verwendet werden, da keine weitere Modifikation der geschützten Nachricht (wie z.B. eine Änderung der Länge durch Anhängen von Prüfbits oder durch Komprimierung) erlaubt ist. Über diese Sicherheits-Gateways werden keine weiteren Aussagen gemacht [WSWZ_97].
Vergleich:
Eine derartige Forderung findet sich in keinem der bisher betrachteten Frameworks. Der Sinn der Forderung wird auch nicht klar: Wenn einer signierten Nachricht in tieferen Schichten Prüfsummen angehängt werden (oder sogar wenn diese Nachricht komplett verändert wird, z.B. durch Komprimierung), die auf der Gegenseite wieder entfernt werden (bzw. rückgängig gemacht werden), so daß die ursprüngliche Nachricht an CORBA weitergegeben wird, so kann das keine Änderung der Integritätssicherung hervorrufen. Die Kommunikation sähe dann etwa folgendermaßen aus: [CORBA] $\rightarrow$ [Gateway mit

Änderung] → [Netz / Transport] → [Gateway, welches die Änderung rückgängig macht] → [CORBA]
Für alle Objektaufrufe existiert eine Zugriffskontrolle (die ebenfalls automatisch im CORBA-Kern durchgeführt wird), die auf sogenannten *Zugriffsentscheidungsfunktionen* basiert [WSWZ_97]. Die nötigen Parameter sind dabei die aktuellen Attribute des Clients, Restriktionen für diese Attribute wie z.B. die Gültigkeitsdauer, die auszuführende Operation sowie die Kontrollattribute des Zielobjekts.
Vergleich:
In SEMPER erfolgt die Zugriffskontrolle ähnlich wie hier durch den Access Control Block, in der GSS-API ist keine Zugriffskontrolle vorgesehen, d.h. dort muß sie außerhalb der API erfolgen. In der GCS-API erfolgt eine Zugriffskontrolle im Rahmen der Session-Verwaltung, zusätzlich gibt es die Authorisationspolitik.

6.6.2.1.3 Nichtabstreitbarkeit

Die Sicherstellung der Nichtabstreitbarkeit erfolgt unter Kontrolle der Anwendungen und wird nicht automatisch bei Objektaufrufen verwendet. Die in CORBA beschriebenen Funktionen zur Nichtabstreitbarkeit können sich auf die verschiedensten Aktionen beziehen, sie umfassen die Beweiserzeugung und -überprüfung. Eventuell kann es je nach zugrundeliegenden Sicherheitsmechanismen nötig sein, für die Nutzung von Nichtabstreitbarkeitsfunktionen dritte Instanzen einzuschalten.
Vergleich:
Nichtabstreitbarkeit gibt es ähnlich wie hier auch in SEMPER im Rahmen der Sicherheitsattribute des Transfer Layers, in der GSS-API werden ebenso wie in der GCS-API keine Angaben darüber gemacht, d.h. dort existieren entsprechende Funktionen nicht und müssen gegebenenfalls außerhalb der API durch externe Protokolle nachgebildet werden.

6.6.2.1.4 Domains

Eine *Domain* in CORBA ist eine Verwaltungseinheit, in der gewisse gemeinsame Merkmale existieren und in der die gleichen Regeln beachtet werden müssen. Für den Bereich der Sicherheit werden drei Domain-Typen beschrieben [WSWZ_97], [OMG_97]:

Sicherheitspolitik-Domain
: Der Bereich innerhalb CORBA, in dem eine bestimmte Sicherheitspolitik gilt. Es kann hierarchische Sub-Domains geben und verschiedene Domains können zu einer zusammengefaßt werden.

Sicherheitsumgebungs-Domain
: Der Bereich, in dem die Durchsetzung einer bestimmten Sicherheitspolitik durch lokale Mechanismen außerhalb des Objektsystems realisiert wird (z.B. ist für den Austausch von Nachrichten zwischen Objekten auf einer Maschine i.d.R. keine Verschlüsselung notwendig).

Sicherheitstechnologie-Domain
: Der Bereich, in dem die gleichen Sicherheitsmechanismen zur Durchsetzung einer Sicherheitspolitik verwendet werden.

Zwischen verschiedenen Sicherheitstechnologie-Domains können Sicherheitstechnologie-Gateways eingesetzt werden, die die Interoperabilität zwischen den verschiedenen Systemen und den dort angesiedelten Objekten ermöglichen.
Vergleich:
Sicherheits-Domains oder etwas damit vergleichbares gibt es weder in SEMPER noch

in der GSS- oder GCS-API. In der GSS- und GCS-API können den Domains entsprechende Einteilungen jedoch entstehen, wenn Kommunikationspartner verschiedene Sicherheitsmechanismen in den unteren Schichten verwenden, wodurch eine gemeinsame Schnittmenge für die Kommunikation verwendet werden muß und dadurch eine Art Sicherheitstechnologie-Domain entsteht.

6.6.3 Abschließende Bemerkungen zu CORBA

Vergleich:
Bei CORBA gibt es keine Crypto-API, SecCom-APIs oder ähnliches, sondern es werden generische Sicherheits-APIs verwendet, um externe Sicherheitsfunktionen anzusprechen. Die Verwaltung dieser Funktionen erfolgt durch den ORB.

6.7 Telecommunication Information Networking Architecture (TINA)

Die *Telecommunication Information Networking Architecture* (TINA) wird vom gleichnamigen Konsortium (siehe Abschnitt 5.3) entwickelt. Die Architektur soll für alle Bereiche von Telekommunikations- und Informationssystemen verwendet werden, z.B. Terminals (Personal Computer etc.), Transport-Server (Switches, Router etc.), Service-Server (Video on Demand, WWW etc.) und Management-Server (Authentikation, Rechnungserstellung etc.). Dafür werden sogenannte *Reference Points* definiert, über die Konformitätsanforderungen für TINA-Produkte spezifiziert werden.
Technisches Ziel von TINA ist die Bereitstellung von Konzepten und Prinzipien für Entwurf, Erstellung, Betrieb und Management von Telekommunikations-Software [WSWZ_97].
Die Architektur basiert unter anderem auf folgenden Prinzipien [http://www.tinac.com]:

1. Objekt-Orientiert

2. Verteilt

3. Entkoppelung von Softwarekomponenten

Durch diese Prinzipien soll die Interoperabilität, Portabilität und Wiederverwendbarkeit der Softwarekomponenten sichergestellt werden, sowie die Unabhängigkeit von spezifischen Technologien erreicht werden.
Für den Aufbau von TINA gibt es zwei Varianten, einmal mit 3 und einmal mit 4 Blöcken. Im folgenden wird die Variante mit 4 Blöcken beschrieben, die auch in [WSWZ_97] verwendet wird. Die Version mit 3 Blöcken stammt aus einer Beschreibung von [http://www.tinac.com] und ist wahrscheinlich älter, leider gibt es dabei keine Datumsangabe.

6.7.1 TINA-C Architektur

Die Architektur von TINA ist in vier technische Bereiche unterteilt, für die jeweils eine Architektur definiert ist, wobei eine Architektur als Menge von Konzepten, Prinzipien und Richtlinien für Entwurf und Aufbau des Systems verstanden wird.
Die Architekturen sind nach [WSWZ_97]

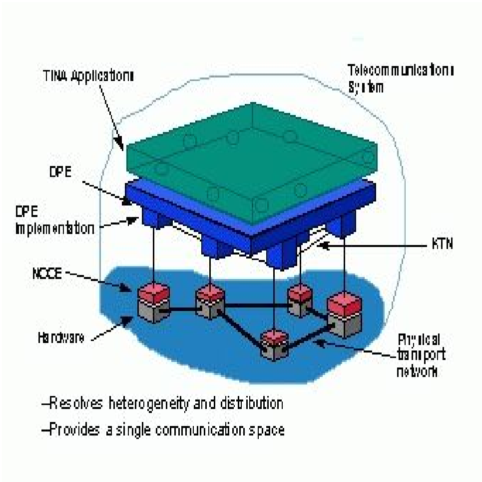

Abbildung 6.23: TINA Architektur (von [http://www.tinac.com])

- *Computing Architecture*
  für die Verfahren, mit denen die interagierenden Software-Komponenten (Computational Objects) spezifiziert werden und mit denen sie miteinander kommunizieren. Ein *Distributed Processing Environment* (DPE) definiert die Plattform für die verteilte Ausführung derartiger Komponenten.

- *Service Architecture*
  für Verfahren zur Spezifikation, Analyse, Entwurf und Betrieb von dienstbezogenen Telekommunikationskomponenten.

- *Management Architecture*
  die generische Konzepte für das Management der anderen Architekturen liefert.

- *Network Architecture*
  für die Definition generischer Netzwerkkomponenten, die eine hohe Abstraktion der realen Ressourcen darstellen, damit diese von anderen Diensten genutzt werden können.

In jeder Architektur werden die in den anderen Architekturen definierten Verfahren verwendet.
Ein Hauptmerkmal der TINA-Architektur sind die *Distributed Processing Environments* (DPEs), siehe Abbildung 6.23, mit einer einheitlichen Benutzungsschnittstelle zu allen zum TINA-System gehörenden Bestandteile (Computer, Vermittlungsrechner, Desktop Boxes, LANs etc.). Jede Interaktion zwischen verschiedenen Dienst-Komponenten, d.h. zwischen den diese darstellenden Anwendungsobjekten, erfolgt entsprechend einem standardisiertem Protokoll über das darunterliegende DPE. Die dafür benötigten Mechanismen werden in der DPE realisiert und über die dazugehörende DPE-Schnittstelle benutzt. Für die DPE ist nach [WSWZ_97] CORBA (siehe Abschnitt 6.6) ein aussichtsreicher Kandidat.
Das DPE ist die Zwischenschicht, die auf dem lokalen Betriebssystem der entsprechenden Rechner aufsetzt und Dienste für die über ihr angesiedelten Anwendungen zur Verfügung stellt. Zusätzliche DPE-Dienste wie z.B. Name-Server stehen für die Vereinfachung der Zusammenarbeit der Anwendungen zur Verfügung [http://www.tinac.com].

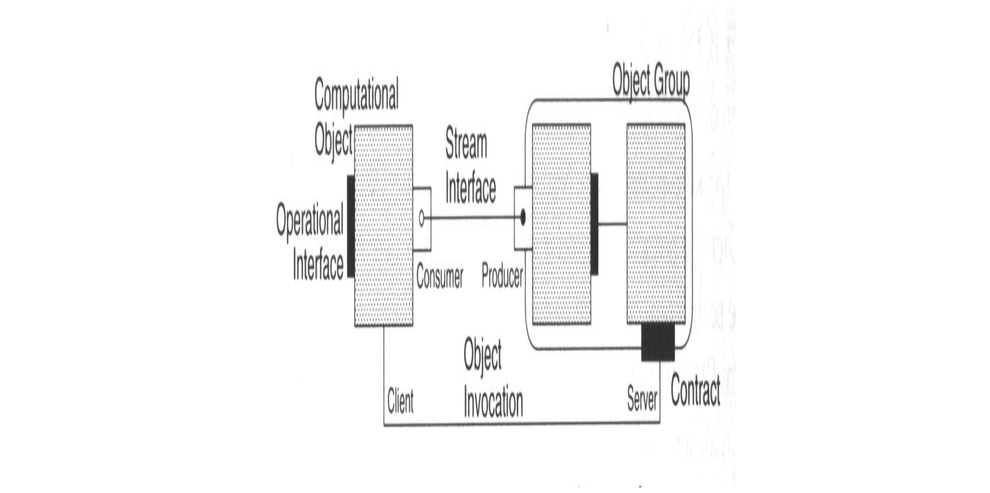

Abbildung 6.24: Objekt-Interfaces (aus [WSWZ_97])

Von den oben aufgeführten Architekturen interessiert hier vor allem die Computing Architecture: Die Anwendungen in TINA sind als verteilte Anwendungen aus miteinander interagierenden Objekten aufgebaut. Diese Interaktion dieser sogenannten *Computational Objects* erfolgt über ihre *Computational Interfaces*, die in zwei Gruppen unterteilt werden,

- die *Operational Interfaces*,
  die eine Menge von Operationen mit dazugehörenden Argumenten, Resultaten und Exceptions eines als Server fungierenden Objekts definieren, welche von einem als Client arbeitenden Objekt aufgerufen werden,

- und die *Stream Interfaces*,
  die keine Operationen besitzen, sondern den Fluß unstrukturierter Informationen, z.B. Audio- oder Videoströme zwischen zwei derartiger Interfaces erlauben, wobei ein Objekt Erzeuger (Producer) und das andere Konsument (Consumer) ist.

Jedes Objekt kann beliebig viele Interfaces besitzen, und mehrere Objekte können zu einer *Object Group* zusammengefaßt werden, wobei nicht alle Interfaces der Mitglieder der Gruppe von außen zugänglich sind, sondern nur die speziell dafür spezifizierten Interfaces, genannt *Contracts*.

Vergleich:
Bei SEMPER hat jeder Benutzer lokale APIs, die Kommunikationspartner kommunizieren über Protokolle. Bei der GSS-API existieren nur die APIs, die Kommunikationspartner kommunizieren unabhängig von den APIs, wobei sie die von den APIs erzeugten Token austauschen. Hier bei TINA existiert eine gemeinsame API bzw. ein gemeinsames Programmierinterface für lokale und entfernte Benutzung, d.h. die Clients verursachen Programmausführungen auf den Servern.

Als Beschreibungssprache für die Computational Objects definiert TINA eine eigene Sprache, genannt *Object Definition Language* (ODL), die besonders dafür geeignet ist, die für die Telekommunikation benötigten Konzepte wie z.B. Stream Interfaces zu beschreiben.

6.7.2 Sicherheit in TINA

In TINA existieren komplexe Probleme sowohl im Bereich klassischer Sicherheit (Stichwort: Nutzungsabrechnung) als auch im Datenschutz (*privacy protection*), da eine große Menge sensibler Daten anfallen, wie die Kommunikationsbeziehungen der Teilnehmer. Bisher ist der Bereich Sicherheit in TINA nicht sehr weit entwickelt [WSWZ_97], evtl. wird dies Teil der Entwicklung in der folgenden Arbeitsperiode sein, bis zum jetzigen Zeitpunkt (Februar 1998) wurden darüber jedoch keine Aussagen gemacht. Für weitere Informationen sei daher auf die Homepage des TINA-Konsortiums verwiesen: <http://www.tinac.com>.
Bisher wurden erst einige grundlegende Prinzipien festgelegt, wie Sicherheit für Dienste und deren Management in TINA realisiert werden soll [WSWZ_97]. Dabei wird eine mehrseitige Sicherheit, d.h. sowohl für Benutzer als auch Betreiber und Diensteanbieter als explizites Ziel festgelegt. Den Benutzern wird auch ein Recht auf Schutz der Privatsphäre und auf Anonymität zugestanden, wobei jedoch keine Angaben gemacht werden, ob dabei nur Anonymität der Benutzer untereinander oder auch gegenüber den Betreibern gemeint ist [WSWZ_97]. Es wird auch nicht präzisiert, wie dies geschehen soll.
In [TINA_97, Abschnitt 8.1], werden für die nächste Ausgabe der Network Architecture für den Bereich Sicherheit angekündigt:

- Die Definition der *Quality of Protection* (QoP), die die Anforderungen an das Sicherheitsmanagement beschreibt, d.h. was wie geschützt werden soll.

- Angaben darüber, wie die QoP erreicht werden soll. Es wird davon ausgegangen, daß die DPE einige Basismechanismen wie Authentikation und Verschlüsselung zur Verfügung stellt, weitere Funktionen müssen gesondert betrachtet werden. Wenn die Network Architecture unabhängig von der DPE eingesetzt werden soll, muß die Sicherheit unabhängig von dieser erreicht werden (was aber nicht betrachtet werden soll).

Leider wurden bei TINA noch keine besonders ergiebigen Aussagen zum Thema Sicherheit gemacht - zwar steht in allen Spezifikationen, daß Sicherheit wichtig ist und eingebaut werden soll, und es werden einigen minimale Angaben gemacht, was passieren soll, nur ist bisher nichts derartiges passiert.

6.7.2.1 Sicherheitsklassifikation

Da verschiedene Teile eines TINA-Systems unterschiedliche Anforderungen bezüglich Sicherheit haben, wird von TINA die folgende Sicherheitsklassifikation eingeführt [WSWZ_97]:

- Sicherheit des Telekommunikationssystems und der Telekommunikationsdienste,
  d.h. z.B. Schutz gegen Gebührenbetrug und Schutz gegen Abhören.

- Sicherheit des Managementsystems,
  d.h. z.B. Schutz der Konfigurationsdaten vor unbefugtem Zugriff,

- Sicherheit des DPE und der DPE-Sicherheitsdienste,
  wodurch die Mechanismen bereitgestellt werden, um die obigen Kategorien zu ermöglichen,

- Sicherheitsmanagement,
  also das Management der obigen Kategorien, wie z.B. die Schlüsselverwaltung.

Vergleich:
Eine derartige Klassifikation existiert weder in SEMPER noch in der GSS- oder GCS-API, sie ist dort aber auch nicht erforderlich, sondern in TINA Folge des besonderen Verwendungszwecks des Frameworks.
Aus Sicht der DPE sind die Sicherung des Telekommunikationssystems und des Managementsystems als Anwendungen oberhalb der DPE sehr ähnlich.

6.7.2.2 Sicherheit der Distributed Processing Environment (DPE) und Sicherheit für Anwendungsobjekte

Falls CORBA als DPE verwendet wird, wird TINA eine Sicherheitsarchitektur ähnlich der in CORBA realisieren. Damit gelten alle dort gemachten Aussagen auch für TINA. Dabei ist insbesondere die Interoperabilität verschiedener Implementierungen sehr wichtig, damit auch bei Verwendung unterschiedlicher Technologien durch die Betreiber die Sicherheit über Betreibergrenzen hinweg sichergestellt werden kann.
Die Anwendungsobjekte bauen auf die DPE auf, also gelten für sie gegebenenfalls die gleichen Sicherheitsaussagen wie für Anwendungen die auf CORBA aufbauen.
Vergleich:
Zur Sicherheit in CORBA siehe dort - ansonsten können keine Vergleiche gemacht werden, da dafür jede Voraussetzung fehlt.

6.8 Intel Common Data Security Architecture (CDSA)

Die *Common Data Security Architecture* (CDSA), die von der US-amerikanischen Intel Corporation entwickelt wird, ist eine Menge in Schichten angeordneter Sicherheitsdienste für Kommunikations- und Datensicherheit in Intranets sowie im Internet [Intel_97]. Die Intel Architecture Labs (IAL) entwickeln die CDSA aus folgenden Gründen [Intel_97]:

- Förderung offener, interoperabler, horizontaler Sicherheitsstandards
- Bereitstellung essentieller Sicherheitskomponenten für die Industrie.

CDSA betrachtet besonders die Sicherheit für verteilte Peer-to-Peer-Systeme mit heterogenen und homogenen Plattformen, berücksichtigt aber auch die Komponenten von Client-Server-Applikationen. Sie umfaßt die Sicherheitsbedürfnisse vieler Applikationen, einschließlich [Intel_97]:

- Electronic Commerce für Business-to-Business- und Home-to-Business-Anwendungen
- Vertrieb elektronischer Güter wie Software, Informationen, Ausbildungsmaterial oder Unterhaltung
- Messung von Inhalten und Diensten sowie damit verbunden die sichere Speicherung von Status und Werte
- Sichere Geschäfts- und Privataktivitäten wie E-Mail, Homebanking und Geldübertragungen

Um diesen Sicherheitsbedürfnissen gerecht zu werden, verwendet die CDSA die folgenden Maßnahmen [Intel_97]:

- Unterstützung in Schichten angeordneter Sicherheitsmechanismen (keiner Politiken)

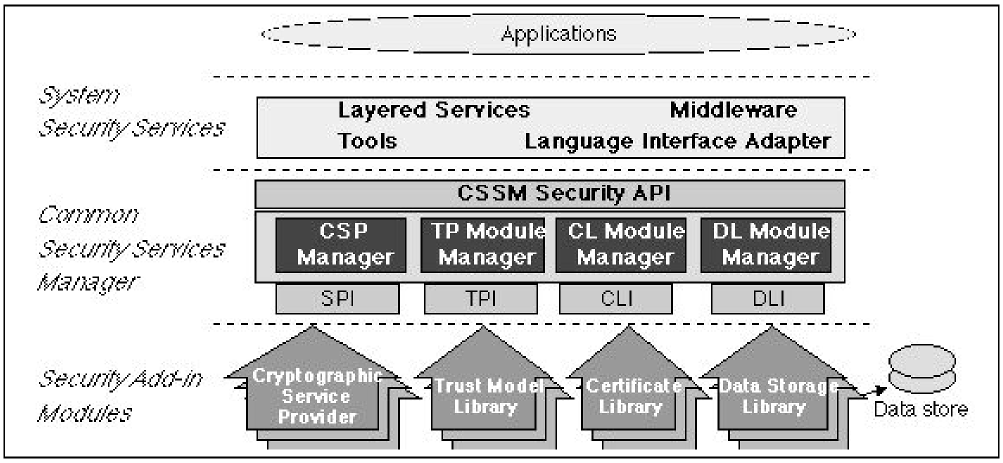

Abbildung 6.25: Der Aufbau der CDSA (aus [Inte1_97])

- Unterstützung Anwendungsspezifischer Politiken, indem erweiterbare Mechanismen für das Management einzufügender, politikspezifischer Module (add-in modules) unterstützt werden
- Flexible Interfaces für eine breite Auswahl von Zertifikat- und Dokumentenformaten wie X.509, SPKI, SDSI und EDI
- Unterstützung sicherere PRotokolle wie SSL und SET

6.8.1 CDSA-Architektur

Die Common Data Security Architecture definiert die Infrastruktur für eine Menge von Sicherheitsdiensten, Kryptographie bildet die Basis für Sicherheitsprotokolle und Sicherheitssysteme. Die CDSA ist eine erweiterbare Architektur, die Mechanismen für die dynamische Einbindung von Sicherheitsmodulen besitzt (Add-in security modules). Abbildung 6.25 zeigt die drei Schichten der Common Data Security Architecture: Der *Common Security Services Manager* (CSSM) ist der Kern der CDSA-Architektur, er bildet eine API, die Anwendungen benutzen müssen, wenn sie eingefügte Servicemodule benutzen wollen. Anwendungen fordern Sicherheitsdienste über die CSSM Security API oder über die durch die CSSM-API implementierten Schichten mit Sicherheitsdiensten und Tools an. Die Anforderungen werden von eingebundenen Sicherheitsmodulen bearbeitet, wobei vier Typen von Modulen definiert sind [Inte1_97]:

1. Kryptographische Dienste (Cryptographic Services),
   spezifiziert in SPI (*Cryptographic Service Provider Interface Specification*)
2. Vertrauenspolitiken (Trust Policy Services),
   spezifiziert in TPI (*Trust Policy Interface Specification*)
3. Zertifikate (Certificate Library Services),
   spezifiziert in CLI (*Certificate Library Interface Specification*)
4. Datenspeicherung (Data Storage Library Services),
   spezifiziert in DLI (*Data Storage Library Interface Specification*)

Die eingefügten Sicherheitsmodule können von unabhängigen Soft- und Hardwareproduzenten als Zusatzprodukte angeboten werden. Anwendungen können ihre

Anforderungen entweder an Module bestimmter Hersteller richten oder allgemein an alle Module, die den gewünschten Dienst anbieten.

Vergleich:

Das Einfügen von bzw. Aufsetzen auf externe kryptographische Funktionen gleicht dem Vorgehen der GSS-API. Ebenso wie dort wird die Art der gewünschten Aktion angegeben und die notwendige Funktion von der API ausgewählt.

Bei SEMPER, der GCS-API und CORBA sind die kryptographischen Funktionen Teil des Frameworks TINA besitzt gar keine kryptographischen Funktionen.

6.8.1.1 Prinzipien der Architektur

Das Design der CDSA folgt den folgenden fünf Prinzipien [Intel_97]:

- In Schichten angeordnetes Modell für Diensteanbieter
  CDSA besteht aus einer Menge von horizontalen Schichten, von denen jede Dienste für die darüberliegende Schicht anbietet. Dieser Ansatz ist portable, anpaßbar, modular und offen.

- Offene Architektur
  Die CDSA ist vollkommen offengelegt, um einen Review durch die Industrie zu ermöglichen.

- Modularität und Erweiterbarkeit
  Komponenten aus jeder Schicht können als separate Module gewählt werden. Ein erweiterbares Framework erlaubt das einfügen Domain-spezifischer Funktionen.

- Verwaltung von Details
  Die CDSA kann Sicherheitsdetails verwalten, so daß individuelle Anwendungen sich nicht damit befassen müssen.

- Berücksichtigung neuer Prinzipien
  Die CDSA basiert auf den neusten Prinzipien der Sicherheit.

Vergleich:

Diese Art des Aufbaus gleicht mehr oder weniger dem Aufbau der GSS- und GCS-API, was sich aus den relativ ähnlichem Verwendungszweck ergibt. SEMPER besitzt durch seine Business Application einen etwas anderen Aufbau, bei CORBA und TINA ergibt sich ein anderer Aufbau durch den anderen Verwendungszweck.

Die CDSA baut auf zwei fundamentalen Prämissen auf [Intel_97]:

- Portable Digitale Token
  werden als „Digitale Persönlichkeiten“ für Handel, Kommunikation und Zugriffskontrolle echter Personen benutzt.Diese Digitalen Token sind Verschlüsselungsmodule mit einem bestimmten Speicherplatz, die je nach Sicherheitsanforderungen der Anwendungen in Soft- oder Hardware ausgeführt sein können. Sie können verschiedene Formen annehmen und verschiedene Funktionen in einer einzigen Einheit zusammenfassen, wie z.B. eine Digitale Brieftasche.

- Digitale Zertifikate
  können als Ausdruck für Vertrauen dienen. Sie bilden keine neuen Vertrauensmodelle oder Verbindungen, sondern sind die Digitale Form der derzeitigen Vertrauensmodelle. Eine Person kann ein Zertifikat für jede Vertrauensbeziehung haben, wie z.B. mehrere Kreditkarten und Scheckbücher.

Vergleich:

Die Token ähneln etwas den Principals in CORBA, in den anderen Frameworks gibt es

etwas derartiges nicht. Sie sind insbesondere nicht identisch mit den Token der GSS-API, die dort die zu übertragenden Daten darstellen.
Die Zertifikate werden hier wie üblich definiert und verwendet, sie gleichen daher etwas den Referenzen der GSS-API, die aber über die üblichen Zertifikate hinausgehende Informationen enthalten. Die CDSA-Zertifikate sind auch vergleichbar mit den kryptographischen Kontexten der GCS-API. In CORBA gibt es nichts direkt vergleichbares.

6.8.1.2 Das Bedrohungsmodell

Die bösartige Beobachtung und Manipulation von Computersystemen kann nach [Intel_97] in drei Kategorien, eingeteilt nach der Herkunft der Bedrohung, klassifiziert werden:

- Kategorie I:
  Angriffe von außerhalb des Computersystems

  Der Angreifer verletzt die Zugriffskontrolle zur Kommunikation, hält aber die Regeln des Kommunikationsprotokolls ein. Die ist der übliche Angriff durch „Hacker“.

  Angriffe der Kategorie I können am besten durch korrekt entwickelte und implementierte Protokolle und Mechanismen zur Zugriffskontrolle sowie eine gründliche Systemverwaltung abgewehrt werden. Manipulationsgeschützte Software (tamper-resistant software) ist zu Abwehr derartiger Angriffe weniger geeignet.

  Das Ziel eines Kategorie I Angriffs ist oft die Vorbereitung eines Angriffs der Kategorie II.

- Kategorie II:
  Angriffe durch Software, die auf dem Computersystem läuft

  Der Angreifer transportiert bösartigen Code in das Computersystem und das Betriebssystem führt ihn aus. Der Angriff erfolgt in die Grenzen des Kommunikationsprotokolls, wird aber vom Betriebssystem, dessen Interfaces benutzt werden, begrenzt. Die entspricht einem üblichen Angriff durch Viren.

- Kategorie III:
  Der Angreifer besitzt die totale Kontrolle über das Computersystem, kann Hardware oder Systemsoftware austauschen und jeden Kommunikationskanal beobachten (z.B. durch eine Busanalysator)

  Diese Angriffe berücksichtigen keine Sicherheitsgrenzen und werden nur durch technische Erfahrung und finanzielle Resourcen begrenzt. Absolut gesehen sind Angriffe der Kategorie III nicht zu verhindern. Die Verteidigung gegen derartige Angriffe besteht darin, den Angriff soweit zu erschweren, daß der Aufwand größer als der Nutzen wird.

Ziel des Common Security Services Manager (CSSM) ist die Abwehr von Angriffen der Kategorie II und III.
Vergleich:
Ein derart detailliertes Bedrohungs- oder Angreifermodell wird in keinem der anderen Frameworks aufgestellt, dort gibt es auch keine Aussagen darüber, welche Arten von Angriffen abgewehrt werden sollen.

6.8.1.3 Überblick über die Architektur

Wie Abbildung 6.25 zeigt, definiert die CDSA drei Basis-Schichten:

- Systemsicherheitsdienste (System Security Services)

- Sicherheitsmanager (Common Security Services Manager, CSSM)
- Add-in Sicherheitsmodule (Kryptographische Funktionen, Module für Vertrauenspolitik, Zertifikatbibliotheken, Datenspeicherung)

6.8.1.3.1 Systemsicherheit

Die Systemsicherheitsschicht (*System Security Services*) befindet sich zwischen den Anwendungsprogrammen und den CSSM-Sicherheitsdiensten. Software auf dieser Schicht

- definiert Sicherheitsabstraktionen auf hohen Niveau, wie z.B. sichere E-Mail,
- unterstützt transparente Sicherheitsdienste wie z.B. sichere Filesysteme oder private Kommunikation,
- erlaubt den Zugriff auf die CSSM-Sicherheitsdienste für Anwendungen, die nicht in der Programmiersprache C geschrieben sind, und
- liefert Werkzeuge für die Verwaltung der Sicherheitsinfrastruktur.

Einige Dienste erlauben Anwendungen den Zugriff auf Sicherheitsdienste ohne expliziten Aufruf der CSSM-API. Damit ist es Anwendungen möglich, implizit Sicherheitsdienste zu nutzen.

Vergleich:

Die Systemsicherheitsschicht ist teilweise vergleichbar mit einem Manager in SEMPER wie z.B. dem SecCom-Manager. In der GSS-API gibt es nichts vergleichbares, sie endet im Prinzip „eine Schicht tiefer", bei der GCS-API ist sie in etwa vergleichbar mit der Session-Verwaltung. Bei TINA und CORBA gibt es für den Bereich Sicherheit nichts vergleichbares.

6.8.1.3.2 Sicherheitsmanager

Die zweite Schicht der CDSA ist der Sicherheitsmanager (*Common Security Services Manager* (CSSM)), der die Sicherheitsdienste in die CDSA integriert und verwaltet. Der CSSM besitzt eine API für die Unterstützung der Entwicklung sicherer Anwendungen und Systemdienste und Service Provider Interfaces (SPIs) für die Unterstützung von Plug-in-Sicherheitsmodulen.
Der CSSM besitzt ein Protokoll zur Integritätsüberprüfung zwischen den Add-in Modulen, den Anwendungen und dem CSSM. Während der Einbindung neuer Module finden eine gegenseitige Authentikation, Integritätsprüfung und Authorisation statt. Die Module besitzen zu diesem Zweck Zertifikate, die unter anderem auch die Rechte und Möglichkeiten der authentizierten Module beschreiben, so daß die CSSM anhand dieser Informationen auch die für einen bestimmten Verwendungszweck geeigneten Module auswählen kann. Die Signaturkette der Zertifikate identifiziert Wesen, denen vertraut wird, Zertifikate entsprechend den Regeln beteiligter Entscheidungsorgane zu erteilen.
Die CSSM schreibt weder eine auf Zertifikaten basierende Sicherheitspolitik vor, noch implementiert es sie. Anwendungsspezifische Sicherheitspolitiken werden durch die Add-in Module und die Sicherheitsschichten definiert und implementiert. Die CSSM integriert und verwaltet die grundlegenden Sicherheitskomponenten und definiert eine API für den Zugriff auf die Dienste der Add-in Module. Sie umfaßt auch keine kryptographischen Algorithmen, sondern leitet entsprechende Anforderungen durch das Service Provider Interface (SPI) an geeignete Add-in Module weiter.
Die CSSM unterstützt Kontextdienste, um Anwendungen bei der Verwaltung der für kryptographische Operationen notwendigen Parameter zu unterstützen. Ein *Sicherheitskontext* ist dabei eine Struktur, die alle zur Laufzeit anfallenden Geheimnisse

und Sicherheitsrelevanten Parameter einer Anwendung enthält. Nachdem ein Kontext gebildet wurde, kann die Anwendung ihn ohne Sicherheitskontrollen durch die CSSM verwenden.
Die CSSM besitzt außerdem grundlegende Integritätsdienste wie die selbständige Überprüfung der digitalen Signatur der CSSM-Programme, um Änderungen, z.B. durch Viren, zu erkennen.
Vergleich:
Auch der Sicherheitsmanager ist teilweise vergleichbar mit einem Manager in SEMPER wie z.B. dem SecCom-Manager. In der GSS-API gibt es nichts vergleichbares, bei der GCS-API ist sie ebenfalls vergleichbar mit der Session-Verwaltung. Bei TINA und CORBA gibt es für den Bereich Sicherheit wiederum nichts vergleichbares.
Der Sicherheitskontext gleicht dem Kontext in SEMPER, in der GSS-API gibt es nichts vergleichbares. In der GCS-API gleichen sie den kryptographischen Kontexten, mit dem Unterschied, daß die CCs der GCS-API für den Benutzer undurchsichtig sind während hier keine Angaben darüber gemacht werden. In TINA existiert nichts vergleichbares, in CORBA sind sie in etwas vergleichbar mit den Credentials, in denen die Attribute eines Principals gespeichert werden.
Durch die Verwaltung der Sicherheit entlastet der CSSM die Benutzer und Anwender von diesen Aufgaben. Die Verwaltungsdienste des CSSM sind auf vier Manager aufgeteilt:

- *Cryptographic Services Manager*
  Der Cryptographic Services Manager ist zuständig für die Verwaltung der auf dem lokalen System installierten kryptographischen Funktionen.

  Er bildet eine API für den Zugriff auf alle installierten kryptographischen Dienste. Diese werden von sogenannten *Cryptographic Service Providers* (CSPs) zur Verfügung gestellt.

- *Trust Policy Services Manager*
  Der Trust Policy Services Manager verwaltet die auf dem lokalen System installierten Vertrauenspolitiken und definiert eine API für diese Libraries. Die API erlaubt Anwendungen das Anfordern von Sicherheitsdiensten, die als ersten Schritt bei ihrer Ausführung die Auswahl und Anwendung einer Politik verlangen.

- *Certificate Services Manager*
  Der Certificate Services Manager verwaltet die Zertifikat-Bibliothek des lokalen Systems und erlaubt die Bildung, Signatur und Überprüfung eines Zertifikats sowie das Auslesen einzelner Parameter.

- *Data Store Services Manager*
  Der Data Store Services Manager definiert eine API für die sichere und persistente Speicherung von Zertifikaten und anderen Objekten. Die API erlaubt den Anwendungen die Suche und Auswahl der Datenobjekte. Die Speicheroperationen werden von Add-in Modulen bereitgestellt.

Abbildung 6.26 zeigt die Details des CSSM.

6.8.1.3.3 Add-in Sicherheitsmodule

CDSA besitzt vier logische Typen von Add-in Sicherheitsmodulen [Intel_97]:

- *Cryptographic Service Providers* (CSPs)
  Die CSPs sind Module, die kryptographische Operationen ausführen und private Schlüssel sicher speichern können. Ein CSP kann eine oder mehrere der folgenden kryptographischen Funktionen implementieren:

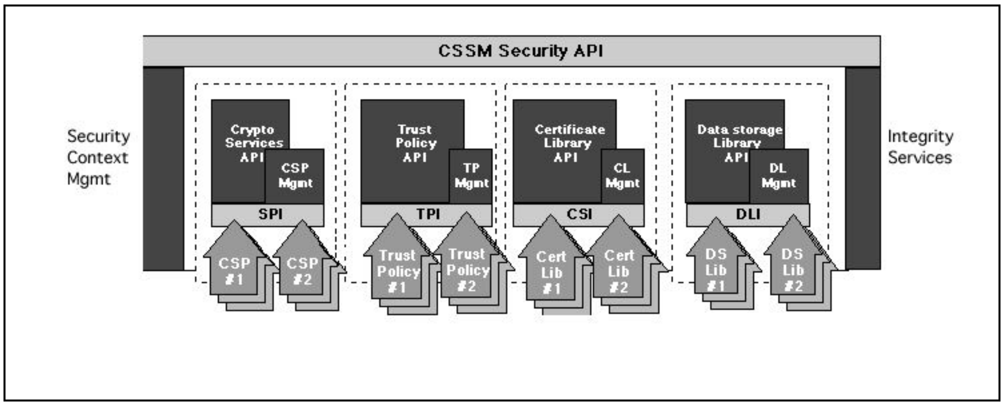

Abbildung 6.26: Der Aufbau des CSSM (aus [Intel_97])

- Verschlüsselungsalgorithmen
- Digitale Signieralgorithmen
- Kryptographische Hashfunktionen
- Einmalige Identifikationsnummern (Unique identification number)
- Zufallszahlengenerator
- Sichere Schlüsselspeicherung
- spezielle Funktionen für den spezifischen CSP

Ein CSP kann als Soft- oder Hardware oder als beides ausgeführt sein. Wird ein CSP durch den CSSM installiert, so ist der CSP auf den lokalen System benutzbar. Bei der Installation werden der Name des CSP, seine kryptographischen Dienste und die Informationen, die für die dynamische Nutzung des CSPs nötig sind, in einer Datenbank (Registry) gespeichert, wo sie von Anwendungen abgefragt werden können.

Jeder CSP muß die verschlüsselte Speicherung privater Schlüssel und Variablen ermöglichen.

- *Trust Policy modules* (TPs)
  Die TPs implementieren durch Autoritäten oder Institutionen definierte Politiken. Politiken definieren den Grad an Vertrauen, der für die Ausführung bestimmter Aktionen notwendig ist. Für alle Zertifikatbasierten Vertrauensbereiche existieren drei Basiskategorien:

  - Aktionen auf Zertifikate
  - Aktionen auf Zertifikatrückruflisten (certificate revocation lists)
  - Domain-spezifische Aktionen wie z.B. das Schreiben einer Datei

  Die CSSM Trust Policy API definiert die generischen Operationen, die von jedem TP-Modul unterstützt werden sollen, jedes Modul kann jedoch auch nur die Teilmenge an Operationen implementieren, die für seine Politik notwendig sind. Es könen auch zusätzliche Operationen implementiert werden, die dann über die Durchreich-Funktion der CSSM-API aufgerufen werden können.

- *Certificate Library modules* (CLs)
  Die CL-Module implementieren Funktionen für die syntaktische Manipulation im Speicher abgelegter Zertifikate und Zertifikatrückruflisten. Die CSSM-API

definiert die generischen Operationen, die von jedem CL-Modul unterstützt werden sollen, jedoch kann jedes Modul auch nur die Funktionen implementieren, die für die Manipulation seiner spezifischen Zertifikate (z.B. X.509) benötigt werden.

Die Implementierung dieser Operationen soll Semantik-frei sein, die semantische Interpretation soll in den TP-Modulen und Anwendungen erfolgen.

- *Data Storage Library modules* (DLs)
  Ein Data Storage Library Modul dient der dauerhaften Speicherung sicherheitsbezogener Datenobjekte. Diese Objekte können Zertifikate, Zertifikatrückruflisten, kryptographische Schlüssel, Politik-Objekte oder Anwendungsspezifische Objekte sein.

Vergleich:
Etwas den Add-in Modulen vergleichbares gibt es in SEMPER, wenn dort Funktionen Dritter eingebunden werden, in der GSS-API entsprechen sie den unter der API liegenden Mechanismen. In der GCS-API kann man die unter der CSF liegenden Algorithmen mit den Add-in Modulen vergleichen. Bei TINA gibt es nichts vergleichbares, bei CORBA werden ebenfalls externe Funktionen für die Sicherheitsfunktionen verwendet.
Wichtig hierbei ist, daß bei CDSA Module nachträglich, d.h. nach Auslieferung an den Kunden durch diesen eingebunden werden können, während dies bei allen anderen Frameworks nur durch den Hersteller vor der Auslieferung an den Kunden möglich ist.

6.8.2 Abschließende Bemerkungen zu CDSA

Vergleich:
CDSA definiert zum einen Managementfunktionen im CSSM, zum anderen die davon benutzten Funktionen in den Modulen, wobei diese Module sowohl von Intel als Herausgeber der Spezifikation als auch von anderen Anbietern geliefert werden können. Von Intel sind z.B. CSP-Module für den Data Encryption Standard (DES) zur Datenverschlüsselung, den Secure Hash Algorithm (SHA1) für die Generierung von Hashwerten, den Digital Signature Standard (DSS) für digitale Signaturen, den Message Digest (MD5) für die Generierung sicherer Hashwerte und ein Zufallszahlengenerator der die MD5- und DES-Algorithmen benutzt, erhältlich [http://www.intel.com]
Für den Vergleich der kryptographischen Funktionen in Tabelle 7.2 wurde die Dokumentation des Cryptographic Service Provider Interface (SPI), [Inte2_97], verwendet, auf die hier nicht einzeln eingegangen wurde.

6.9 RSA Cryptographic Token Interface (Cryptoki)

Die RSA Laboratories, eine Abteilung der RSA Data Security, Inc., entwickelt im Zusammenarbeit mit Vertretern von Industrie, Wissenschaft und Regierung eine Serie von Standards, genannt *Public-Key Cryptography Standards* (PKCS). Das *Cryptographic Token Interface* (Cryptoki) ist dabei das Dokument PKCS#11 [RSAD_95]. Dieser Standard spezifiziert eine API für Geräte (Devices), die kryptographische Informationen speichern und kryptographische Funktionen ausführen. Er folgt einem einfachen objektbasierten Ansatz mit dem Ziel der Technologieunabhängigkeit (jedes mögliche Gerät) und dem Teilen von Ressourcen (mehre Anwendungen benutzen mehrere Geräte). Den Anwendungen soll eine einheitliche, logische Sicht auf das Gerät, genannt „cryptographic token", ermöglicht werden. Dafür spezifiziert der Standard die Datentypen und Funktionen, die eine Anwendung benötigt, um kryptographische Dienste unter Verwendung der Programmiersprache C zu benutzen.

Diese Datentypen und Funktionen werden vom Lieferanten einer Cryptoki-Library als C-Headerfile zur Verfügung gestellt, ein separates Dokument liefert ein generisches, von Programmiersprachen unabhängiges Cryptoki-Interface [RSAD_95].
Cryptoki isoliert eine Anwendung von den Details der kryptographischen Geräte, sodaß die Anwendung nicht verändert werden muß, um ein anderes Gerät zu benutzen oder in einer anderen Umgebung zu laufen.
Vergleich:
Dies ist etwas gänzlich neues und mit keinem der anderen Frameworks vergleichbar: Die eigentlichen Funktionen und Geheimnisse befinden sich in sicheren Geräten, nicht im gleichen Rechner oder System wie bei den anderen Frameworks.

6.9.1 Überblick

Portable Geräte wie Smartcards, PCMCIA-Karten und Smart-Disketten sind ideale Werkzeuge für die implementierung von kryptographischen Funktionen mit öffentlichen Schlüsseln (Public Key), da in ihnen der private Schlüssel eines Schlüsselpaares aus geheimen und öffentlichen Schlüssel sicher unter Kontrolle eines einzelnen Benutzers gespeichert werden kann. Ebenso kann eine Funktion statt von der Anwendung selber direkt im Gerät ausgeführt werden, sodaß sensitive Informationen wie der private Schlüssel nie gezeigt werden muß. Da immer mehr Anwendungen für Public Key Kryptographie entwickelt werden, ergab sich die Notwendigkeit eines standardisierten Programmierinterfaces für derartige Geräte, die mit der Veröffentlichung des Cryptoki-Standards befriedigt wurde [RSAD_95].

6.9.1.1 Ziele der API

Cryptoki war von Anfang an als Interface zwischen Anwendungen und allen möglichen kryptographischen Geräten gedacht. Da bereits auf einigen Ebenen Standards (sowohl offiziell als auch de-facto) für die Schnittstellen zu diesen Geräten bestehen, wie z.B. für die mechanischen Charakteristiken und elektrischen Verbindungen ebenso wie für die Kommunikation mit diesen Geräten (siehe z.B. den PCMCIA-Standard oder ISO 7816 für Smartcards), blieb die Definition eines Befehlssatzes für kryptographische Funktionen. Da es nicht ausreicht, für jedes Gerät einen spezifischen Befehlssatz zu definieren, da damit kein von den Geräten unabhängiges Anwendungsinterface zu bilden ist, war es Ziel der Entwicklung des Cryptoki-Standards, ein Programmierinterface zu entwickeln, das die Details der Geräte abstrahiert und den Anwendungen ein einheitliches Modell eines kryptographischen Geräts, genannt „Cryptographic Token“ oder kurz „Token“, präsentiert. Ein weiteres Entwicklungsziel war das Teilen von Ressourcen, da Multitasking-Betriebssysteme immer populärer werden und damit ein einzelnes Gerät von mehreren Anwendungen benutzt werden kann. Es war nicht Ziel der Cryptoki-Entwicklung, ein generisches Interface für kryptographische Operationen oder Sicherheitsdienste zu bilden, auch wenn derartige Operationen mit Hilfe der Cryptoki-Funktionen gebildet werden können. Cryptoki wird als Komplement zur GSS-API (Abschnitt 6.4) und GCS-API (Abschnitt 6.5) gesehen, nicht als Konkurrent [RSAD_95].
Vergleich:
Wie schon geschrieben, ist Cryptoki keine Konkurrenz zu den anderen Frameworks, sondern eine Ergänzung. Daher bleibt nicht viel zu vergleichen ...

6.9.1.2 Modell der API

Das allgemeine Modell der Cryptoki-API zeigt Abbildung 6.27: Es beginnt mit einer oder mehreren Anwendungen, die verschiedene kryptographische Funktionen ausführen wollen, und endet mit einem oder mehreren Geräten, in denen diese

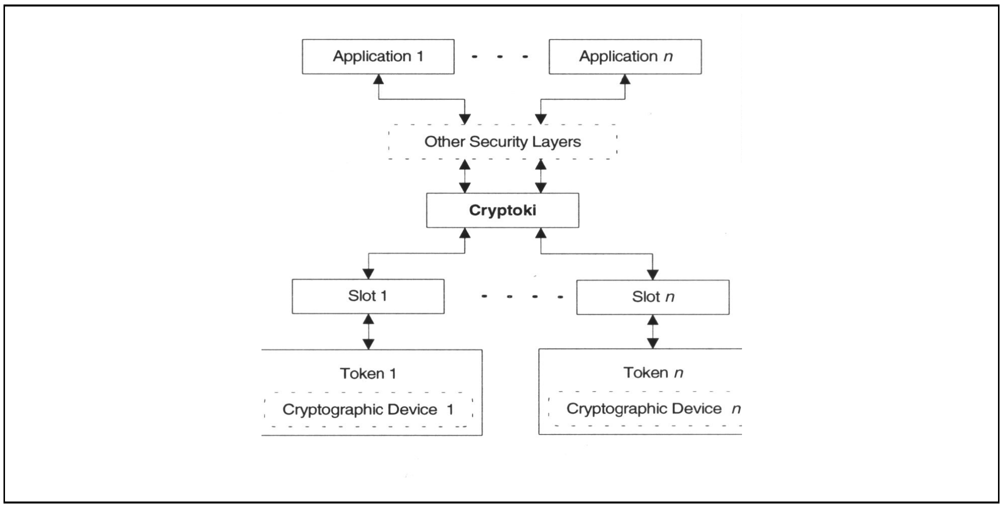

Abbildung 6.27: Allgemeines Modell von Cryptoki (aus [RSAD_95])

Funktionen ausgeführt werden. Eine Anwendung kann dabei mit einem Benutzer gleichgesetzt werden.
Cryptoki liefert ein Interface zu einen oder mehreren kryptographischen Geräten, die im System durch eine Anzahl von „Slots“ aktiv sind. Jeder *Slot* entspricht einem physikalischem Lesegerät oder anderem Interface und kann ein Token enthalten. Ein Token befindet sich im Slot (ist „present in the slot [RSAD_95]“), wenn ein kryptographisches Gerät sich im Lesegerät befindet bzw. an dieses Interface angeschlossen ist. Da Cryptoki eine logische Sicht dieser Dinge liefert, kann die physikalische Sichtweise von dieser Darstellung abweichen, so können z.B. mehrere Slots demselben physikalischem Gerät zugeordnet sein. Für die API ist lediglich wichtig, daß das System eine Anzahl Slots besitzt und Anwendungen mit allen sich in den Slots befindenden Token verbunden werden können.
Ein kryptographisches Gerät kann einige kryptographische Operationen entsprechend einem bestimmten Befehlssatz ausführen, wobei diese Befehle durch einen Standard-Gerätetreiber wie z.B. einen PCMCIA-Karten Treiber übermittelt werden. Cryptoki sorgt dafür, daß diese logisch alle gleich aussehen, unabhängig von der verwendeten Implementierung. Daher benötigen die Anwendungen kein direktes Interface zu den Gerätetreibern und auch keine Informationen darüber, welche Gerätetreiber benutzt werden. Da Cryptoki alle diese Details verbirgt, kann das „Gerät“ auch komplett als Software implementiert sein, die z.B. als Prozeß auf einem Server läuft, wobei keine Hardware notwendig ist [RSAD_95].
Cryptoki wird als Bibliothek (Library) implementiert, die die Funktionen in den Interfaces unterstützt und mit den Anwendungen gelinkt wird. Dabei kann eine Anwendung sowohl direkt mit Cryptoki gelinkt werden, oder Cryptoki wird als „Shared Library“ benutzt und die Anwendungen dynamisch gelinkt. Dabei hat die Verwendung als Shared Library den Vorteil, daß neue Libraries einfacher verwendet werden können, es ergeben sich aber aus dem Blickwinkel der Sicherheit einige Nachteile, da eine einfach zu ersetzende Library auch von einem potentiellen Angreifer durch eine gefälschte Library ersetzt werden kann, die geheime Daten mißbraucht. Daher ist aus Sicht der Sicherheit eine direkt mit der Anwendung gelinkte Library vorzuziehen. Unabhängig von diesen Betrachtungen ist das Programmierinterface zwischen den Anwendungen und Cryptoki jedoch das gleiche [RSAD_95].
Die unterstützten Geräte und Möglichkeiten sind von der jeweiligen Implementierung der Cryptoki-Library abhängig, der Standard definiert lediglich die Schnitt-

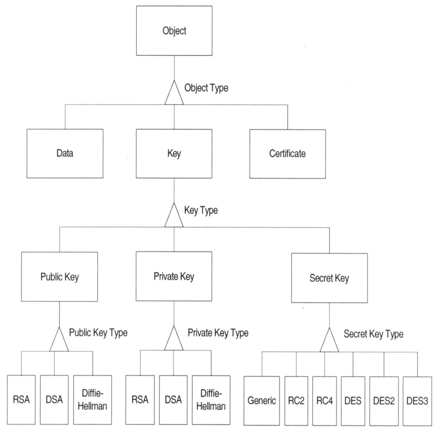

Abbildung 6.28: Logische Sicht eines Token (aus [RSAD_95])

stelle zur Library, nicht ihre Fähigkeiten. Nicht alle Libraries unterstützen alle in der Spezifikation definierten Funktionen, ebenso wie nicht alle Token sie implementieren [RSAD_95, Abbildung 5-1, S. 9].

Vergleich:

Cryptoki gleicht von Aufbau her den anderen Frameworks, benutzt aber einen gänzlich anderen Unterbau. Neu sind die Betrachtungen über die Art der Library, etwas derartiges gibt es bei den anderen Frameworks nicht.

6.9.1.3 Logische Sicht eines Token

Cryptokis logische Sicht eines Token ist die eines Geräts, welches Objekte speichert und kryptographische Funktionen ausführt. Cryptoki definiert drei Klassen von Objekten: Daten, Zertifikate und Schlüssel.

- Ein Datenobjekt wird von einer Anwendung definiert,
- ein Zertifikatobjekt speichert ein Zertifikat zu einem öffentlichen Schlüssel und
- ein Schlüsselobjekt speichert einen Verschlüsselungs-Schlüssel, d.h. einen öffentlichen Schlüssel (z.B. bei RSA, DSA oder Diffie-Hellman-Systemen), einen privaten Schlüssel (z.B. bei RSA, DSA oder Diffie-Hellman-Systemen) oder einen geheimen Schlüssel (z.B. bei RC2, RC4, DES).

Diese Sichtweise zeigt Abbildung 6.28, dabei werden die Schlüsseltypen angegeben, die in [RSAD_95]unterstützt werden, in zukünftigen Versionen können weitere Typen unterstützt werden.

Eine weitere Einordnung der Objekte erfolgt nach der Lebenszeit und Sichtbarkeit:

- Tokenobjekte („Token objects“) sind für alle mit dem Token verbundenen Anwendungen sichtbar und verbleiben nach der Sitzung oder dem Schließen der Verbindung im Token.
- Sitzungsobjekte („Session objects“) sind nur für die Anwendung sichtbar, die sie gebildet hat und werden bei Beendigung der Sitzung automatisch gelöscht.

Weitere Klassifikationen richten sich nach den Zugriffsmöglichkeiten:

- Öffentliche Objekte („Public objects") sind für alle Anwendungen sichtbar, die mit dem Token verbunden sind.
- Private Objekte („Privat objects") sind für eine Anwendung nur sichtbar, nachdem der Benutzer sich gegenüber dem Token durch eine PIN (Personal Identification Number) authentiziert hat.

Ein Token kann Objekte bilden und löschen, sie manipulieren, nach ihnen suchen und kryptographische Funktionen auf sie anwenden. Es ist möglich, daß ein Token Operationen parallel zur Anwendung ausführt, wenn das benutzte Gerät einen eigenen Prozessor besitzt. Zusätzlich können Token interne Zufallszahlengeneratoren besitzen.
Attribute charakterisieren verschiedene Instanzen eines Objekts. In Cryptoki gibt es allgemeine Attribute, die ausdrücken, ob ein Objekt privat oder öffentlich ist, und spezielle Attribute für bestimmte Objekte, wie z.B. den Modulus oder Exponenten eines RSA-Schlüssels.
Es ist wichtig, zwischen der logischen Sicht eines Tokens und seiner tatsächlichen Implementierung zu unterscheiden, da nicht alle kryptographischen Geräte das Konzept der Objekte benutzen oder alle kryptographischen Funktionen ausführen können. Viele Geräte werden eine feste Anzahl Speicherplätze für Schlüssel eines bestimmten Algorithmus besitzen und nur eine bestimmte Menge verschiedener Operationen ausführen können. Die Aufgabe von Cryptoki ist es dann, diese gegebenen Systeme in die logische Sichtweise der Token zu übersetzen und z.B. die Speicherplätze als Schlüsselobjekte zu verwalten[RSAD_95].
Vergleich:
Token lassen sich mit nichts in den anderen Frameworks vergleichen, da es diese Geräte dort nicht gibt. Sie könnten aufgrund der Namensgleichheit mit den Token der GSS-API verwechselt werden - dort handelt es sich aber um die übertragenen Daten, hier um Geräte, so das eine Verwechslung aufgrund der grundsätzlich anderen Art und Verwendung sehr unwahrscheinlich ist.

6.9.1.4 Benutzer von Cryptoki

Cryptoki unterscheidet zwei Typen von Benutzern [RSAD_95]:

- *Normale Benutzer*,
  die sich gegenüber dem Token durch eine PIN authentisieren müssen, bevor sie Zugriff auf private Objekte erhalten. Einige Token können es erfordern, daß sich die Benutzer authentisieren, bevor irgendeine kryptographische Funktion auf dem Token ausgeführt werden kann, unabhängig davon, ob private Objekte benutzt werden oder nicht. Der zweite Benutzertyp sind die
- Sicherheitsbeauftragten (*Security Officer* (SO)),
  die sich ebenso wie normale Benutzer authentisieren müssen, aber zusätzlich ein Token initialisieren können und die PIN eines normalen Benutzers setzen können. Zusätzlich dürfen sie einige öffentliche Objekte manipulieren. Ein normaler Benutzer kann sich nicht einloggen, bevor der SO seine PIN gesetzt hat.

Obwohl Cryptoki diese zwei Typen von Benutzern unterstützt, werden keine Aussagen über die Beziehungen zwischen den Typen gemacht: Ein SO und der Benutzer können identisch oder verschieden sein - diese Betrachtungen sind nicht Teil des Standards.
Vergleich:
Die SOs sind eine Art von Systemverwaltern oder Sicherheitsbeauftragten, die Cryptoki für die einfachen Benutzer verwalten.

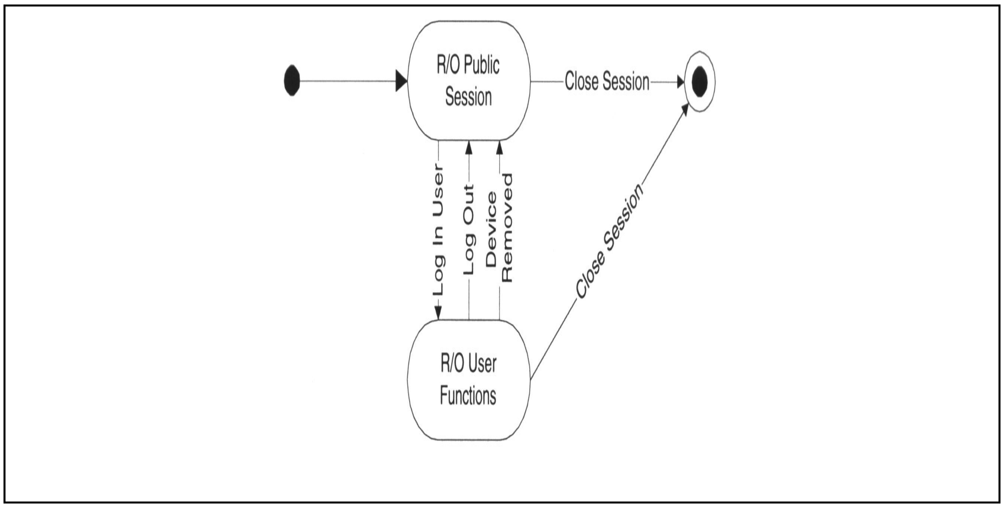

Abbildung 6.29: Zustände einer Nur-Lese-Sitzung (aus [RSAD_95])

6.9.1.4.1 PINs

Bezüglich PINs setzt Cryptoki nur voraus, daß es sich um Zeichenketten variabler Länge handelt. Jede Übersetzung in die Notwendigkeiten eines Geräts ist Aufgabe der Cryptoki Library.
Nicht betrachtet wird, wie die PINs gestaltet oder generiert werden.
Vergleich:
Auch die anderen Frameworks machen keine Aussagen über das Format der verwendeten Schlüssel, intern werden sie meist als Bitstrings verwaltet, wodurch sie sehr variabel gestaltet sein können.

6.9.1.5 Sitzungen

Cryptoki erfordert, daß eine Anwendung eine Sitzung mit einem Token eröffnet („open a session“), bevor die Anwendung Zugriff auf die Objekte und Funktionen des Tokens hat. Die Sitzung liefert die logische Verbindung zwischen dem Token und der Anwendung. Sitzungen werden unterschieden in Schreib/Lese-Sitzungen (read/write, R/W) und Nur-Lese-Sitzungen (read-only, R/O), wobei nach dem Zugriff auf die Tokenobjekte unterschieden wird. In beiden Sitzungstypen kann die Anwendung Sitzungsobjekte bilden, lesen, schreiben und löschen sowie Tokenobjekte lesen, lediglich in Schreib/Lese-Sitzungen kann eine Anwendung Tokenobjekte bilden, schreiben und löschen.
Nachdem eine Sitzung geöffnet wurde, hat die Anwendung Zugriff zu den öffentlichen Objekten des Tokens. Um Zugriff zu den privaten Objekten des Tokens zu erhalten, muß ein Benutzer sich einloggen und authentisieren.
Cryptoki erlaubt mehrere Sitzungen auf mehreren Token, eine Anwendung kann eine oder mehrere Sitzungen mit einem oder mehreren Token haben, und ein Token kann eine oder mehrere Sitzungen mit einer oder mehreren Anwendungen haben. Einige Token können nur eine bestimmte Anzahl an Schreib/Lese-Sitzungen zur gleichen Zeit erlauben.
Eine Sitzung kann sich in verschiedenen Zuständen befinden, siehe Abbildung 6.29 und 6.30. In [RSAD_95, Abschnitt 5.5] werden die Zustände und die Übergänge von einem Zustand in den anderen aufgeführt.
Vergleich:
Sitzungen gibt es in dieser oder ähnlicher Form bei allen Frameworks - neu ist hier der

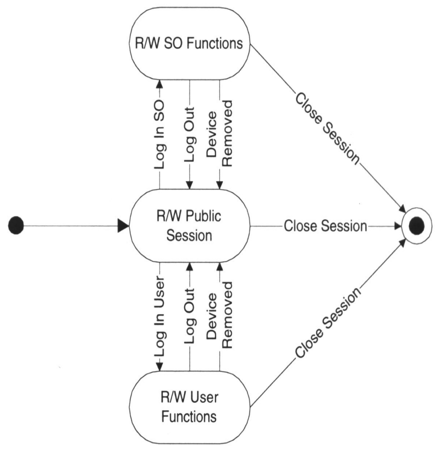

Abbildung 6.30: Zustände einer Schreib/Lese-Sitzung (aus [RSAD_95])

Verbindungsaufbau zu externen Geräten, nämlich den Token.

6.9.2 Sicherheitsbetrachtungen

Als Schnittstelle zu kryptographischen Geräten liefert Cryptoki die Grundlage für Sicherheit in einem Computer oder einem Kommunikationssystem. In [RSAD_95, Kapitel 6] werden einige Aussagen über die Sicherheit in und mit Cryptoki gemacht. So sind z.B. private Objekte sowie teilweise auch die kryptographischen Funktionen in den Token nur nach Eingabe einer PIN zugänglich, und für als „Sensitiv" markierte Objekte gibt es maximalen Schutz: Sie können nicht aus dem Token gelesen werden und auch nicht durch kryptographische Funktionen exportiert werden. Es wird erwartet, daß der Zugriff zu privaten und sensitiven Objekten durch andere als Cryptoki (z.B. durch Reverse Engineering) schwierig ist.

Wenn das Gerät keine manipulationssichere Umgebung (tamper-proof environment) und keinen geschützten Speicher für private und sensitive Objekte besitzt, kann es die Daten mit einem Hauptschlüssel (master key) verschlüsseln, der z.B. aus der PIN des Benutzers abgeleitet wird. Wie der Schutz privater Objekte erfolgt, ist der Implementierung des Geräts überlasse und nicht Bestandteil der Cryptoki-Spezifikation.

Werden die eben gemachten Aussagen beachtet, können Anwendungen so entwickelt werden, daß die Token eine adäquate Sicherheit für die von der Anwendung verwalteten Objekte garantieren können [RSAD_95].

Kryptographie ist nur ein Element der Sicherheit, und das Token ist nur eine Komponente eines Systems. Wenn das Token selbst sicher ist, muß auch die Sicherheit des Betriebssystems betrachtet werden, über das die Anwendung mit dem Token kommuniziert und z.B. auch die PIN überträgt. Es ist möglich, daß dabei durch bösartige Anwendungen die PIN abgehört oder Kommandos verfälscht werden. Daher ist es wichtig, daß das System sicher gegen derartige Angriffe ist.

Vergleich:
Diese Sicherheitsbetrachtungen sind das, was man sinnvollerweise erwarten würde: Die allgemein üblichen Forderungen, angepaßt an die besonderen Umstände, die sich durch die Token ergeben.

6.9.3 Objekte, Funktionen und Mechanismen

In [RSAD_95, Kapitel 8 bis 9] werden die vorhandenen Objekt, Funktionen und Mechanismen detailliert aufgeführt und beschrieben.
Für die vorhandenen Funktionen sei auf die Tabellen 7.1, 7.3 und 7.2 verwiesen.
Vergleich:
Zum Vergleich siehe ebenfalls die Tabellen.

6.10 ISO/IEC 10181: Information technology - Open Systems Interconnection - Security frameworks for open systems

Die ISO (Abschnitt 2.3.1) und das IEC (Abschnitt 2.3.2) haben in ihrem gemeinsamen Technischen Komitee JTC 1, Subkomitee SC 21, in Zusammenarbeit mit der ITU-T (siehe Seite 2.3.3.1), die Norm *ISO/IEC 10181: Information technology - Open Systems Interconnection - Security frameworks for open systems* entwickelt. Die Norm besteht aus den Teilen

- Part 1: Overview,
- Part 2: Authentication Framework,
- Part 3: Access Control Framework,
- Part 4: Non-repudiation Framework,
- Part 5: Confidentiality Framework,
- Part 6: Integrity Framework und
- Part 7: Security audit and alarms framework,

von denen im folgenden Part 1, Overview, näher betrachtet wird.

6.10.1 Überblick

Die Norm ISO/IEC 10181 befaßt sich mit der Sicherheit in offenen Systemen, worunter Gebiete wie Datenbanken, Verteilte Anwendungen und OSI verstanden werden. Das Sicherheitsframework befaßt sich sowohl mit Datenelementen als auch mit Operationen, nicht jedoch mit Protokollelementen, die benutzt werden, um spezifische Sicherheitsdienste zu erhalten.
Die Norm beginnt mit einer Reihe von Definitionen, wobei zum einen auf andere Normen verwiesen wird, zum anderen aber auch eigene Definitionen angegeben werden.
Alle Frameworks der Norm ISO/IEC 10181 werden im folgenden kurz beschrieben:

6.10.1.1 Teil 2: Authentikation

Teil 2 von ISO/IEC 10181 beschreibt alle Aspekte der Authentikation im Rahmen offener Systeme, die Zusammenhänge der Authentikation mit den anderen Frameworks, wie z.B. der Zugriffskontrolle, sowie die Verwaltungsfunktionen für Authentikation.
Das Authentikations-Framework

- definiert die Basiskonzepte der Authentikation,
- identifiziert die möglichen Klassen von Authentikationsmechanismen,

- definiert die Dienste für diese Klassen,
- identifiziert die funktionalen Anforderungen für Protokolle für diese Klassen und
- identifiziert allgemeine Verwaltungsfunktionen für die Authentikation.

Das Authentikations-Framework steht an der Spitze einer Hierarchie von Authentikationsstandards, die Konzepte, Nomenklatur und Klassifikation von Authentikationsverfahren liefern. Direkt unter ihm befinden sich Standards wie die Norm ISO/IEC 9798 (Entity Authentication Mechanisms), beschreiben einen Teil dieser Funktionen detaillierter. Am Boden der Hierarchie stehen Normen wie ITU-T Recommendation X.509 (Directory Authentication Frameworks), die diese Funktionen für bestimmte Anwendungen oder Anforderungen verwenden.
Das Authentikations-Framework beschreibt ein Modell für Authentikation, eine Anzahl Phasen, in die Authentikationsaktivitäten eingeteilt werden können, die Benutzung vertrauenswürdiger Dritter (trusted third party), die Benutzung von Authentikationszertifikaten für den Austausch von Authentikationsinformationen, einen generischen Authentikationsdienst auf Basis dieser Phasen und fünf Klassen von Authentikationsmechanismen, die die generischen Authentikationsdienste liefern. Dabei werden auch der Schutz gegen eine Enthüllung authentisierter Informationen sowie die Enthüllung oder der Replay gegenüber denselben und/oder anderen Testern betrachtet.
Vergleich:
Hier gibt es nichts neues im Vergleich zu den anderen Frameworks.
Etwas seltsam ist die letzte Bemerkung: Eine Enthüllung gegenüber denselben Tester würde bedeuten, jemanden etwas zu zeigen, was er schon kennt - was aber keine Gefahr darstellen kann, da er ja keine neuen Informationen erhält. Auch ein Replay ist in diesem Zusammenhang keine Gefahr: Was man weiß, weiß man - unabhängig davon, ob es einmal oder mehrmals vorgelegt wird.
Gefährlich könnte ein Replay gegenüber anderen Testern sein, wenn der ursprüngliche Tester dies nicht wünscht, vergleiche hierzu die nichtherumzeigbaren Unterschriften, z.B. in [Pfit_93]

6.10.1.2 Teil 3: Zugriffskontrolle

Teil 3 von ISO/IEC 10181 beschreibt alle Aspekte der Zugriffskontrolle im Rahmen offener Systeme, also für die Bereiche Benutzer–Prozeß, Benutzer–Daten, Prozeß–Prozeß und Prozeß–Daten. es werden die Beziehung zu anderen Sicherheitsfunktionen wie z.B. Authentikation und Audit sowie die benötigten Verwaltungsfunktionen betrachtet.
Das Zugriffskontroll-Framework

- definiert die Basiskonzepte der Zugriffskontrolle,
- demonstriert wie diese Basiskonzepte für spezielle Aufgaben verwendet werden können,
- definiert diese Dienste und die dazugehörigen Zugriffskontrollmechanismen,
- identifiziert die funktionalen Anforderungen für Protokolle zur Unterstützung dieser Dienste und Mechanismen,
- identifiziert die Anforderungen für die Verwaltung dieser Dienste und Mechanismen und
- betrachtet die Interaktion von Zugriffskontrollfunktionen und anderen Sicherheitsfunktionen.

Das Zugriffskontroll-Framework beschreibt ein Modell für Zugriffskontrolle, eine Anzahl Phasen, in die Zugriffskontrollaktivitäten eingeteilt werden können, einen generischen Zugriffskontrolldienst auf der Grundlage dieser Phasen sowie drei Klassen von Zugriffskontrollmechanismen, die die generischen Zugriffskontrolldienste bereitstellen. Dies umfaßt Zugriffskontrolllisten, Capabilities und Etiketten (Labels).
Vergleich:
Hierbei handelt es sich um die klassische Zugriffskontrolle, die vergleichbar auch in einigen der anderen Frameworks vorkam.

6.10.1.3 Teil 4: Nichtabstreitbarkeit

Teil 4 von ISO/IEC 10181 verfeinert und erweitert die Konzepte für Nichtabstreitbarkeit, die in CCITT REcommendation X.800 und ISO 7498-2 beschrieben werden und definiert ein Framework für die Entwicklung und Verwendung dieser Dienste.
Das Nichtabstreitbarkeits-Framework

- definiert die Basiskonzepte für Nichtabstreitbarkeit,
- definiert allgemeine Nichtabstreitbarkeitsdienste,
- identifiziert mögliche Mechanismen für die Bereitstellung von Nichtabstreitbarkeitsdiensten und
- identifiziert allgemeine Verwaltungsfunktionen für diese Mechanismen.

Vergleich:
Nichtabstreitbarkeit gibt es außer hier nur noch in SEMPER.

6.10.1.4 Teil 5: Vertraulichkeit

Zweck der Vertraulichkeitsdienste ist der Schutz von Informationen vor unbefugter Veröffentlichung. Dieses Framework betrachtet die Vertraulichkeit von Informationen für Abfragen, Übertragungen und Verwaltung.
Das Vertraulichkeits-Framework

- definiert die Basiskonzepte für Vertraulichkeit,
- identifiziert mögliche Klassen von Vertraulichkeitsmechanismen,
- definiert Einzelheiten für jeder dieser Klassen,
- identifiziert die notwendigen Verwaltungsfunktionen für diese Mechanismen und
- betrachtet die Interaktion von Vertraulichkeitsmechanismen und den sie unterstützenden Diensten mit anderen Sicherheitsfunktionen.

Einige der in diesem Framework beschriebenen Prozeduren erhalten Vertraulichkeit durch die Anwendung kryptographischer Techniken. Die Verwendung des Frameworks ist nicht von der Benutzung bestimmter Algorithmen abhängig, auch wenn einige Klassen von Vertraulichkeitsmechanismen auf die Fähigkeiten bestimmter Algorithmen angewiesen sein können.
Vergleich:
Auch hier gibt es nichts neues im Vergleich zu den anderen betrachteten Frameworks.

6.10.1.5 Teil 6: Integrität

Dieses Framework befaßt sich mit der Integrität von Daten in Imformationretrieval, Übertragung und Verwaltung.
Das Integritäts-Framework

- definiert die Basiskonzepte für Integrität,
- identifiziert mögliche Klassen von Integritätsmechanismen,
- definiert Details für jede dieser Klassen,
- identifiziert Verwaltungsfunktionen für diese Klassen und
- betrachtet die Interaktion zwischen Integritätsmechanismen und anderen Sicherheitsfunktionen.

Auch in diesem Framework werden von einigen Prozeduren kryptographische Techniken verwendet, hierfür gilt das gleiche wie für Teil 5.
Die hier betrachtete Integrität ist definiert als Konstanz der Datenwerte, nicht als Konstanz der dadurch repräsentierten Informationen. Andere Formen der Invarianz werde nicht betrachtet.
Vergleich:
Auch hier gibt es nichts neues im Vergleich zu den anderen betrachteten Frameworks. Etwas seltsam erscheint die letzte Aussage: Wenn der Behälter, d.h. die Datenwerte, unverändert ist, muß auch der Inhalt, d.h. die Informationen, unverändert sein, da niemand an den Inhalt heran kann, ohne den Behälter zu verändern.

6.10.1.6 Teil 7: Sicherheitsprüfung und Alarm

Dieses Framework

- definiert die Basiskonzepte für Sicherheitsprüfungen und Alarmen,
- liefert ein allgemeines Modell dafür und
- identifiziert die Zusammenhänge zwischen den Sicherheitsprüfungen und Alarmen und den anderen Sicherheitsdiensten.

Ebenso wie die anderen Sicherheitsdienste, kann eine Sicherheitsprüfung nur im Rahmen einer Sicherheitspolitik stattfinden. Die Sicherheitspolitik wird von einer Sicherheitauthorität in deren Sicherheitsbereich definiert. Alle Standards, die Mechanismen auf Basis dieses Frameworks definieren, sollten die Möglichkeit besitzen, verschiedene Sicherheitspolitiken zu benutzen.
Vergleich:
Hierzu gibt es nichts vergleichbares in den anderen Frameworks.

6.10.1.7 Schlüsselverwaltung

Das Schlüsselverwaltungs-Framework, Teil 1 von ISO/IEC 11770, hat eine enge Beziehung zu den Frameworks der Norm ISO/IEC 10181, eine Schlüsselverwaltung wird daher hier nicht betrachtet.
Vergleich:
Ein Vergleich entfällt, da die Schlüsselverwaltung nicht Teil von ISO/IEC 10181 ist und nur dies hier betrachtet wird.

6.10.2 Gemeinsame Konzepte für alle Teile

Viele Konzepte werden in mehr als einem Framework verwendet, so daß sie einmal in Teil 1, Überblick, definiert werden.
Es handelt sich dabei um Angaben zu

- Sicherheitsinformationen (Security information),
  die benötigt werden, um Sicherheitsfunktionen zu definieren, wie z.B. die Regeln einer Sicherheitspolitik oder spezifische Informationen für bestimmte Funktionen,
- Sicherheitsbereiche (Security domain),
  eine Menge von Elementen unter einer gegebenen Sicherheitspolitik, die von einer einzelnen Sicherheitsauthorität verwaltet werden,
- Sicherheitspolitiken für bestimmte Sicherheitsdienste,
- vertrauenswürdigen Instanzen (Trusted entities),
- Vertrauen (trust) und
- vertrauenswürdigen Dritten (trusted third parties).

Vergleich:
Auch hier gibt es nichts, was nicht schon in den anderen Frameworks in der einen oder anderen Form vorkam. Neu ist die ausführliche Definition von Vertrauen und Vertrauenswürdigkeit.
Außerdem werden noch generische Sicherheitsinformationen definiert, dabei handelt es sich um

- Sicherheitsetiketten (Security labels),
  einer Menge von Sicherheitsattributen, die einem Element, Kommunikationskanal oder Datenelement zugeordnet sind,
- Kryptographische Checkwerte,
- Sicherheitszertifikate und
- Sicherheitstoken,
  einer Menge von Daten, die gemeinsam durch einen oder mehrere Sicherheitsdienste geschützt werden.

Vergleich:
Hier gibt es ebenfalls nicht neues, lediglich eine neu Bedeutung von Token: Nach zu übertragenden Daten (GSS-API) und kryptographischen Geräten (Cryptoki) sind es nun geschützte Daten, von daher aber wieder mit den Token der GSS-API vergleichbar.
Zusätzlich werden noch einige grundlegende Verwaltungsfunktionen beschrieben.
Letztendlich wird noch kurz die Interaktion zwischen verschiedenen Sicherheitsmechanismen beschrieben.

6.10.3 Schlußbemerkungen

Für die Erstellung der Tabellen in Kapitel 7 wurden zusätzlich zu Teil 1 auch die anderen Teile der Norm verwendet.

Kapitel 7

Vergleich der Funktionen der Frameworks

Im folgenden werden Funktionen der untersuchten Frameworks in Tabellenform zusammengefaßt. Tabelle 7.1 vergleicht allgemeine Aussagen, während in Tabelle 7.2 kryptographischen Funktionen und in Tabelle 7.3 Verwaltungsfunktionen zusammengefaßt werden.
Da TINA keine eigene Sicherheitsarchitektur besitzt, sondern wahrscheinlich auf CORBA aufsetzen wird, gelten die Aussagen für CORBA ebenso für TINA.

7.1 Erklärungen zu den Tabellen

7.1.1 Tabelle 7.1: Allgemeines

Bei „Sicherheitsfunktionen" wird angegeben, ob die Implementierung der Sicherheitsfunktionen Teil des Frameworks ist oder ob die Sicherheitsfunktionen von externen Systemen zur Verfügung gestellt werden müssen. In der Zeile „Datenübertragung" wird aufgelistet, ob die Übertragung der Daten unter Kontrolle des Frameworks erfolgt oder nicht. Die Zeile „Disput" listet auf, ob ein Disput im Framework möglich ist, nur außerhalb des Systems erfolgen kann oder etwa gar nicht möglich ist. Unter „Anonymität" wird erfaßt, ob das Framework auch anonyme Kommunikation erlaubt, in „Übertragene Datentypen" wird aufgeführt, was für Datentypen von den Frameworks übertragen werden können, bzw. genauer: Welche Datentypen geschützt werden können, d.h. als Eingaben für die Funktionen vorgesehen sind.

7.1.2 Tabelle 7.2: Kryptograpische Funktionen

Hier wird aufgelistet, welche Typen kryptographischer Funktionen (Authentikation, Signaturen, symmetrische Verschlüsselung, asymmetrische Verschlüsselung, (Pseudo)zufallsgeneratoren, Hashfunktionen) zur Verfügung stehen. Bei Nichtabstreitbarkeit wird erfaßt, ob es Protokolle dafür gibt, unter „Höhere Protokolle" wird die Existenz eventuell vorhandener höherer Protokolle angegeben, und unter „Einfügen neuer Funktionen" wird aufgeführt, ob es möglich ist, auf einfache Art und Weise neue, beim Entwurf des Frameworks noch nicht berücksichtigte Funktionen einzufügen. Dies ist in der Regel immer dann der Fall, wenn generische Aufrufe zur Verfügung stehen, die nicht auf die Benutzung bestimmter Funktionen zugeschnitten sind.

7.1.3 Tabelle 7.3: Verwaltungsfunktionen

Bei „Manager für Sicherheitsfunktionen“ wird angegeben, ob ein Manager vorhanden ist, der die Sicherheitsfunktionen verwaltet. In der Spalte „Verwaltung verschiedener Systeme“ wird angegeben, wie zwischen verschiedenen Systemen und Funktionen ausgewählt werden kann. Es wird außerdem angegeben, welche Funktionen zur Verwaltung der Sicherheitsfunktionen zur Verfügung stehen, d.h. im einzelnen, ob eine Zugriffskontrolle, Schlüssel- und Zertifikatverwaltung vorhanden ist. Dabei bedeutet Zugriffskontrolle den Zugriff auf die Funktionen des Frameworks sowie das Netzwerk, Schlüsselverwaltung umfaßt die Verwaltung privater, öffentlicher und geheimer Schlüssel bzw. den damit vergleichbaren Daten, falls ein Framework keine Schlüssel besitzt. Die Zertifikatverwaltung erfaßt die Verwaltung, Speicherung etc. von Zertifikaten bzw. den damit vergleichbaren Datentypen.

7.1.4 Die Tabellen

Funktion \ Framework	SEMPER	GSS API	GCS API	CORBA (TINA)	CDSA	Cryptoki	ISO/IEC 10181
Verwendungszweck	Electronic Commerce	Sichere Kommunikation	Kryptographische Funktionen	verteile Zugriffskontrolle	Electronic Commerce	Kryptographische Funktionen mit Geräten	Kryptographische Funktionen für offene Systeme
Implementierungssprache	Beispielimplementierung in C	unabhängig, Bindings für C	unabhängig, Beispiele in C	keine Angabe	Beispiele in C	unabhängig, Beispiele in C	unabhängig
Sicherheitsfunktionen	durch interne Servicemodule	durch tiefere Schichten	durch externe Funktionen	durch externe Funktionen	durch externe Funktionen	durch externe Hardware (Smartcard etc.)	durch externe Funktionen
Datenübertragung	Funktionen, um ComPoints und Channels aufzubauen und zu benutzen	Übertragung durch den Aufrufer ohne Unterstützung der API	keine Angaben	im Framework	keine Angaben	keine Angaben, aufgrund der Konstruktion nicht im Framework	keine Angaben
Disput	im Framework	nicht vorgesehen und auch nicht möglich, da dann Kontext fehlt	nicht vorgesehen, wahrscheinlich extern möglich	keine Angaben	keine Angaben, wahrscheinlich extern möglich	keine Angaben, wahrscheinlich extern möglich	keine Angaben, wahrscheinlich teilweise extern möglich
Anonymität	ja	teilweise	nein	nein	nein	nein	nein
Übertragene Datentypen	Container (eigener Datentyp)	Bytestring	Bytestring	-	Bytestring	Objekte, z.B. Bytestring	keine Angaben

Tabelle 7.1: Allgemeine Vergleiche der Frameworks

Funktion \ Framework	SEMPER	GSS API	GCS API	CORBA (TINA)	CDSA	Cryptoki	ISO/IEC 10181
Authentikation	ja	ja	ja	ja	ja	ja	ja
Signaturen	ja	nein	ja	ja	ja	ja	ja
symmetrische Verschlüsselung	ja	keine Angaben	ja	keine Angaben	ja	ja	ja
asymmetrische Verschlüsselung	ja	keine Angaben	ja	keine Angaben	ja	ja	ja
(Pseudo)zufallsgeneratoren	ja (Crypto-Block)	nein	ja	nein	ja	ja	nein
Hashfunktionen	ja	nein	ja	nein	nein	ja	ja
Nichtabstreitbarkeit	ja	nein	ja	ja	nein	nein	ja
Höhere Protokolle	ja, z.B. Fair Exchange	nein	nein	nein	nein	nein	nein
Einfügen neuer Funktionen	ja	ja	ja	ja	ja (Add-in)	ja	keine Angaben

Tabelle 7.2: Auflistung der in den Frameworks vorhandenen kryptographischen Funktionen

Funktion \ Framework	SEMPER	GSS API	GCS API	CORBA (TINA)	CDSA	Cryptoki	ISO/IEC 10181
Manager für Sicherheitsfunktionen	SecCom Manager	nein, nur Referenzverwaltung und Kontextaufbau	Session Management	durch ORB	Systemsicherheit und CSSM	nein	nein
Verwaltung verschiedener Systeme	Sicherheitsattribute	Referenzen	Kryptographischer Kontext	keine Angaben	durch CSSM	keine Angaben	keine Angaben
Zugriffskontrolle	ja	keine Angaben	ja	ja	ja	ja	ja
Schlüsselverwaltung	ja	ja	ja	keine Angaben	ja	ja	nein (aber durch andere Norm)
Zertifikatverwaltung	ja	ja	nein	keine Angaben	ja	ja	ja

Tabelle 7.3: Auflistung der in den Frameworks vorhandenen Verwaltungsfunktionen

Anhang A

Mitglieder des CEN

Land	Organisation	Gewicht
Belgien	Institut Belge de Normalisation (IBN)	5
Dänemark	Dansk Standard (DS)	3
Deutschland	Deutsches Institut für Normung e.V. (DIN)	10
Finnland	Suomen Standardisoimisliito (SFS)	3
Frankreich	Association Francaise de Normalisation (AFNOR)	10
Griechenland	Hellenic Organization for Standardization (ELOT)	5
Irland	National Standards Authority of Ireland (NSAI)	3
Italien	Ente Nazionale Italiano di Unificazione (UNI)	10
Island	Icelandic Council for Standardization (STRI)	1
Luxemburg	Inspection du Travail et des Mines (ITM)	2
Niederlande	Nederlands Normalisatie-Instituut (NNI)	5
Norwegen	Norges Standardiseringsforbund (NSF)	3
Österreich	Östereichisches Normungsinstitut (ON)	5
Portugal	Instituto Portuges da Qualidade (IPQ)	5
Schweden	Standardiseringen i Sverige (SIS)	5
Schweiz	Schweizerische Normen-Vereinigung (SNV)	5
Spanien	Asociacion Espanola de Normalizacion y Certificacion (AENOR)	8
Tschechische Republik	Czech Office for Standards, Metrology and Testing (COSMT)	?
Vereinigtes Königreich	British Standards Institution (BSI)	10

Tabelle A.1: Mitgliedsländer des CEN nach [CEN_91]

Land	Organisation
Albanien	Directorate of Standardization and Quality (DSC)
Bulgarien	Committee for Standardization and Metrology (CSM)
Estland	National Standards Board of Estonia (EVS)
Kroatien	State Office of Standardization and Metrology (DZNM)
Lettland	Department of Quality Management and Structure Development
Litauen	Lithuanian Standards Board (LST)
Polen	Polish Committee for Standardization (PKN)
Rumänien	Instiutul Roman de Standardizare (IRS)
Slowakei	Slovak Office of Standardization, Metrology and Testing (UNMS)
Slowenien	Standards and Metrology Institute of the Republic of Slovenia (SMIS)
Tschechische Republik	Czech Office for Standards, Metrology and Testing (COSMT)
Türkei	Turkish Standards Institution (TSE)
Ungarn	Hungarian Standards Institution (MSZH)
Zypern	Cyprus Organization for Standards (CYS)

Tabelle A.2: CEN Angegliederte Normungsinstitute nach [CEN_94]

Organisation	
ANEC	European Association for the co-ordination of consumer representation in standardization (Europäische Vereinigung für die Koordinierung der Verbrauchervertretung)
CEFIC	European Chemical Industry Council
ECMA	European Computer Manufacturers Association
FIEC	European Construction Industry Federation (Verband der Europäischen Bauwirtschaft)
TUTB	European Trade Union Technical Bureau for Health and Safety (Europäisches Technikbüro der Gewerkschaften für Gesundheit und Sicherheit)

Tabelle A.3: CEN Assoziierte nach [CEN_94]

Organisation	
AECMA	Association Europeenne des Constructeurs de Material Aerospatial (Europäischer Verband der Hersteller von Luft- und Raumfahrtgerät)
ECISS	European Committee for Iron and Steel Standardization (Europäisches Komitee für die Eisen- und Stahlnormung)
EWOS	European Workshop for Open Systems
WE/EB	Western European EDIFACT Board

Tabelle A.4: CEN „Assoziierte Organisationen“ (ASBs) nach [CEN_94]

Anhang B

Mitglieder der ISO

Land	Organisation (Abkürzung)
Ägypten	Egyptian Office for Standardization and Quality Control (EOS)
Äthiopien	Ethiopian Authority for Standardization (EAS)
Albanien	Dretoria e Standardizimit dhe Cilesie (DSC)
Algerien	Institut algérien de normalisation et de propriété industrielle (INAPI)
Argentinien	Instituto Argentino der Normalización (IRAM)
Armenien	Department for Standardization, Metrology and Certiciation (SARM)
Belarus	Committee for Standardization, Metrology and Certiciation (BELST)
Belgien	Institut belge de normalisation (IBN)
Bosnien - Herzegowina	Institute for Standardization, Metrology and Patents (BASMP)
Brasilien	Associaçao Brasileira de Normas Técnicas (ABNT)
Bulgarien	Committee for Standardization and Metrology (BDS)
Chile	Instituto Nacional de Normalización (INN)
China	China State Bureau of Technical Supervision (CSBTS)
Costa Rica	Instituto de Normas Técnicas de Costa Rica (INTECO)
Dänemark	Dansk Standard (DS)
Deutschland	DIN Deutsches Institut für Normung (DIN)
Equador	Instituto Ecuatoriano de Normalización (INEN)
Finnland	Finnish Standards Association SFS (SFS)
Frankreich	Association française de normalisation (AFNOR)
Ghana	Ghana Standards Board (GSB)
Griechenland	Hellenic Organization for Standardization (ELOT)
Großbritannien	British Standards Institution (BSI)
Indien	Bureau of Indian Standards (BIS)
Indonesien	Dewan Standardiasi Nasional - DSN (DSN)
Iran	Institute of Standards and Industrial Research of Iran (ISIRI)
Irland	National Standards Authority of Ireland (NSAI)
Island	Icelandic Council for Standardization (STRI)
Israel	Standards Institution of Israel (SII)
Italien	Ente Nazionale Italiano di Unificazione (UNI)
Jamaika	Jamaica Bureau of Standards (JBS)
Japan	Japanesw Indurstrial Standards Committee (JISC)
Jugoslawien	Savezni zavod za standardizaciju (SZS)
Kanada	Standards Council of Canada (SCC)
Kenia	Kenya Bureau of Standards (KEBS)
Kolumbien	Instituto Columbiano de Normas Técnicas y Certificación (ICONTEC)

Tabelle B.1: Vollmitglieder der ISO nach [http://www.iso.org]

Korea (VR)	Committee for Standardization of the Democratic People's Republic of Korea (CSK)
Korea	Korean National Institute of Technology and Quality (KNITQ)
Kroatien	State Office for Standardization and Metrology (DZNM)
Kuba	Oficina Nacional de Normalización (NC)
Libyen	Libyan National Centre for Standardization and Metrology (LNCSM)
Malaysia	Department of Standards Malaysia (DSM)
Marokko	Service de normalisation industrielle marocaine (SNIMA)
Mauritius	Mauritius Standards Bureau (MSB)
Mazedonien	Zavod za standardizacija i metrologija (ZSM)
Mexiko	Dirección General de Normas (DGN)
Mongolei	Mongolian National Centre for Standardization and Metrology (MNCSM)
Neuseeland	Standards New Zealand (SNZ)
Niederlande	Nederlands Normalisatie-institut (NNI)
Nigeria	Standards Organisation of Nigeria (SON)
Norwegen	Norges Standardiseringsforbund (NSF)
Pakistan	Pakistan Standards Institution (PSI)
Panama	Comisión Panameña de Normas Industriales y Técnicas (COPANIT)
Philipinen	Bureau of Product Standards (BPS)
Polen	Polish Committee for Standardization (PKN)
Portugal	Instituto Português da Qualidade (IPQ)
Rumänien	Institutul Român de Standardizare (IRS)
Rußland	Committee of the Russian Federation for Standardization, Metrology and Certification (GOST R)
Saudi Arabien	Saudi Arabian Standards Organization (SASO)
Schweden	SIS - Standardiseringen i Sverige (SIS)
Schweiz	Swiss Association for Standardization (SNV)
Singapur	Singapore Productivity and Standards Board (PSB)
Simbabwe	Standards Association of Zimbabwe (SAZ)
Slowakei	Slovak Office of Standards, Metrology and Testing (UNMS)
Slowenien	Standards and Metrology Institute (SMIS)
Spanien	Asociación Española de Normalización y Certificación (AENOR)
Sri Lanka	Sri Lanka Standards Institution (SLSI)
Südafrika	South African Bureau of Standards (SABS)
Syrien	Syrian Arab Organization for Standardization and Metrology (SASMO)
Tansania	Tanzania Bureau of Standards (TBS)
Thailand	Thai Industrial Standards Institute (TISI)
Tschechische Republik	Czech Office for Standards, Metrology and Testing (COSMT)
Trinidad und Tobago	Trinidad and Tobago Bureau of Standards (TTBS)
Tunesien	Institut national de la normalisation et de la propriété industrielle (INNORPI)
Türkei	Türk Standardlari Enstiüsü (TSE)
Ukraine	State Committee of Ukraine for Standardization, Metrology and Certification (DSTU)
Ungarn	Magyar Szabványügyi Testület (MSZT)
Uruquay	Instituto Uruquayo de Normas Técnicas (UNIT)
USA	American National Standards Institute (ANSI)
Usbekistan	Uzbek State Centre for Standardization, Metrology and Certification (UZGOST)
Venezuela	Comisión Venezolana de Normas Industriales (COVENIN)
Vietnam	Directorate for Standards and Quality (TCVN)

Tabelle B.1: Vollmitglieder der ISO nach [http://www.iso.org]

Zypern	Cyprus Organization for Standards and Control of Quality (CYS)

Tabelle B.1: Vollmitglieder der ISO nach [http://www.iso.org]

Land	Organisation (Abkürzung)
Bahrain	Directorate of Standards and Metrology (BSMD)
Barbados	Barbados National Standards Institution (BNSI)
Botswana	Botswana Bureau of Standards (BOBS)
Brunei	Construction Planning and Reseach Unit (CPRU)
Elfenbeinküste	CODINORM (CODINORM)
El Salvador	Consejo Nacional de Ciencia y Tecnología (CONACYT)
Estland	National Standards Board of Estonia (EVS)
Guatemala	Comision Guatemalteca de Normas (COGUANOR)
Hong Kong	Industry Department (keine Angabe)
Jordanien	Jordanian Institution for Standards and Metrology (JISM)
Kuwait	Public Authority for Industry (keine Angabe)
Kyrgyzstan	State Inspection for Standardization and Metrology (KYRGYZST)
Letland	Latvian National Center of Standardization and Metrology (LVS)
Libanon	Lebanese Standards Institution (LIBNOR)
Litauen	Lithuanian Standards Board (LST)
Malawi	Malawi Bureau of Standards (MBS)
Malta	Malta Standardisation Authority (MSA)
Moldavien	Department of Standards, Metrology and Technical Supervision (MOLDST)
Mosambique	National Institute of Standardization and Quality (INNOQ)
Nepal	Nepal Bureau of Standards and Metrology (NBSM)
Oman	Directorate General for Specification and Measurements (DGSM)
Papua / Neu Guinea	National Institute of Standards and Industrial Technology (NISIT)
Paraquay	Instituto Nacional de Tecnología y Normalización (INTN)
Peru	Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI)
Qatar	Department of Standards, Measurements and Consumer Protection (keine Angabe)
Turkmenistan	Major State Inspection of Turkmenistan (MSIT)
Uganda	Uganda National Bureau of Standards (UNBS)
Vereinigte Arabische Emirate	Directorate of Standardization and Metrology (SSUAE)

Tabelle B.2: Assoziierte Mitglieder (correspondent members) der ISO nach [http://www.iso.org]

Land	Organisation (Abkürzung)
Antiqua und Barbuda	Antiqua and Barbuda Bureau of Standards (ABBS)
Benin	Direction de la Promotion de la Qualité et du Conditionnement des Produits (DPQC)
Bolivien	Instituto Boliviano de Normalización y Calidad (IBNORCA)
Dominikanische Republik	Dirección General de Normas y Sistemas de Calidad (DIGENOR)
Fitschi	Fiji Trade Standards and Quality Control Office (keine Angabe)
Grenada	Grenada Bureau of Standards (GDBS)

Tabelle B.3: Teilmitglieder (subscriber members) der ISO nach [http://www.iso.org]

Guinea	Guyana National Bureau of Standards (GNBS)
Kambodscha	Ministry of Industry, Mines and Energy (keine Angabe)
Namibia	Namibia Standards Information and Quality Office (NSIQO)
St. Lucia	Saint Lucia Bureau of Standards (SLBS)

Tabelle B.3: Teilmitglieder (subscriber members) der ISO nach [http://www.iso.org]

Anhang C

Übersicht über alle gefundenen Normen

Im folgenden werden alle für diese Diplomarbeit erfaßten Normen aufgeführt. Die Quellen wurden mit der Literaturdatenbank Lina verwaltet.

C.1 Verwendete Quellen

Der erste Ansatz zur Suche nach Standards und Normen für den Bereich Sicherheit, Datenschutz un Kryptographie war die Benutzung von Suchmaschinen für das World Wide Web, wobei davon ausgegangen wurde, daß sich dort Standards zum Thema besonders leicht finden lassen würden, eben weil sie dort auch verwendet werden. Dieser Versuch schlug fehl - auch mit starken Einschränkungen bei den Suchbegriffen wurden mehr Fundstellen ausgegeben (minimal mehrere 10.000, darunter sehr viele unbrauchbare), als sich mit vertretbarem Aufwand auf Brauchbarkeit überprüfen ließen. Der nächste Ansatz war dann die Benutzung der PERINORM-Datenbank in der Technischen Informationsbibliothek, Hannover. Diese CD-ROM Datenbank ist speziell für die Suche nach Patenten und Normen ausgelegt und lieferte bei der Suche nach Suchbegriffen wie „Datenschutz", „Sicherheit", „Kryptographie" etc. sowie nach Aussortieren der Ergebnisse „von Hand" letztendlich 96 Fundstellen. Außerdem wurde der „ISO/TC 68 Catalogue of Security Related Standards" ausgewertet. Anhand der gefundenen Normen wurde wiederum im WWW nach weiteren Standards gesucht, z.B. indem die Websites der ISO, ITU und des DIN nach Standards zum Thema hin abgesucht wurden. Ebenso wurde für die Suche nach Internet-Standards das WWW benutzt, genauer die entsprechende Auflistung des Computer Emergency Response Teams (CERT) des Deutschen Forschungsnetz (DFN) in Hamburg[1]. Insgesamt wurden im WWW 76 allgemeine Standards sowie 78 RFCs (beim CERT) gefunden.
Um die Anzahl der gefundenen Normen zu verringern, wurde bei Normen die sowohl vom DIN als auch von CEN und/oder ISO herausgegeben wurden, jeweils nur die internationale oder regionale Version in die Datenbank aufgenommen, versehen mit einem Verweis darauf, daß sie auch regional bzw. national gültig ist. D.h., wurde eine Norm sowohl als DIN-Norm als auch als CEN (EN-) und ISO-Norm gefunden, so wurde nur die ISO-Norm erfaßt, bei Normen, die sowohl als DIN- als auch als EN-Norm gefunden wurden, die EN-Norm. Teilweise wurden auch nur nationale bzw. regionale Umsetzungen einer ISO-Norm gefunden. Auch in diesem Fall wurde die entsprechende ISO-Norm (die aufgrund der Notation für Normen aus dem Titel

[1] <http://www.cert.dfn.de/resource/rfc/>

der nationale bzw. regionalen Norm ermittelt werden kann), versehen mit einem entsprechenden Vermerk, anstelle der gefundenen Norm in die Datenbank aufgenommen.
Nachdem der Schwerpunkt auf den Bereich der Frameworks gelegt wurde, wurde gezielt nach bestimmten Industriestandards zu diesem Thema gesucht.
Letztendlich wurden so 280 Normen und Standards für den Bereich Sicherheit und Kryptographie gefunden.

C.2 Auflistung aller Normen

Im folgenden werden alle gefundenen Normen und Standards aufgelistet. Dabei wurde folgendes Muster eingehalten:

- Nummer der Norm, z.B. DIN xyz oder RFC ijk, bzw. Kürzel
  Autor bzw. Herausgeber
  Titel, wobei bei ISO- und EN-Normen teilweise der deutsche Titel der entsprechenden DIN-Norm angegeben ist, sofern diese anstelle der ISO- bzw. EN-Norm gefunden wurde
  Rubriken - Die Literatur wird in der Datenbank Lina in Rubriken eingeteilt. Diese sind baumförmig angeordnet, wobei die Knoten durch „. “ voneinander getrennt sind. Diese Rubriken sind hier angegeben.
  Stichwörter: Weitere Stichwörter, die die Norm bzw. den Text beschreiben, diese stammen Teilweise aus dem entsprechendem Feld der PERINORM-Datenbank.

Auflistung

- 5A/179/CDV
  Autor: Original: IEC / hier: British Standards Institution
  Titel: Draft International Standard IEC 1508-1. Functional safety: safety related systems. Part 1: General requirements (65A/179/CDV)
  Rubriken: Weißnicht.
  Stichworte: Datenverarbeitung, Sicherheit, Softwaretechnik
- 5A/180/CDV
  Autor: Original: IEC / hier: British Standards Institution
  Titel: Draft International Standard IEC 1508-2. Functional safety: Safety related systems. Part 1: Requirements for electrical/electronic/programmable electronic systems (65A/180/CDV)
  Rubriken: Weißnicht.
  Stichworte: Datenverarbeitung, Sicherheit, Hardware
- 5A/185/CDV
  Autor: Original: IEC / hier: British Standards Institution
  Titel: IEC 1508-7. Functional safety: Safety related systems. Part 7: Bibliography of techniques and measures (65A/180/CDV)
  Rubriken: Weißnicht.
  Stichworte: Datenübertragung, Sicherheit
- 95/46/EG * 95/46/EC * 95/46/CE
  Autor: Europäische Gemeinschaften / Rat der Europäischen Gemeinschaften
  Titel: Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr
  Rubriken: Motive. Dschutz. Jura.
  Stichworte: Datengeheimnis, Datenschutz, Sicherheit
- AFNOR 96
  Autor: AFNOR

Titel: Informationstechnik. Sicherheitsanforderungen des elektronischen Datenaustauschs
Rubriken: Motive. weißnicht.
Stichworte: Datenverarbeitung, Sicherheit

- ANSI X 3.105
Autor: American National Standards Institute
Titel: Informationssysteme - Datenübermittlungsabschnittsverschlüsselung / Revision 1990
Rubriken: Krypto. Kryps. weißnicht., Schutz. Verschlüsselung.
Stichworte: Datenübermittlung, Informationssystem, Verschlüsselung

- ANSI X 3.106
Autor: American National Standards Institute
Titel: Informationssysteme - Algorithmus für die Datenverschlüsselung - Betriebsarten / Revision 1990
Rubriken: Schutz. Verschlüsselung., Krypto. Kryps. weißnicht.
Stichworte: Algorithmus, Daten, Informationssystem, Verschlüsselung

- ANSI X 3.92
Autor: American National Standards Institute
Titel: Algorithmus für die Datenverschlüsselung / Revision 1987
Rubriken: Krypto. Kryps. weißnicht., Schutz. Verschlüsselung.
Stichworte: Algorithmus, Informationssystem, Verschlüsselung

- ANSI X 9.17
Autor: American National Standards Institute
Titel: Geldinstitut-Schlüsselverwaltung (Großhandel)
Rubriken: Schutz. Werte., Schutz. Verschlüsselung.
Stichworte: Bankwesen, Codierung, Datenschutz, Datenübermittlung, Datenverarbeitung, Verschlüsselung

- ANSI X 9.30 Part 1
Autor: American National Standards Institute
Titel: Kryptographie für öffentliche Schlüssel mit irreversiblen Algorithmen für die Finanz-Dienstleistungsbranche - Teil 1: Algorithmus mit digitalen Signaturen
Rubriken: Schutz. Werte., Krypto. Kryps.
Stichworte: Algorithmus, Bankwesen, Datenschutz, Verschlüsselung

- ANSI X 9.8
Autor: American National Standards Institute
Titel: Bankwesen - PIN-Ausgabe und Verwaltung und PIN-Sicherheit - Teil 1: Prinzipien und Verfahren zum PIN-Schutz - Teil 2: Anerkannte Algorithmen zur PIN-Codierung
Rubriken: Schutz. Werte., Schutz. Zugang.
Stichworte: Algorithmus, Daten, Informationssystem, Verschlüsselung, Paßwort

- AWV 89
Autor: Arbeitsgemeinschaft für wirtschaftliche Verwaltung e.V.
Titel: Die Anfälligkeit der Datenverarbeitung für Systemmanipulation; Ein Leitfaden zur Risikominderung
Rubriken: Motive. weißnicht.
Stichworte: Datensicherung, Datenverarbeitung, Sicherheit

- BSIZertV 92
Autor: Bundesrepublik Deutschland, Bundesminister des Inneren
Titel: Verordnung über das Verfahren der Erteilung eines Sicherheitszertifikats durch das Bundesamt für Sicherheit in der Informationstechnik (BSI - Zertifizierungsverordnung - BSIZertV)
Rubriken: Schutz. Verschlüsselung.
Stichworte: Datenschutz, Datenverarbeitung, Sicherheit, Zertifikat

- CCITT F.4
Autor: ITU Internationale Fernmeldeunion - Studienkommission 1 - Dienstedefinitionen

Titel: Offene und geheime Sprache
Rubriken: Weißnicht.
Stichworte: Fernmeldewesen, Telekommunikation, Verschlüsselung

- CCITT X.800
  Autor: ITU Internationale Fernmeldeunion; Studienkommission 7 - Datennetze und Kommunikation offener Systeme
  Titel: Sicherheitsarchitektur für die Zusammenarbeit offener Systeme für CCITT-Anwendungen
  Rubriken: Schutz. Netze.
  Stichworte: Datenaustausch, Datenvermittlung, OSI, Sicherheit

- Corb 97
  Autor: OMG
  Titel: CORBAservices: Common Object Services Specification
  Stichworte: Verteiltes System, Framework

- csl91-11
  Autor: NIST
  Titel: NIST CSL Bulletin „Advanced Authentication Technology"
  Rubriken: Krypto. Auth. weißnicht.

- csl92-03
  Autor: NIST
  Titel: NIST CSL Bulletin „An Introduction to Secure Telephone Terminals"
  Rubriken: Weißnicht.

- csl93-05
  Autor: NIST
  Titel: NIST CSL Bulletin „Security Issues in Public Access Systems"
  Rubriken: Weißnicht.

- csl93-07
  Autor: NIST
  Titel: NIST CSL Bulletin „Connecting to the Internet: Security Considerations"
  Rubriken: Weißnicht., Motive. Netze.

- csl93-08
  Autor: NIST
  Titel: NIST CSL Bulletin „Security Program Management"
  Rubriken: Weißnicht.

- csl94-11
  Autor: NIST
  Titel: NIST CSL Bulletin „Digital Signature Standard"
  Rubriken: Krypto. Auth. asym. adhoc. DSS.

- csl95-02
  Autor: NIST
  Titel: NIST CSL Bulletin „The Data Encryption Standard: An Update"
  Rubriken: Krypto. Kryps. sym. adhoc. DES.

- csl95-08
  Autor: NIST
  Titel: NIST CSL Bulletin „A Framework for Cryptographic Standards"
  Rubriken: Krypto. Standards.

- csl96-08
  Autor: NIST
  Titel: NIST CSL Bulletin „Implementation Issues for Cryptography"
  Rubriken: Krypto. weißnicht., Motive. weißnicht.

- csl97-02
  Autor: NIST
  Titel: NIST CSL Bulletin „Advanced Encryption Standard"
  Rubriken: Krypto. Kryps. sym.

- Draft prEN 301 002-1 Edition 1.1.1
  Autor: ETSI Europäisches Institut für Telekommunikationsnormen
  Titel: Integrated Services Digital Network (ISDN); Personal Identification Number (PIN) security tool procedures; Digital Subscriber Signalling System No. one (DSS1) protocol;
  Rubriken: Schutz. Zugang.

- Draft prEN 301 002-2 Edition 1.1.1
  Autor: ETSI Europäisches Institut für Telekommunikationsnormen
  Titel: Integrated Services Digital Network (ISDN); Personal Identification Number (PIN) security tool procedures; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 2: Protocol Implementation Conformance
  Rubriken: Schutz. Zugang.

- DrSW 90
  Autor: NIST: Dray, Smid & Warner
  Titel: Implementing an Access Control System with Smart Token Technology
  Rubriken: Schutz. Zugang., Schutz. physi. Token. weißnicht.
  Stichworte: Datensicherheit, Datenübermittlung, Datenverarbeitung, OSI, Sicherheit

- ECMA TR/64
  Autor: ECMA European Manufacturers Association
  Titel: Secure Information Processing versus the Context of Product Evaluation
  Rubriken: Schutz. Bewertung. weißnicht.

- ECMA-205
  Autor: ECMA European Manufacturers Association
  Titel: Commercially Oriented Functionality Class for Security Evaluation (COFC)
  Rubriken: Schutz. Bewertung. weißnicht.

- ECMA-206
  Autor: ECMA European Manufacturers Association
  Titel: Association Context Management including Security Context Management
  Rubriken: Schutz. weißnicht.

- ECMA-219
  Autor: ECMA European Manufacturers Association
  Titel: Echtheit und privilegierte Attribute mit zugehörigen verteilten Schlüsselfunktionen für Datenschutzanwendungen - Teil 1: Übersicht und Funktionsmodell - Teil 2: Objekte der Datenschutz-Sicherheitseintragung - Teil 3: Bedienungsdefinition
  Rubriken: Weißnicht.
  Stichworte: Datenübertragung, Datenschutz, Datenverarbeitung, Informationsaustausch, Sicherheit

- ECMA-97
  Autor: ECMA European Manufacturers Association
  Titel: Lokalnetze; Sicherheitsvorschriften
  Rubriken: Fehlertol. Netze.
  Stichworte: Begriffe, Datenverarbeitung, Elektroinstallation, Sicherheit, Verkabelung

- ECMA/TR 46
  Autor: ECMA European Manufacturers Association
  Titel: Sicherheit in offenen Systemen; ein Sicherheitsrahmen
  Rubriken: Schutz. Netze.
  Stichworte: Begriffe, Datensicherheit, Datenverarbeitung, OSI, Sicherheit

- ENV 1068
  Autor: Original: ENV / hier: DIN Deutsches Institut für Normung e.V., NA Medizin
  Titel: Medizinische Informatik; Informationsaustausch im Gesundheitswesen; Registrierung von Kodierungsschemata; Englische Fassung ENV 1068:1993
  Rubriken: Sonstiges. Medizin.

Stichworte: Anforderung, Codierung, Datenverarbeitung, Gesundheitswesen, Registrierung

- ENV 12388
  Autor: Europäisches Komitee für Normung
  Titel: Medizinische Informatik - Algorithmen für digitale Unterschriftsdienste im Gesundheitswesen
  Rubriken: Sonstiges. Medizin., Krypto. Auth. asym. weißnicht.
  Stichworte: Algorithmus, Datenverarbeitung, Medizinische Informatik
- ErHM 96
  Autor: Marlena Erdos, Bret Hartman, Marianne Mueller
  Titel: Security Reference Model for the Java Developer's Kit 1.0.2
  Stichworte: Java, Framework, Crypto
- ETG 35
  Autor: EWOS Technical Guides
  Titel: OSI Lower Layers Security Profiles Options
  Rubriken: Schutz. Netze.
- ETG 48 Rev 1
  Autor: EWOS Technical Guides
  Titel: Application of Security Specifications in Functional Profiling
  Rubriken: Schutz. Bewertung. weißnicht.
- ETG 54
  Autor: EWOS Technical Guides
  Titel: Specification of Security Aspects in Functional Profiles
  Rubriken: Weißnicht.
- ETG 66
  Autor: EWOS Technical Guides
  Titel: Electronic Commerce
  Rubriken: Weißnicht., Schutz. Werte.
- ETG 73
  Autor: EWOS Technical Guides
  Titel: Security Requirements for OSI Management and TMN
  Rubriken: Schutz. Netze.
- ETR 234
  Autor: ETSI Europäisches Institut für Telekommunikationsnormen ETSI/TC NA
  Titel: Security Techniques Advisory Group (STAG) - A guide to specifying requirements for cryptographic algorithms
  Rubriken: Motive. Dsicherheit., Schutz. Spezifikation.
  Stichworte: Algorithmus, Fernmeldetechnik, Sicherheit, Verschlüsselung
- ETR 235
  Autor: ETSI Europäisches Institut für Telekommunikationsnormen ETSI/TC NA
  Titel: Security Techniques Advisory Group (STAG) - Requirements specification for an encryption algorithm for operators of European public telecommunication networks
  Rubriken: Schutz. Netze.
  Stichworte: Algorithmus, Fernmeldetechnik, Sicherheit, Verschlüsselung
- ETR 237
  Autor: ETSI Europäisches Institut für Telekommunikationsnormen
  Titel: Security Techniques Advisory Group (STAG); Baseline security standards; Features and mechanisms
  Rubriken: Weißnicht.
- ETR 277
  Autor: ETSI Europäisches Institut für Telekommunikationsnormen
  Titel: Security Algorithms Group of Experts (SAGE) - Requirements specification for an encryption algorithm for use in audio visual systems
  Rubriken: Krypto. Kryps. sym. weißnicht., Schutz. Spezifikation.
  Stichworte: Algorithmus, Sicherheit, Verschlüsselung

- ETR 278
  Autor: ETSI Europäisches Institut für Telekommunikationsnormen
  Titel: Security Algorithms Group of Experts (SAGE) - Report on the specification and evaluation of the GSM cipher algorithm A5/2
  Rubriken: Krypto. weißnicht., Krypto. Kryps. sym. adhoc. Sonstiges.
  Stichworte: Algorithmus, Sicherheit, Telekommunikation, Verschlüsselung

- FIPS 102
  Autor: NIST
  Titel: Guidelines for Computer Security Certification and Accreditation
  Rubriken: Schutz. Bewertung.

- FIPS 112
  Autor: NIST
  Titel: Password Usage
  Rubriken: Weißnicht.

- FIPS 113
  Autor: NIST
  Titel: Computer Data Authentication
  Rubriken: Krypto. Auth. Weißnicht.

- FIPS 140-1
  Autor: NIST
  Titel: Security Requirements for Cryptographic Modules
  Rubriken: Krypto. weißnicht., Motive. weißnicht.

- FIPS 171
  Autor: NIST
  Titel: Key Management Using ANSI X9.17
  Rubriken: Schutz. Verschlüsselung.

- FIPS 180-1
  Autor: NIST
  Titel: Secure Hash Standard
  Rubriken: Krypto. Einweg. Hash., Krypto. Standards.

- FIPS 181
  Autor: NIST
  Titel: Automated Password Generator
  Rubriken: Weißnicht.

- FIPS 185
  Autor: NIST
  Titel: Escrowed Encryption Standard
  Rubriken: Krypto. Kryps. weißnicht., Krypto. Standards.

- FIPS 186
  Autor: NIST
  Titel: Digital Signature Standard (DSS)
  Rubriken: Krypto. Auth. adhoc. DSS., Krypto. Standards.

- FIPS 188
  Autor: NIST
  Titel: Standard Security Labels for Information Transfer
  Rubriken: Weißnicht.

- FIPS 190
  Autor: NIST
  Titel: Guideline for the Use of Advanced Authentication Technology Alternatives
  Rubriken: Motive. Dsicherheit.

- FIPS 191
  Autor: NIST
  Titel: Guideline for The Analysis Local Area Network Security
  Rubriken: Motive. Dschutz.

- FIPS 196
  Autor: NIST
  Titel: Entity Authentication Using Public Key Cryptography
  Rubriken: Krypto. Auth. Weißnicht.
- FIPS 46-2
  Autor: NIST
  Titel: Data Encryption Standard (DES)
  Rubriken: Krypto. Kryps. sym. adhoc. DES., Krypto. Standards.
- FIPS 74
  Autor: NIST
  Titel: Guidelines for Implementing and Using the NBS Data Encryption Standard
  Rubriken: Krypto. Kryps. sym. adhoc. DES. Impl.
- FIPS 81
  Autor: NIST
  Titel: DES Modes of Operation
  Rubriken: Krypto. Kryps. sym. adhoc. DES.
- FTZ TL-A 3000 Teil 5
  Autor: Deutsche Bundespost TELEKOM, Forschungs- und Technologiezentrum / Referat Z 45-DrV
  Titel: Internationales Network Management System (INMS) (Sicherheits- und Zuverlässigkeitsaspekte)
  Rubriken: Schutz. Netze.
  Stichworte: Datensicherung, Datenübertragung, Datenverarbeitung, Sicherheit
- Gold 96
  Autor: Theodore Goldstein
  Titel: The Gateway Security Model in the Java Electronic Commerce Framework
  Stichworte: Java, Framework, JECF, E-Commerce
- Gong 96
  Autor: Li Gong
  Titel: New Security Architectural Directions for Java (Extended Abstract) December 19, 1996
  Stichworte: Java, Framework, Crypto
- IBM 96
  Autor: IBM Corp.
  Titel: Introduction to the Open Blueprint: A Guide to
  Stichworte: Framework, Open Blueprint
- IBM2 96
  Autor: IBM Corp.
  Titel: Open Blueprint: Security in the Open Blueprint
  Stichworte: Framework, Open Blueprint
- IBM3 96
  Autor: IBM Corp.
  Titel: Open Blueprint: Open Blueprint Technical Overview
  Stichworte: Framework, Open Blueprint
- IEC 65A/181/CDV
  Autor: Internationale Elektronische Kommission (IEC) - IEC/SC 65A
  Titel: Draft IEC 1508-3: Funktional safety - Safety related systems - Part 3: Software requirements
  Rubriken: Weißnicht.
  Stichworte: Begriffe, Datenverarbeitung, Elektrische Sicherheit, Programmierung, Sicherheit, Zuverlässigkeit
- IEC 65A/182/CDV
  Autor: Internationale Elektronische Kommission (IEC) - IEC/SC 65A
  Titel: Draft IEC 1508-4: Functional Safety - Safety related systems - Part 4: Definitions and abbreviation of terms

Rubriken: Weißnicht.
Stichworte: Anforderung, Begriffe, Datenverarbeitung, Hardware, Sicherheit

- IEEE 1228
Autor: IEEE Computer Society
Titel: Planung von Computersicherheit
Rubriken: Weißnicht.
Stichworte: Datensicherheit, Datenverarbeitung, Sicherheit

- Inte1 97
Autor: Intel Corp.
Titel: Common Security Services Manager Application Programming Interface (API)
Stichworte: Framework, E-Commerce

- Inte2 97
Autor: Intel Corp.
Titel: Common Security Services Manager Cryptographic Service Provider Interface (SPI) Specification
Stichworte: Framework, E-Commerce

- Inte3 97
Autor: Intel Corp.
Titel: Common Security Services Manager Data Storage Library Interface (DLI) Specification
Stichworte: Framework, E-Commerce

- Inte4 97
Autor: Intel Corp.
Titel: Common Security Services Manager Certificate Library Interface (CLI) Specification
Stichworte: Framework, E-Commerce

- Inte5 97
Autor: Intel Corp.
Titel: Common Security Services Manager Trust Policy Interface (TPI) Specification
Stichworte: Framework, E-Commerce

- Inte6 97
Autor: Intel Corp.
Titel: CSSM Application Notes
Stichworte: Framework, E-Commerce

- Inte7 97
Autor: Intel Corp.
Titel: Common Data Security Architecture Specification
Stichworte: Framework, E-Commerce

- ISO 10126-1
Autor: ISO International Organisation for Standardization ISO/TC 68
Titel: Bankwesen; Prozeduren für die Verschlüsselung von Nachrichten zwischen Banken; Teil 1: Allgemeine Grundsätze
Rubriken: Schutz. Verschlüsselung.
Stichworte: Bankwesen, Codierte Darstellung, Datenschutz, Verschlüsselung

- ISO 10126-2
Autor: ISO International Organisation for Standardization ISO/TC 68
Titel: Bankwesen; Prozeduren für die Nachrichtenverschlüsselung zwischen Banken; Teil 2: Algorithmen
Rubriken: Schutz. Verschlüsselung. algebraisch., Krypto. Kryps. weißnicht.
Stichworte: Algorithmus, Bankwesen, Codierte Darstellung, Datenschutz, Verschlüsselung

- ISO 10202-1
Autor: ISO International Organisation for Standardization ISO/TC 68
Titel: Financial Transaction Cards - Security Architectures of Financial Transaction

Systems using Integrated Circuit Cards - Part 1: Card Life Cycle
Rubriken: Schutz. physi. Token. allg.
Stichworte: Bankwesen, Bankkarte

- ISO 10202-2
  Autor: ISO International Organisation for Standardization ISO/TC 68
  Titel: Financial Transaction Cards - Security Architectures of Financial Transaction Systems using Integrated Circuit Cards - Part 2: Transaction Process
  Rubriken: Schutz. physi. Token. allg.
  Stichworte: Bankwesen, Bankkarte

- ISO 10202-4
  Autor: ISO International Organisation for Standardization ISO/TC 68
  Titel: Financial Transaction Cards - Security Architectures of Financial Transaction Systems using Integrated Circuit Cards - Part 4: Secure Application Modules
  Rubriken: Schutz. physi. Token. allg.
  Stichworte: Bankwesen, Bankkarte

- ISO 10202-6
  Autor: ISO International Organisation for Standardization ISO/TC 68
  Titel: Financial Transaction Cards - Security Architectures of Financial Transaction Systems using Integrated Circuit Cards - Part 6: Cardholder Verification
  Rubriken: Schutz. physi. Token. allg., Krypto. Auth. Weißnicht.
  Stichworte: Bankwesen, Bankkarte

- ISO 11131
  Autor: ISO International Organisation for Standardization ISO/TC 68
  Titel: Bankwesen; Benutzer-Authentisierung
  Rubriken: Schutz. Werte., Krypto. Auth. Weißnicht.
  Stichworte: Algorithmus, Bankwesen, Dokument, Unterschrift

- ISO 11166-1
  Autor: ISO International Organisation for Standardization ISO/TC 68
  Titel: Bankwesen - Schlüsselverwaltung durch asymmetrische Algorithmen - Teil 1: Grundsätze, Prozeduren und Formate
  Rubriken: Schutz. Werte., Schutz. Verschlüsselung.
  Stichworte: Algorithmus, Bankwesen, Datenschutz, Datenverarbeitung, Sicherheit

- ISO 11166-2
  Autor: ISO International Organisation for Standardization ISO/TC 68
  Titel: Bankwesen - Schlüsselverwaltung durch asymmetrische Algorithmen - Teil 2: Erlaubte Algorithmen bei der Benutzung des RSA-Verschlüsselungsverfahrens
  Rubriken: Schutz. Verschlüsselung., Schutz. Werte.
  Stichworte: Algorithmus, Bankwesen, Datenschutz, Datenverarbeitung, Sicherheit

- ISO 11568-1
  Autor: ISO International Organisation for Standardization ISO/TC 68
  Titel: Bankwesen - Schlüsselverwaltung (Einzelhandel) - Teil 1: Einführung in die Schlüsselverwaltung
  Rubriken: Schutz. Werte., Schutz. Verschlüsselung.
  Stichworte: Algorithmus, Bankwesen, Datenschutz, Echtheit, Kreditkarte, Verschlüsselung

- ISO 11568-2
  Autor: ISO International Organisation for Standardization ISO/TC 68
  Titel: Bankwesen - Schlüsselverwaltung (Einzelhandel) - Teil 2: Schlüsselverwaltungstechniken für symmetrische Verschlüsselung
  Rubriken: Schutz. Werte., Schutz. Verschlüsselung.
  Stichworte: Algorithmus, Ausweiskarte, Bankwesen, Datenschutz

- ISO 11568-3
  Autor: ISO International Organisation for Standardization ISO/TC 68
  Titel: Bankwesen - Schlüsselverwaltung (Einzelhandel) - Teil 3: Schlüsselzyklus für symmetrische Verschlüsselung

Rubriken: Schutz. Werte., Schutz. Verschlüsselung.
Stichworte: Algorithmus, Ausweiskarte, Bankwesen, Datenschutz, Verschlüsselung

- ISO 2382-8
  Autor: Original: ISO / hier: AFNOR
  Titel: Informationsverarbeitungssysteme. Begriffe. Teil 8: Kontrolle, Unversehrtheit und Sicherheit
  Rubriken: Weißnicht.
  Stichworte: Datenverarbeitung, Datenaustausch, Sicherheit
- ISO 7498-2
  Autor: ISO International Organisation for Standardization JTC 1 / SC 21
  Titel: Informationsverarbeitungssysteme. Kommunikation Offener Systeme. Basis Referenzmodell. Teil 2: Sicherheits-Architektur
  Rubriken: Schutz. Netze.
  Stichworte: Datenverarbeitung, Datenaustausch, Datenübertragung, Sicherheit
- ISO 8372
  Autor: ISO International Organisation for Standardization ISO/IEC/JTC 1
  Titel: Informationsverarbeitung; Betriebsarten für einen 64-bit-Blockschlüsselalgorithmus
  Rubriken: Krypto. Kryps. weißnicht.
  Stichworte: Algorithmus, Datenverarbeitung, Verschlüsselung
- ISO 8613 DAD 4
  Autor: ISO International Organisation for Standardization ISO/IEC/JTC 1
  Titel: Informationsverarbeitung; Text- und Bürosysteme; Büro-Dokumenten Architektur und Austauschformat; Ergänzung 4: Sicherheit
  Rubriken: Weißnicht. **Stichworte:** Datenaustausch, Datenverarbeitung, Sicherheit
- ISO 8730
  Autor: ISO International Organisation for Standardization ISO/TC 68
  Titel: Banking - Requirements For Message Authentication (Wholesale)
  Rubriken: Schutz. Werte., Krypto. Auth. Sonstiges.
  Stichworte: Bankwesen
- ISO 8731-1
  Autor: ISO International Organisation for Standardization ISO/TC 68
  Titel: Bankwesen; Erlaubte Algorithmen zur Authentisierung von Nachrichten; Teil 1: DEA-1 Algorithmus
  Rubriken: Schutz. Werte., Krypto. Auth. Weißnicht.
  Stichworte: Algorithmus, Bankwesen, Datenschutz, Datenverarbeitung
- ISO 8731-2
  Autor: ISO International Organisation for Standardization ISO/TC 68
  Titel: Bankwesen; Erlaubte Algorithmen zur Authentisierung von Nachrichten; Teil 2: Nachrichten-Authentisierungsalgorithmus
  Rubriken: Schutz. Werte., Krypto. Auth. Weißnicht.
  Stichworte: Algorithmus, Bankwesen, Datenaustausch, Datenübermittlung, Nachrichten
- ISO 8732
  Autor: ISO International Organisation for Standardization ISO/TC 68
  Titel: Banking: Key Management (Wholesale)
  Rubriken: Schutz. Werte., Schutz. Verschlüsselung.
  Stichworte: Bankwesen
- ISO 9160
  Autor: ISO International Organisation for Standardization ISO/TC 68
  Titel: Informationsverarbeitung; Datenverschlüsselung; Datenverschlüsselungsanforderungen für Kommunikation in der Bit-Übertragungsschicht
  Rubriken: Schutz. Netze.
  Stichworte: Datenaustausch, Datenverarbeitung, Kommunikation, OSI, Verschlüsselung

- ISO 9564-1
  Autor: ISO International Organisation for Standardization ISO/TC 68
  Titel: Bankwesen; PIN-Ausgabe und -Verwaltung und PIN-Sicherheit; Teil 1: Grundsätze und Verfahren zum Schutz der PIN
  Rubriken: Schutz. Werte., Schutz. Zugang.
  Stichworte: Algorithmus, Bankwesen, Datenschutz, Datensicherheit
- ISO 9564-2
  Autor: ISO International Organisation for Standardization ISO/TC 68
  Titel: Bankwesen; PIN-Ausgabe und -Verwaltung und PIN-Sicherheit; Teil 2: Anerkannte Algorithmen zur PIN-Verschlüsselung
  Rubriken: Schutz. Werte., Schutz. Zugang., Krypto. Standards.
  Stichworte: Algorithmus, Bankwesen, Datenschutz, Verschlüsselung
- ISO 9807
  Autor: ISO International Organisation for Standardization ISO/TC 68
  Titel: Bankwesen; Anforderungen für die Nachrichtenechtheitsprüfung (im Handel)
  Rubriken: Krypto. Auth., Schutz. Werte.
  Stichworte: Algorithmus, Bankwesen, Datensicherheit, Echtheit
- ISO 9992-1
  Autor: ISO International Organisation for Standardization ISO/TC 68
  Titel: Financial Transaction Cards - Messages Between the Integrated Circuit Card and the Card Accepting Device - Part 1: Concepts and Structures
  Rubriken: Schutz. physi. Token. allg., Schutz. Werte.
  Stichworte: Bankwesen, Bankkarte
- ISO DIS 10202-3
  Autor: ISO International Organisation for Standardization ISO/TC 68
  Titel: Financial Transaction Cards - Security Architectures of Financial Transaction Systems using Integrated Circuit Cards - Part 3: Cryptographic Key Relationships
  Rubriken: Schutz. physi. Token. allg., Schutz. Werte.
  Stichworte: Bankwesen, Bankkarte
- ISO DIS 11568-6
  Autor: ISO International Organisation for Standardization ISO/TC 68
  Titel: Banking - Key Management (Retail) Part 6: Key Management Schemes
  Rubriken: Schutz. Werte., Schutz. Verschlüsselung.
  Stichworte: Bankwesen
- ISO DIS 13489
  Autor: ISO International Organisation for Standardization ISO/TC 68
  Titel: Data elements to be used in international interchange in relation to bit 55 of ISO 8583
  Rubriken: Weißnicht.
  Stichworte: Bankwesen
- ISO/CD 9992-2
  Autor: ISO International Organisation for Standardization ISO/TC 68
  Titel: Financial Transaction Cards - Messages Between the Integrated Circuit Card and the Card Accepting Device - Part 2: Functions, Messages (Commands and Responses), Data Elements And Structures
  Rubriken: Schutz. physi. Token. allg.
  Stichworte: Bankwesen, Bankkarte
- ISO/DIS 10202-5
  Autor: ISO International Organisation for Standardization ISO/TC 68
  Titel: Bankkarten - Sicherheitsarchitektur in Zahlungsverkehrssystemen für Karten mit integrierten Schaltkreisen - Teil 5: Anwendung der Algorithmen
  Rubriken: Schutz. physi. Token. allg., Krypto. weißnicht.
  Stichworte: Algorithmus, Bankkarte, Zahlungsverkehr
- ISO/DIS 10202-7
  Autor: ISO International Organisation for Standardization ISO/TC 68
  Titel: Financial Transaction Cards - Security Architectures of Financial Transaction

Systems using Integrated Circuit Cards - Part 7: Key Management
Rubriken: Schutz. physi. Token. allg., Schutz. Verschlüsselung.
Stichworte: Bankwesen, Bankkarte

- ISO/DIS 10202-8
Autor: ISO International Organisation for Standardization ISO/TC 68
Titel: Financial Transaction Cards - Security Architectures of Financial Transaction Systems using Integrated Circuit Cards - Part 8: General Principles And Overview
Rubriken: Schutz. physi. Token. allg.
Stichworte: Bankwesen, Bankkarte

- ISO/DIS 11568-4
Autor: ISO International Organisation for Standardization ISO/TC 68
Titel: Bankwesen - Schlüsselverwaltung (Einzelhandel) - Teil 4: Schlüsselverwaltungstechniken für asymmetrische Verschlüsselungssysteme
Rubriken: Schutz. Werte., Schutz. Verschlüsselung.
Stichworte: Algorithmus, Bankwesen, Codierung, Datenschutz, Identifikationskarte, Verschlüsselung

- ISO/DIS 11568-5
Autor: ISO International Organisation for Standardization ISO/TC 68
Titel: Bankwesen - Schlüsselverwaltung (Einzelhandel) - Teil 5: Gültigkeitsdauer für Schlüssel in asymmetrische Verschlüsselungssysteme
Rubriken: Schutz. Werte., Schutz. Verschlüsselung.
Stichworte: Algorithmus, Bankwesen, Codierung, Datenschutz, Identifikationskarte, Verschlüsselung

- ISO/DIS 13491-1
Autor: ISO International Organisation for Standardization ISO/TC 68
Titel: Bankwesen - Sichere Verschlüsselungsgeräte (Einzelhandel) - Teil 1: Konzepte, Anforderungen und Zertifizierungsmethoden
Rubriken: Schutz. Werte., Schutz. Verschlüsselung., Schutz. physi. Token. allg.
Stichworte: Bankwesen, Datenschutz, Datenverarbeitung, Verschlüsselung

- ISO/DIS 13492
Autor: ISO International Organisation for Standardization ISO/TC 68
Titel: Banking - Key Management Related Data Elements (Retail)
Rubriken: Schutz. Werte.
Stichworte: Bankwesen

- ISO/DIS 8227
Autor: Original: ISO / hier: DIN Deutsches Institut für Normung e.V., NA Informationstechnik
Titel: Informationsverarbeitung; Datenverschlüsselung; Festlegung des Algorithmus DEA 1; Identisch mit ISO/DIS 8227, Ausgabe 1985
Rubriken: Krypto. Kryps. weißnicht.
Stichworte: Algorithmus, Codierung, Datenverarbeitung, Verschlüsselung

- ISO/IEC 10116
Autor: ISO International Organisation for Standardization, Internationale Elektrotechnische Kommission (IEC) - ISO/IEC/JTC 1
Titel: Informationstechnik; Betriebsarten für einen n-bit-Blockschlüssel-Algorithmus
Rubriken: Krypto. Kryps. weißnicht.
Stichworte: Algorithmus, Codierung, Datenschutz, Datensicherheit, Datenverarbeitung

- ISO/IEC 10118-1
Autor: ISO International Organisation for Standardization, Internationale Elektrotechnische Kommission (IEC) - ISO/IEC/JTC 1
Titel: Informationstechnik - Sicherheitstechniken - Hashfunktionen - Teil 1: Allgemeines Modell
Rubriken: Krypto. Einweg. Hash.
Stichworte: Algorithmus, Datenschutz, Datenverarbeitung

- ISO/IEC 10118-2
  Autor: ISO International Organisation for Standardization, Internationale Elektrotechnische Kommission (IEC) - ISO/IEC/JTC 1
  Titel: Informationstechnik - Sicherheitstechniken - Hashfunktionen - Teil 2: Hashfunktionen unter Benutzung eines n-bit-Blockschlüssel-Algorithmus
  Rubriken: Krypto. Einweg. Hash.
  Stichworte: Algorithmus, Datenschutz, Datenverarbeitung
- ISO/IEC 10181-1
  Autor: Original: ISO/IEC / hier: ITU Internationale Fernmeldeunion
  Titel: Information technology - Open Systems Interconnection - Security frameworks for open systems: Overview
  Rubriken: Schutz. Netze.
  Stichworte: Datenkommunikation, Fernmeldetechnik, OSI, Sicherheit
- ISO/IEC 10181-2
  Autor: Original: ISO/IEC / hier: ITU Internationale Fernmeldeunion
  Titel: Informationstechnik - Kommunikation Offener Systeme - Rahmenrichtlinien für IT-Sicherheit in Offenen Systemen: Authentifikation
  Rubriken: Krypto. Auth. Weißnicht., Schutz. Netze.
  Stichworte: Datenkommunikation, Fernmeldetechnik, OSI, Sicherheit
- ISO/IEC 10181-3
  Autor: ISO International Organisation for Standardization * Internationale Elektrotechnische Kommission (IEC) ISO/IEC/JTC 1
  Titel: Informationstechnik - Kommunikation Offener Systeme - Rahmenrichtlinien für IT-Sicherheit in Offenen Systemen - Teil 3: Rahmenrichtlinien für die Zugriffskontrolle
  Rubriken: Schutz. Netze., Schutz. Zugriff.
  Stichworte: Begriffe, Datenkommunikation, Datenschutz, Datensicherheit, OSI, Sicherheit
- ISO/IEC 10181-4
  Autor: ISO International Organisation for Standardization * Internationale Elektrotechnische Kommission (IEC) ISO/IEC/JTC 1
  Titel: Informationstechnik - Kommunikation offener System - Rahmenrichtlinien für IT-Sicherheit in Offenen System - Teil 4: Nicht- Verweigerung
  Rubriken: Schutz. Netze.
  Stichworte: Datenverarbeitung, Informationsaustausch, Sicherheit
- ISO/IEC 10181-5
  Autor: ISO International Organisation for Standardization * Internationale Elektrotechnische Kommission (IEC) ISO/IEC/JTC 1
  Titel: Informationstechnik - Kommunikation Offener Systeme - Rahmenrichtlinien für IT-Sicherheit in Offenen Systemen - Teil 5: Rahmenrichtlinien für den Echtheitsnachweis
  Rubriken: Schutz. Netze.
  Stichworte: Begriffe, Datennetz, Datensicherheit,OSI, Sicherheit
- ISO/IEC 10181-6
  Autor: ISO International Organisation for Standardization * Internationale Elektrotechnische Kommission (IEC) ISO/IEC/JTC 1
  Titel: Informationstechnik - Kommunikation Offener Systeme - Rahmenrichtlinien für IT-Sicherheit in Offenen Systemen - Teil 6: Rahmenrichtlinien für Vertraulichkeit
  Rubriken: Schutz. Netze.
  Stichworte: Datenschutz, Datensicherheit,Sicherheit
- ISO/IEC 10181-7
  Autor: Original: ISO/IEC / hier: ITU Internationale Fernmeldeunion
  Titel: Information technology - Open Systems Interconnection - Security frameworks for open systems: Security audit and alarms framework
  Rubriken: Schutz. Netze.
  Stichworte: Datenkommunikation, Fernmeldetechnik, OSI, Sicherheit

- ISO/IEC 10736
  Autor: ISO International Organisation for Standardization * Internationale Elektrotechnische Kommission (IEC) ISO/IEC/JTC 1
  Titel: Informationstechnik; Telekommunikation und Informationsaustausch zwischen Systemen; Sicherheitsprotokoll der Transportschicht
  Rubriken: Schutz. Netze.
  Stichworte: Datensicherheit, Datenübermittlung, Datenverarbeitung, OSI, Sicherheit
- ISO/IEC 10745
  Autor: Original: ISO/IEC / hier: ITU Internationale Fernmeldeunion - Studienkom. 7: Datennetze u. Kommunikation offener Systeme
  Titel: Informationstechnik - Kommunikation Offener Systeme - Modell für IT-Sicherheit in den anwendungsorientierten OSI-Schichten
  Rubriken: Schutz. Netze.
  Stichworte: Anwendungsschicht, Fernmeldetechnik, OSI, Sicherheit
- ISO/IEC 11577
  Autor: ISO International Organisation for Standardization * Internationale Elektrotechnische Kommission (IEC) ISO/IEC/JTC 1
  Titel: Informationstechnik - Kommunikation offener Systeme - Sicherheitsprotokoll der Vermittlungsschicht
  Rubriken: Schutz. Netze.
  Stichworte: Datenverarbeitung, Sicherheit
- ISO/IEC 11586-1
  Autor: Original: ISO/IEC / hier: ITU Internationale Fernmeldeunion
  Titel: Informationstechnik - Kommunikation Offener Systeme - Allgemeine Sicherheitsmechanismen für die anwendungsorientierten OSI-Schichten: Konzepte, Modelle und Notation
  Rubriken: Schutz. Netze.
  Stichworte: Datenkommunikation, Fernmeldetechnik, OSI, Sicherheit
- ISO/IEC 11586-2
  Autor: Original: ISO/IEC / hier: ITU Internationale Fernmeldeunion
  Titel: Informationstechnik - Kommunikation Offener Systeme - Allgemeine Sicherheitsmechanismen für die anwendungsorientierten OSI-Schichten: Dienstelement für den Austausch von Sicherheitsinformationen (SESE)
  Rubriken: Schutz. Netze.
  Stichworte: Datenkommunikation, Fernmeldetechnik, OSI, Sicherheit, Übertragungsschicht
- ISO/IEC 11586-3
  Autor: Original: ISO/IEC / hier: ITU Internationale Fernmeldeunion
  Titel: Informationstechnik - Kommunikation Offener Systeme - Allgemeine Sicherheitsmechanismen für die anwendungsorientierten OSI-Schichten: Protokollspezifikation für das Dienstelement für den Austausch von Sicherheitsinformationen (SESE)
  Rubriken: Schutz. Netze.
  Stichworte: Datenkommunikation, Fernmeldetechnik, OSI, Sicherheit, Übertragungsschicht
- ISO/IEC 11586-4
  Autor: Original: ISO/IEC / hier: TU Internationale Fernmeldeunion
  Titel: Informationstechnik - Kommunikation Offener Systeme - Allgemeine Sicherheitsmechanismen für die anwendungsorientierten OSI-Schichten: Spezifikation der schützenden Übertragungssyntax
  Rubriken: Schutz. Netze.
  Stichworte: Datenkommunikation, Fernmeldetechnik, OSI, Sicherheit, Übertragungsschicht
- ISO/IEC 11586-5
  Autor: ISO International Organisation for Standardization * Internationale Elektrotechnische Kommission (IEC) ISO/IEC/JTC 1

Titel: Informationstechnik - Kommunikation offener Systeme - Generische Mechanismen für anwendungsorientierte OSI - Schichten - Teil 5: Formularsatz für Konformitätsaussagen zu einer Protokollimplementierung des Dienstelements für den Austausch von Sicherheitsinformationen
Rubriken: Schutz. Netze.
Stichworte: Anwendungsschicht, Datenverarbeitung, Informationsaustausch, OSI, Sicherheit

- ISO/IEC 11586-6
  Autor: ISO - International Organisation for Standardization - Intern. Elektrische Kommission IEC - JTC 1 / SC 21
  Titel: Information technology. Open systems interconnection. Generic upper layers security. Protecting transfer syntax implementation conformance statement (PICS) proforma
  Rubriken: Schutz. Netze.
  Stichworte: Datenverarbeitung, Codierung
- ISO/IEC 11770-2
  Autor: ISO International Organisation for Standardization, Internationale Elektrotechnische Kommission (IEC) - ISO/IEC/JTC 1
  Titel: Informationstechnik - Sicherheitstechniken - Schlüsselmanagement - Teil 2: Mechanismen unter Benutzung von symmetrischen Techniken
  Rubriken: Schutz. Verschlüsselung.
  Stichworte: Algorithmus, Datenübertragung, Datenschutz, Datenverarbeitung, Echtheit
- ISO/IEC 13594
  Autor: Original: ISO/IEC / hier: ITU Internationale Fernmeldeunion
  Titel: Information technology - Lower layers security model
  Rubriken: Schutz. Netze.
  Stichworte: Datenübertragung, Fernmeldetechnik, OSI, Sicherheit
- ISO/IEC 9594-8
  Autor: ISO International Organisation for Standardization * Intern. Elektrotechnische Kommission (IEC) ISO/IEC/JTC 1 / SC 27
  Titel: Information technology - Open Systems Interconnection - The Directory: Authentication Framework
  Rubriken: Schutz. Netze.
  Stichworte: Datenverarbeitung, Sicherheit
- ISO/IEC 9796
  Autor: ISO International Organisation for Standardization * Internationale Elektrotechnische Kommission (IEC) ISO/IEC/JTC 1
  Titel: Informationstechnik; Sicherheitsverfahren; Digitaler Unterschriftsmechanismus mit Rückgewinnung der Nachricht
  Rubriken: Krypto. Auth. Weißnicht.
  Stichworte: Datenaustausch, Datenschutz, Datensicherheit, Datenverarbeitung, Sicherheit
- ISO/IEC 9797
  Autor: ISO International Organisation for Standardization * Internationale Elektrotechnische Kommission (IEC) ISO/IEC/JTC 1
  Titel: Informationstechnik; Sicherheitsverfahren; Mechanismus zur Gewährleistung der Datenunversehrtheit unter Benutzung eines Blockschlüssel-Algorithmus
  Rubriken: Krypto. Kryps. weißnicht.
  Stichworte: Algorithmus, Datenschutz, Datensicherheit
- ISO/IEC 9798-1
  Autor: ISO International Organisation for Standardization * Internationale Elektrotechnische Kommission (IEC) ISO/IEC/JTC 1 / SC 27
  Titel: Information technology - Security techniques - Entity authentication mechanisms - Part 1: General
  Rubriken: Krypto. Auth. Weißnicht.
  Stichworte: Datenverarbeitung, Sicherheit

- ISO/IEC 9798-2
Autor: ISO International Organisation for Standardization * Internationale Elektrotechnische Kommission (IEC) ISO/IEC/JTC 1
Titel: Informationstechnik - Sicherheitsverfahren - Authentifikation von Instanzen - Teil 2: Mechanismen unter Benutzung von Verschlüsselungsalgorithmen
Rubriken: Krypto. Auth. Weißnicht.
Stichworte: Algorithmus, Datenschutz, Datensicherheit, Datenverarbeitung, Echtheitsprüfung
- ISO/IEC 9798-3
Autor: ISO International Organisation for Standardization, Internationale Elektrotechnische Kommission (IEC) - ISO/IEC/JTC 1
Titel: Informationstechnik - Sicherheitsverfahren - Mechanismen zur Authentifikation von Instanzen - Teil 3: Authentifikation von Instanzen unter Benutzung eines Algorithmus mit öffentlichem Schlüssel
Rubriken: Krypto. Auth. Weißnicht.
Stichworte: Algorithmus, Datensicherheit, Datenverarbeitung
- ISO/IEC 9798-4
Autor: ISO International Organisation for Standardization * Internationale Elektrotechnische Kommission (IEC) ISO/IEC/JTC 1 / SC 27
Titel: Information technology - Security techniques - Entity authentication mechanisms - Part 4: Mechanisms using a cryptographic check function
Rubriken: Krypto. Auth. Weißnicht.
Stichworte: Datenverarbeitung, Sicherheit
- ISO/IEC 9979
Autor: ISO International Organisation for Standardization * Internationale Elektrotechnische Kommission (IEC) - ISO/IEC/JTC 1
Titel: Kryptographische Techniken; Verfahren für die Registrierung von kryptographischen Algorithmen
Rubriken: Krypto. weißnicht.
Stichworte: Algorithmus, Codierte Darstellung, Datenkonvertierung, Datenverarbeitung, Registrierung
- ISO/IEC DIS 10116
Autor: ISO International Organisation for Standardization, Internationale Elektrotechnische Kommission (IEC) - ISO/IEC/JTC 1
Titel: Informationstechnik - Betriebsarten für einen n-bit-Blockschlüssel-Algorithmus
Rubriken: Krypto. weißnicht.
Stichworte: Algorithmus, Begriffe, Codierung, Datenschutz, Datensicherheit, Datenverarbeitung
- ISO/IEC DIS 10118-3
Autor: ISO International Organisation for Standardization, Internationale Elektrotechnische Kommission (IEC) - ISO/IEC/JTC 1
Titel: Information technology - Security techniques - Hash-functions - Part 3: Dedicated hash-functions
Rubriken: Krypto. Einweg. Hash.
Stichworte: Algorithmus, Datenschutz, Datenverarbeitung
- ISO/IEC DIS 10118-4
Autor: ISO International Organisation for Standardization, Internationale Elektrotechnische Kommission (IEC) - ISO/IEC/JTC 1 / SC 27
Titel: Information technology - Security techniques - Hash-functions - Part 4: Hash-functions using modular arithmetic
Rubriken: Krypto. Einweg. Hash.
Stichworte: Algorithmus, Datenschutz, Datenverarbeitung
- ISO/IEC DIS 10736 DAM 1
Autor: ISO International Organisation for Standardization * Internationale Elektrotechnische Kommission (IEC) ISO/IEC/JTC 1
Titel: Informationstechnik; Telekommunikation und Informationsaustausch zwischen

Systemen; Sicherheitsprotokoll der Transportschicht; änderung 1: Einrichten einer Sicherheits-Assoziation
Rubriken: Weißnicht.
Stichworte: Datensicherheit, Datenübermittlung, Datenverarbeitung, OSI, Sicherheit

- ISO/IEC DIS 11770-1
  Autor: ISO International Organisation for Standardization * Internationale Elektrotechnische Kommission (IEC) ISO/IEC/JTC 1
  Titel: Informationstechnik - Sicherheitstechniken - Schlüsselmanagement - Teil 1: Rahmenrichtlinien
  Rubriken: Weißnicht.
  Stichworte: Begriffe, Datensicherheit, Datenverarbeitung, Sicherheit, Verschlüsselung

- ISO/IEC DIS 11770-3
  Autor: ISO International Organisation for Standardization, Internationale Elektrotechnische Kommission (IEC) - ISO/IEC/JTC 1
  Titel: Informationstechnik - Sicherheitstechniken - Schlüsselmanagement - Teil 3: Mechanismen unter Benutzung von asymmetrischen Techniken
  Rubriken: Schutz. Verschlüsselung.
  Stichworte: Algorithmus, Datenübertragung, Datenschutz, Datenverarbeitung

- ISO/IEC DIS 13888-1
  Autor: ISO International Organisation for Standardization, Internationale Elektrotechnische Kommission (IEC) - ISO/IEC/JTC 1 / SC 27
  Titel: Information technology - Security techniques - Non-repudiation - Part 1: General
  Rubriken: Weißnicht.
  Stichworte: Algorithmus, Datenschutz, Datenverarbeitung

- ISO/IEC DIS 13888-3
  Autor: ISO International Organisation for Standardization * Internationale Elektrotechnische Kommission (IEC) ISO/IEC/JTC 1
  Titel: Information technology - Security techniques - Non-repudiation - Part 3: Using asymetric techniques
  Rubriken: Weißnicht.
  Stichworte: Datenschutz, Datenverarbeitung, OSI, Sicherheit

- ISO/IEC DIS 14980
  Autor: ISO International Organisation for Standardization * Internationale Elektrotechnische Kommission (IEC) ISO/IEC/JTC 1
  Titel: Informationstechnik - Richtlinien für das Management von IT-Sicherheit
  Rubriken: Weißnicht.
  Stichworte: Codierte Darstellung, Datenschutz, Datenverarbeitung, Informationsaustausch, Sicherheit

- ISO/IEC DIS 9796-2
  Autor: ISO International Organisation for Standardization * Internationale Elektrotechnische Kommission (IEC) ISO/IEC/JTC 1
  Titel: Informationstechnik - Sicherheitstechniken - Digitaler Unterschriftenmechanismus mit Rückgewinnung der Nachricht - Teil 2: Mechanismen unter Nutzung einer Hash-Funktion (Überarbeitung von ISO/IEC 9796:1991)
  Rubriken: Krypto. Einweg. Hash., Krypto. Auth. Weißnicht.
  Stichworte: Begriffe, Datenaustausch, Datenschutz, Datensicherheit, Datenverarbeitung, Sicherheit

- ISO/IEC DISP 12059-7
  Autor: ISO International Organisation for Standardization * Internationale Elektrotechnische Kommission (IEC) ISO/IEC/JTC 1
  Titel: Informationstechnik - Internationale Profilnormen - OSI-Management - Allgemeine Management-Informationsfunktionen - Teil 7: Sicherheitsalarmmeldefunktionen

Rubriken: Schutz. Netze.
Stichworte: Datenverarbeitung, Sicherheit

- ISO/IEC DISP 12059-8
  Autor: ISO International Organisation for Standardization * Internationale Elektrotechnische Kommission (IEC) ISO/IEC/JTC 1
  Titel: Informationstechnik - Internationale Profilnormen - OSI-Management - Allgemeine Management-Informationsfunktionen - Teil 8: Sicherungsnachweis für Sicherheitszwecke
  Rubriken: Schutz. Netze.
  Stichworte: Datenverarbeitung, Sicherheit
- ISO/IEC DISP 12060-6
  Autor: ISO International Organisation for Standardization * Internationale Elektrotechnische Kommission (IEC) ISO/IEC/JTC 1
  Titel: Informationstechnik - Internationale Profilnormen - OSI-Management - Managementfunktionen - Teil 6: Fähigkeiten von Sicherheitsmangement (including profiles AOM2421, AOM 2422 and AOM2423)
  Rubriken: Schutz. Netze.
  Stichworte: Datenübertragung, Datenverarbeitung, OSI, Sicherheit
- ISO/IEC DTR 13335-2
  Autor: ISO International Organisation for Standardization, Internationale Elektrotechnische Kommission (IEC) - ISO/IEC/JTC 1 / SC 27
  Titel: Information technology - Guidelines for the management of IT security - Part 2: Planning and managing IT security (Future Technical Report)
  Rubriken: Weißnicht.
  Stichworte: Algorithmus, Datenschutz, Datenverarbeitung
- ISO/IEC DTR 13335-3
  Autor: ISO International Organisation for Standardization, Internationale Elektrotechnische Kommission (IEC) - ISO/IEC/JTC 1 / SC 27
  Titel: Information technology - Guidelines for the management of IT security - Part 3: Techniques for the management of IT security
  Rubriken: Weißnicht.
  Stichworte: Algorithmus, Datenschutz, Datenverarbeitung
- ISO/IEC TR 13335-1
  Autor: ISO International Organisation for Standardization, Internationale Elektrotechnische Kommission (IEC) - ISO/IEC/JTC 1 / SC 27
  Titel: Information technology - Guidelines for the management of IT security - Part 1: Concepts and models for IT security
  Rubriken: Weißnicht.
  Stichworte: Algorithmus, Datenschutz, Datenverarbeitung
- ISO/TR 13569
  Autor: ISO International Organisation for Standardization ISO/TC 68
  Titel: Banking and related financial services - Information Security Guidelines For Banking
  Rubriken: Schutz. Werte.
  Stichworte: Bankwesen
- ITSicherhKritBek
  Autor: Bundesrepublik Deutschland, Bundesminister des Inneren
  Titel: IT-Sicherheitskriterien; Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (IT); Fassung 1989-01-11
  Rubriken: Motive. weißnicht.
  Stichworte: Datenschutz, Datenverarbeitung, Sicherheit, Spezifikation
- TSicherhKritEGBek
  Autor: Bundesrepublik Deutschland, Bundesminister des Inneren
  Titel: EG-Einheitliche „Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik - ITSEC“
  Rubriken: Motive. weißnicht.
  Stichworte: Datenverarbeitung, Sicherheit

- ITU-T H.234
  Autor: ITU Internationale Fernmeldeunion - Studienkommission 15 - Übertragungssysteme und -geräte
  Titel: Encryption key management and authentication system for audiovisual services
  Rubriken: Krypto. weißnicht.
  Stichworte: Datenübertragung, Echtheitsprüfung, Fernmeldetechnik, Telekommunikation, Verschlüsselung
- JIS X 5052-1990
  Autor: Japanese Industrial Standards Committee (JISC) - information processing
  Titel: Modes of operation for a 64-bit block cipher algorithm
  Rubriken: Krypto. weißnicht.
  Stichworte: Algorithmus, Programmierverfahren
- JIS X 5060-
  Autor: Japanese Industrial Standards Committee (JISC) - information processing
  Titel: Data cryptographic techniques - Procedures for the registration of cryptographic algorithms
  Rubriken: Weißnicht.
  Stichworte: OSI, Datenbearbeitung, Algorithmus, Programmierverfahren
- NF C98-310
  Autor: AFNOR
  Titel: Endgeräte für den Zahlungsverkehr
  Rubriken: Schutz. physi. Token. allg., Schutz. Werte.
  Stichworte: Datenverarbeitung, Bankdokumente, Magnetkarte, Sicherheit,
- NIST-sp4rpt
  Autor: NIST
  Titel: Report on NIST Research Effort on SP4 Secure Protocol under OSI
  Rubriken: Weißnicht.
  Stichworte: Datensicherheit, Datenübermittlung, Datenverarbeitung, OSI, Sicherheit
- OMG 94
  Autor: OMG
  Titel: OMG White Paper on Security
  Stichworte: Verteiltes System, Framework, Sicherheit
- PKCS #11 V2
  Autor: RSA Laboratories
  Titel: PKCS #11: Cryptographic Token Interface Standard (Cryptoki)
  Stichworte: Framework, Crypto, Smartcards
- PKCS #11
  Autor: RSA Laboratories
  Titel: PKCS #11: Cryptographic Token Interface Standard (Cryptoki)
  Stichworte: Framework, Crypto, Smartcards
- RFC 1004
  Autor: IETF: D. L. Mills
  Titel: A Distributed-Protocol Authentication Scheme
  Rubriken: Krypto. Auth. Weißnicht.
- RFC 1108
  Autor: IETF: S. Kent
  Titel: Security Options for the Internet Protocol
- RFC 1135
  Autor: IETF: J. Reynolds
  Titel: The Helminthiasis of the Internet
- RFC 1170
  Autor: IETF: R. Fougner
  Titel: Public Key Standards and Licenses

- RFC 1244
  Autor: IETF: P. Holbrook & J. Reynolds
  Titel: Site Security Handbook
- RFC 1272
  Autor: IETF: C. Mills, D. Hirsh & G. Ruth
  Titel: Internet accounting: background
- RFC 1281
  Autor: IETF: R. D. Pethias, S. Crocker & B. Fraser
  Titel: Guidelines for the Secure Operation of the Internet
  Rubriken: Motive. weißnicht.
- RFC 1319
  Autor: IETF: B. Kaliski
  Titel: The MD2 Message-Digest Algorithm
  Rubriken: Krypto. weißnicht.
- RFC 1320
  Autor: IETF: R. Rivest
  Titel: The MD4 Message-Digest Algorithm
  Rubriken: Krypto. weißnicht.
- RFC 1321
  Autor: IETF: R. Rivest
  Titel: The MD5 Message-Digest Algorithm
  Rubriken: Krypto. weißnicht.
- RFC 1334
  Autor: IETF: B. Lloyd & W. Simpson
  Titel: PPP Authentication Protocols
  Rubriken: Krypto. Auth. Weißnicht.
- RFC 1352
  Autor: IETF: J. Calvin, K. McCloghrie & J. Davin
  Titel: SNMP Security Protocols
- RFC 1355
  Autor: IETF: J. Curran & A. Marine
  Titel: Privacy and Accuracy Issues in Network Information Center Databases
- RFC 1411
  Autor: IETF: D. Borman
  Titel: Telnet Authentication: Kerberos Version 4
  Rubriken: Krypto. Auth. Weißnicht.
- RFC 1412
  Autor: IETF: K. Alagappan
  Titel: Telnet Authentication: SPX
  Rubriken: Krypto. Auth. Weißnicht.
- RFC 1413
  Autor: IETF: M. St. Johns
  Titel: Identification Protocol
- RFC 1414
  Autor: IETF: M. St. Johns & M. Rose
  Titel: Identification MIB
- RFC 1416
  Autor: IETF: D. Borman
  Titel: Telnet Authentication Option
  Rubriken: Krypto. Auth. Weißnicht.
- RFC 1421
  Autor: IETF: J. Linn
  Titel: Privacy enhancement for Internet electronic mail: Part I: Message encryption and authentication procedures

- RFC 1422
Autor: IETF: S. T. Kent & J. Linn
Titel: Privacy enhancement for Internet electronic mail: Part II: Certificate-based key management
- RFC 1423
Autor: IETF: D. Balenson
Titel: Privacy enhancement for Internet electronic mail: Part III: Algorithms, modes and identifiers
- RFC 1424
Autor: IETF: B. Kaliski
Titel: Privacy enhancement for Internet electronic mail: Part IV: Key Certification and Related Services
- RFC 1446
Autor: IETF: J. Galvin & K. McCloghrie
Titel: Security Protocols for version 2 of the Simple Network Management Protocol (SNMPv2)
- RFC 1455
Autor: IETF: D. Eastlake
Titel: Physical Link Security Type of Service
- RFC 1457
Autor: IETF: R. Housley
Titel: Security Label Framework for the Internet
- RFC 1472
Autor: IETF:F. Kastenholz
Titel: The Definitions of Managed Objects for the Security Protocols of the Point-to-Point Protocol
- RFC 1492
Autor: IETF:C. Finseth
Titel: An Access Control Protocol, Sometimes Called TACACS
- RFC 1507
Autor: IETF:C. Kaufman
Titel: DASS - Distributed Authentication Security Service
Rubriken: Krypto. Auth. Weißnicht.
- RFC 1508
Autor: IETF: J. Linn
Titel: Generic Security Service Application Programm Interface
- RFC 1509
Autor: IETF: J. Wray
Titel: Generic Security Service API: C-bindings
- RFC 1510
Autor: IETF: J. Kohl & C. Neumann
Titel: The Kerberos Network Authentication Service (V5)
Rubriken: Krypto. Auth. Weißnicht.
- RFC 1511
Autor: IETF: J. Linn
Titel: Common Authentication Technology Overview
- RFC 1535
Autor: IETF: E. Gavron
Titel: A Security Problem and Proposed Correction With Widely Deployed DNS Software
- RFC 1636
Autor: IETF: R. Braden, D. Clark, S. Crocker & C. Huitema
Titel: Report of IAB Workshop on Security in the Internet Architecture (February 8-10, 1994)

- RFC 1675
  Autor: IETF: S. Bellovin
  Titel: Security Concerns for IPng
- RFC 1704
  Autor: IETF: N. Haller & R. Atkinson
  Titel: On Internet Authentication
  Rubriken: Krypto. Auth. Weißnicht.
- RFC 1710
  Autor: IETF: R. Hidden
  Titel: Simple Internet Protocol Plus White Paper
- RFC 1731
  Autor: IETF: J. Myers
  Titel: IMAP4 Authentication Mechanisms
  Rubriken: Krypto. Auth. Weißnicht.
- RFC 1734
  Autor: IETF: J. Myers
  Titel: POP3 AUTHentication command
  Rubriken: Krypto. Auth. Weißnicht.
- RFC 1750
  Autor: IETF: D. Eastlake, 3rd., S. Crocker & J. Schiller
  Titel: Randomnes Recommendations for Security
- RFC 1751
  Autor: IETF: D. McDonald
  Titel: A Convention for Human-Readable 128-bit Keys
- RFC 1760
  Autor: IETF: N. Haller
  Titel: The S/KEY One-Time Password System
- RFC 1805
  Autor: IETF: A. Rubin
  Titel: Location-Independent Data/Software Integrity Protocol
- RFC 1810
  Autor: IETF: J. Touch
  Titel: Report on MD5 Performance
- RFC 1824
  Autor: IETF: H. Danisch
  Titel: The Exponential Security System TESS: An Identity-Based Cryptographic Protocol for Authenticated Key-Exchange
- RFC 1825
  Autor: IETF: R. Atkinson
  Titel: Security Architecture for the Internet Protocol
- RFC 1826
  Autor: IETF: R. Atkinson
  Titel: IP Authentication Header
  Rubriken: Krypto. Auth. Weißnicht.
- RFC 1827
  Autor: IETF: R. Atkinson
  Titel: IP Encapsulating Security Payload (ESP)
- RFC 1828
  Autor: IETF: P.Metzger & W. Simpson
  Titel: IP Authentication using Keyed MD5
  Rubriken: Krypto. Auth. Weißnicht.
- RFC 1829
  Autor: IETF: P.Karn, P.Metzger & W. Simpson
  Titel: The ESP DES-CBC Transform

- RFC 1847
  Autor: IETF: J. Galvin, S. Murphy, S. Crocker & N. Freed
  Titel: Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted
- RFC 1848
  Autor: IETF: S. Crocker, N. Freed, J. Galvin & S. Murphy
  Titel: MIME Object Security Services
- RFC 1851
  Autor: IETF: P.Carn, P. Metzger & W. Simpson
  Titel: The ESP Triple DES Transform
  Rubriken: Krypto. Kryps. sym. adhoc. DES. Verwandte.
- RFC 1852
  Autor: IETF: P. Metzger & W. Simpson
  Titel: IP Authentication using Keyed SHA
  Rubriken: Krypto. Auth. Weißnicht.
- RFC 1853
  Autor: IETF: W. Simpson
  Titel: IP in IP Tunneling
- RFC 1858
  Autor: IETF: G. Ziemba, D. Reed & P. Traina
  Titel: Security Considerations for IP Fragment Filtering
- RFC 1864
  Autor: IETF: J. Myers & M. Rose
  Titel: The Content-MD5 Header Field
- RFC 1875
  Autor: IETF: N. Berge
  Titel: UNINETT PCA Policy Statements
- RFC 1910
  Autor: IETF: G. Waters, Editor
  Titel: User-based Security Model for SNMPv2
- RFC 1928
  Autor: IETF: M. Leech et al.
  Titel: SOCKS Protocol Version 5
- RFC 1929
  Autor: IETF: M. Leech
  Titel: Username/Password Authentication for SOCKS V5
  Rubriken: Krypto. Auth. Weißnicht.
- RFC 1938
  Autor: IETF: N. Haller et al.
  Titel: A One-Time Password System
- RFC 1948
  Autor: IETF: S. Bellovin
  Titel: Defending Against Sequence Number Attacks
- RFC 1949
  Autor: IETF: A. Ballardie
  Titel: Scalable Multicast Key Distribution
- RFC 1961
  Autor: IETF: P. McMahon
  Titel: GSS-API Authentication Method for SOCKS Version 5
  Rubriken: Krypto. Auth. Weißnicht.
- RFC 1964
  Autor: IETF: J. Linn
  Titel: The Kerberos Version 5 GSS-API Mechanism

- RFC 1968
  Autor: IETF:G. Meyer
  Titel: The PPP Encryption Control Protocol (ECP)
- RFC 1969
  Autor: IETF: K. Sklower & G. Meyer
  Titel: The PPP DES Encryption Protocol (DESE)
  Rubriken: Krypto. Kryps. sym. adhoc. DES. Verwandte.
- RFC 1984
  Autor: IETF: IAB & IESG
  Titel: IAB and IESG Statement on Cryptographic Technology and the Internet
  Rubriken: Motive. weißnicht.
- RFC 1991
  Autor: IETF: D. Atkins, W. Stallings & P. Zimmermann
  Titel: PGP Message Exchange Formats
- RFC 2015
  Autor: IETF: M. Elkins
  Titel: MIME Security with Pretty Good Privacy (PGP)
- RFC 2025
  Autor: IETF: C. Adams
  Titel: The Simple Public-Key GSS-API Mechanism (SPKM)
- RFC 2040
  Autor: IETF: R. Baldwin & R. Rivest
  Titel: The RC5, RC5-CBC, RC5-CBC-Pad, and RC5-CTS Algorithms
- RFC 2057
  Autor: IETF: S. Bradner
  Titel: Source Directed Access Control on the Internet
- RFC 2058
  Autor: IETF: C. Rigney, A. Rubens, W. Simpson & S. Willens
  Titel: Remote Authentication Dial In User Service (RADIUS)
  Rubriken: Krypto. Auth. Weißnicht.
- RFC 2059
  Autor: IETF: C. Rigney
  Titel: RADIUS Accounting
- RFC 2065
  Autor: IETF: D. Eastlake, 3rd & C. Kaufman
  Titel: Domain Name System Security Extensions
- RFC 2069
  Autor: IETF: J. Franks, P. Hallam-Baker, J. Hostetler, P. Leach, A. Luotonen, E. Sink & L. Stewart
  Titel: An Extension to HTTP: Digest Access Authentication
  Rubriken: Krypto. Auth. Weißnicht.
- SET 1
  Autor: Mastercard / VISA
  Titel: Secure Electronic Transaction (SET) Specification Book 1: Business Description DRAFT for testing
  Rubriken: Schutz. Werte.
- SET 2
  Autor: Mastercard / VISA
  Titel: Secure Electronic Transaction (SET) Specification Book 2: Programmer's Guide DRAFT for testing
  Rubriken: Schutz. Werte.
- SET 3
  Autor: Mastercard / VISA
  Titel: Secure Electronic Transaction (SET) Specification Book 3: Formal Protocol

Definition DRAFT for testing
Rubriken: Schutz. Werte.

- SP 500-189
  Autor: NIST
  Titel: Security in ISDN
  Rubriken: Netze. ISDN.
- SP 800-2
  Autor: NIST
  Titel: Public-key Cryptography
  Rubriken: Krypto. weißnicht.
- SP 800-3
  Autor: NIST
  Titel: Establishing a CSL Computer Security Incident Response Capability
  Rubriken: Weißnicht.
- SP 800-7
  Autor: NIST
  Titel: Security in Open Systems
- SP 800-8
  Autor: NIST
  Titel: Security Issues in the Database Language SQL
- TCRTR 028
  Autor: ETSI Europäisches Institut für Telekommunikationsnormen
  Titel: Security Techniques Advisory Group (STAG); Glossary of security technology
  Rubriken: Weißnicht.
- TCRTR 031
  Autor: ETSI Europäisches Institut für Telekommunikationsnormen
  Titel: Security Algorithms Group of Experts (SAGE) ; Universal Personal Telecommunication (UPT) authentication; Rules for the management of the USA-4
  Rubriken: Krypto. Auth. Weißnicht.
- TCRTR 037
  Autor: ETSI Europäisches Institut für Telekommunikationsnormen
  Titel: Security Techniques Advisory Group (STAG); Requirements specification for an encryption algorithm for operators of European public telecommunication networks
  Rubriken: Weißnicht.
- TCRTR 042
  Autor: ETSI Europäisches Institut für Telekommunikationsnormen
  Titel: Security Techniques Advisory Group (STAG); Baseline security standards; Features and mechanisms
  Rubriken: Weißnicht.
- Tene 97
  Autor: Jay M. Tenenbaum
  Titel: eCo System: CommerceNet's Architectural Framework for Internet Commerce
  Stichworte: Framework, E-Commerce, eco
- UL 1998
  Autor: Underwriters Laboratories Inc.
  Titel: Sicherheitsbezogene Software
  Rubriken: Weißnicht.
  Stichworte: Begriffe, Codierung, Datenverarbeitung, Fehlererkennung, Sicherheit, Zuverlässigkeit
- VDI-Dokumentnummer fehlt
  Autor: Verein Deutscher Ingenieure, VDI-Gesellschaft Entwicklung - Konstruktion - Vertrieb

Titel: Bürokommunikation; Informationssicherheit in der Bürokommunikation
Rubriken: Weißnicht.
Stichworte: Datenschutz, Datensicherheit, Datenverarbeitung, Sicherheit

- X. 802
  Autor: ITU Internationale Fernmeldeunion
  Titel: Information technology - Lower layers security model
  Rubriken: Weißnicht.

- X.273
  Autor: ITU Internationale Fernmeldeunion
  Titel: Information Technology - Open Systems Interconnection - Network Layer Security Protocol
  Rubriken: Weißnicht.

- X.274
  Autor: ITU Internationale Fernmeldeunion
  Titel: Information technology - Telecommunication and information exchange between systems - transport layer security protocol
  Rubriken: Schutz. Netze.

- X.803
  Autor: ITU Internationale Fernmeldeunion
  Titel: Information technology - Open Systems Interconnection - Upper layers security model

- X.831
  Autor: ITU Internationale Fernmeldeunion
  Titel: Information technology - Open Systems Interconnection - Generic upper layers security: Security Exchange Service Element (SESE) service definition

- X.832
  Autor: ITU Internationale Fernmeldeunion
  Titel: Information technology - Open Systems Interconnection - Generic upper layers security: Security Exchange Service Element (SESE) protocol definition

- X.833
  Autor: ITU Internationale Fernmeldeunion
  Titel: Information technology - Open Systems Interconnection - Generic upper layers security: Protecting transfer syntax specification

- X.834
  Autor: ITU Internationale Fernmeldeunion
  Titel: Information technology - Open Systems Interconnection - Generic upper layers security: Security Exchange Service Element (SESE) protocol implementation conformance statement

- X.835
  Autor: ITU Internationale Fernmeldeunion
  Titel: Information technology - Open Systems Interconnection - Generic upper layers security: Protecting transfer syntax Protocol Implementation Conformance Statements (PICS) proforma

- XOpe 96
  Autor: X/Open
  Titel: Generic Cryptographic Service API (GCS-API) Base - Draft 8
  Stichworte: Verteiltes System, Framework, Sicherheit

- Yell 96
  Autor: Frank Yellin
  Titel: Low Level Security in Java
  Stichworte: Java, Framework, Crypto

- Z74-200
  Autor: AFNOR

Titel: Informationstechnik. Schutz der dem Verteidigungsgeheimnis nicht unterliegenden empfindlichen Informationen. Empfehlungen für die Datenverarbeitungsarbeitsplätze
Rubriken: Motive. weißnicht.
Stichworte: Datenverarbeitung, Sicherheit, Technische Spezifikation

Literaturverzeichnis

[Adam_96] Dean Adams (Hrsg.); Security Survival: A Source Book from The Open Group; X/Open Company Ltd, Reading 1996

[Bisk1_93] Joachim Biskup; Probleme der Sicherheit in Rechensystemen; Unterlagen zu einer Vorlesung im SS 1993, Universität Hildesheim, 21.12.1993

[Broc_??] Der große Brockhaus

[BrSc_97] Jürgen Brauckmann, Matthias Schunter; Secure Communication Channels; SEMPER internal activity paper 235UD044; Version 4; 13.10.1997

[Brüg_94] Hans Herrmann (Jimmy) Brüggemann; Sicherheit in Informationssystemen; Vorlesungsnotizen SS 1994, Universität Hildesheim, Version 1.9, 4.7.1994

[CEN_91] CEN/CENELEC Geschäftsordnung; Juni 1991; in [DIN_95, Seiten 433 - 505]

[CEN_94] CEN Informationsbroschüre (1994)

[Cro_93] D. Crocker; Making Standards the IETF Way; Association for Computing Machinery; 1993; (Reprinted from StandardView, Vol. 1, No. 1, 1993(1)) in [http://www.ietf.org]

[DIN1_75] DIN Deutsches Institut für Normung e.V. Geschäftsordnung des Präsidiums; Oktober 1975; in [DIN_95, Seiten 13 - 26]

[DIN2_75] „Normenvertrag" - Vertrag zwischen der Bundesrepublik Deutschland, vertreten durch den Bundesminister für Wirtschaft, und dem DIN Deutsches Institut für Normung e.V., vertreten durch dessen Präsidenten; Bonn 1975; in [DIN_95]

[DIN_90] DIN Deutsches Institut für Normung e.V. Richtlinie für Normenausschüsse; Juni 1990; in [DIN_95, Seiten 65 - 79]

[DIN_91] DIN Deutsches Institut für Normung e.V. Satzung; 16.10.1991 in [DIN_95, Seiten 9 - 12]

[DIN_95] DIN Deutsches Institut für Normung (Hrsg.); Grundlagen der Normungsarbeit des DIN; Beuth, Berlin 1995

[DIN_95] DIN Deutsches Institut für Normung (Hrsg.); DIN-Memorandum zur IT-Normung; 1. Auflage; Beuth, Berlin 1990

[DIN_820] Deutsche Norm 820; Normungsarbeit; abgedruckt in [DIN_95]

[ECMA_96] ECMA Memento 1996, gefunden bei [http://www.ecma.org]

[EN_45020] Europäische Norm 45020 von 1993; Allgemeine Fachausdrücke und deren Definitionen betreffend Normung und damit zusammenhängende Tätigkeiten; abgedruckt in [DIN_95]

[Fait_94] Belinda Faithorne (Ed.), OMG Security Working Group; OMG White Paper on Security; Issue 1.0, April 1994

[FlZü_97] C. Floyd, H. Züllighoven; Softwaretechnik; Kapitel D14 in [RePo_97]

[Ford_94] Warwick Ford; Computer Communications Security - Principles, Standards, Protocols and Techniques; Prentice Halle, Englewood Cliffs 1994

[Heid_97] Antwort-Mail von wolfgang.heidrich@bapt.de, Wed Sep 17 11:55 MET 1997

[Inte1_97] Intel Corporation; Common Data Security Architecture Specification; Draft Release 1.2; March 1997

[Inte2_97] Intel Corporation; Common Security Services Manager, Cryptographic Service Provider Interface (SPI) Specification; Draft for Release 1.2; March 1997

[ISO_10181-1] ISO/IEC 10181-1; Information technology - Open Systems Interconnection - Security frameworks for open systems - Part 1: Overview

[ISOC_97] „Frequently Asked Questions" zur Internet Society; Version vom 10.3.1997; zu finden unter [http://www.isoc.org]

[MüPf_97] Günter Müller, Andreas Pfitzmann (Hrsg.); Mehrseitige sicherheit in der Kommunikationstechnik: Verfahren, Komponenten und Integration; Addison-Wesley-Longmann, Bonn Reading (Massachusetts) 1997

[Ohne_97] ohne Autorenangabe; Overview auf CORBA; http://www.cs.wustl.edu/s̃chmidt/corba-overview.html; Last modified 16:40:46 CDT 20 July 1997

[OMG_97] OMG; CORBAservices: Common Object Services Specification; Revised Edition - March 31, 1995, Updated: July 1997

[Open_96] The Open Group - Corporate Background; Mai 1996; zu finden unter [http://www.open-group.com]

[PCLe_94] Das große EDV & PC Lexikon; Isis Verlag AG; Chur/Schweiz 1994

[Pfit_90] Andreas Pfitzmann; Diensteintegrierende Kommunikationsnetze mit teilnehmerüberprüfbarem Datenschutz; Informatik-Fachberichte 234; Springer Verlag, Berlin Heidelberg New York 1990

[Pfit_93] Andreas Pfitzmann; Sicherheit in Rechnernetzen; Vorlesungsskript; Universität Hildesheim; WS 1992/93

[Priv_97] Private Kommunikation mit der Deutschen Elektrotechnischen Kommission im DIN und VDE (DKE), 21.8. / 1.9.1997

[RePo_97] Peter Rechenberg, Gustav Pomberger (Hrsg.); Informatik-Handbuch; Hanser Verlag, München Wien 1997

[RFC_1718] RFC 1718- The TAO of the IETF

[RFC_2026] RFC 2026 - The Internet Standards Process - Revision 3; Oktober 1996

[RFC_2078] RFC 2078 - Generic Security Service Application Program Interface, Version 2 (GSS-API); J. Linn; Januar 1997

[RSAD_95] RSA Laboratories; RSA Data Security, Inc. Public-Key Cryptography Standards (PKCS) #11: Cryptographic Token Interface Standard; Version 1.0, April 28, 1995

[SEMP1_96] SEMPER Consortium; Basic Services, Architecture and Design; Deliverable D03 of ACTS Project AC026; Public Specification; September 24, 1996

[StWi_97] Sebastian Staamann, Uwe G. Wilhelm; Mehrseitige Sicherheit in der Telecommunications Information Networking Architecture; [MüPf_97, S. 284-308]

[Tane_97] Andrew S. Tanenbaum; Computernetzwerke; Prentice Hall, Haar 1997

[TINA_97] TINA Consortium; Network Resource Architecture; TINA-C Deliverable; Version 3.0; Februar 1997; zu finden unter [http://www.tinac.com]

[Wagn_93] Robert Wagner; OMG setzt Standards - Object-World 92 in Wiesbaden; c't 1/93, S. 22 (it)

[WaPP_87] Michael Waidner, Birgit Pfitzmann, Andreas Pfitzmann; Über die Notwendigkeit genormter kryptographischer Verfahren; in „DuD, Datenschutz und Datensicherung, Recht und Sicherheit der

Informations- und Kommunikationssysteme“; Vieweg & Sohn, Wiesbaden, Heft 6 / Juni 1987, Seite 293-299

[WPSW_97] Gritta Wolf, Andreas Pfitzmann, Alexander Schill, Guntram Wicke, Jan Zöllner; Sicherheitsarchitekturen: Überblick und Optionen; [MüPf_97, S. 221-251]

[WSWZ_97] Uwe G. Wilhelm, Sebastian Staamann, Gritta Wolf, Jan Zöllner; Sicherheit in CORBA und TINA; [MüPf_97, S. 267-284]

[XOpe2_96] X/Open Company Ltd.; Generic Cryptographic Service API (GCS-API) Base - Draft 8; X/Open Preliminary (1996) (Draft April 20, 1996), X/Open Company Ltd, Apex Plaza, Forbury Road Reading Berkshire RG1 1AX, UK,

[XOpe_??] X/Open Company Ltd.; Comparison of The Open Groups GCS-API and Microsoft Crypto API Version 1.0; auf [http://www.open-group.com];

[ZaEh_96] K. Zangeneh, H. Ehmke; Specification of the Cryptographic Manager; SEMPER internal activity paper 221GM013; Version 3; 20.02.1996

[Johnson 88] Johnson, R.; Foote, B.: Designing reuseable classes. Journal of Object-Oriented Programming 1/2 (1988) 22-35

[http://www.bapt.de] WWW-Seiten des BAPT; http://www.bapt.de; Juli 1997

[http://www.dfn-cert.de] WWW-Seiten des DFN-CERT; http://www.dfn-cert.de; Juni 1997

[http://www.din.de] WWW-Seiten des DIN; http://www.din.de; Juni 1997

[http://www.ecma.org] WWW-Seiten der ECMA; http://www.ecma.org; Juni 1997

[http://www.etsi.org] WWW-Seiten des ETSI; http://www.etsi.org; Juli 1997

[http://www.iab.org] WWW-Seiten des IAB; http://www.iab.org; Juli 1997

[http://www.iesg.org] WWW-Seiten der IESG; http://www.iesg.org; Juli 1997

[http://www.ietf.org] WWW-Seiten der IETF;
http://www.ietf.org;
Juli 1997

[http://www.intel.com] WWW-Seiten der Intel Corp.;
http://www.intel.com;
Januar 1998

[http://www.irtf.org] WWW-Seiten der IRTF;
http://www.irtf.org;
Juli 1997

[http://www.iso.org] WWW-Seiten der ISO;
http://www.iso.org;
Juni 1997

[http://www.isoc.org] WWW-Seiten der ISOC;
http://www.isoc.org;
Juli 1997

[http://www.itu.org] WWW-Seiten der ITU;
http://www.itu.org;
Juni 1997

[http://www.omg.org] WWW-Seiten der Object Management Group;
http://www.omg.org;
Oktober 1997

[http://www.sis.se] WWW-Seiten des SIS;
http://www.sis.se;
Juni 1997

[http://www.open-group.com] WWW-Seiten der Open Group;
http://www.open-group.com;
Juni 1997

[http://www.tinac.com] WWW-Seiten des TINA-C;
http://www.tinac.com;
Oktober 1997

[http://www.vde.de] WWW-Seiten des VDE;
http://www.vde.de;
Juli 1997

Index