Trustcenter und Multifunktionskarten

Autor: Univ. Prof. Dr. sc. Christoph Meinel
Coautoren: Dipl.-Inform. Lutz Vorwerk,
Dr. nat. rer. Thomas Engel

Inhaltsverzeichnis

1. **Motivation für die Multifunktionalität einer Chipkarte**
2. **Skalierbarkeit als Vorteil multifunktionaler Karten**
3. **Planung der Multifunktionalität**
4. **Einsatz multifunktionaler Karten durch Trustcenter**
5. **Zusammenfassung**
6. **Literatur**

Trustcenter und Multifunktionskarten

1. Motivation für die Multifunktionalität einer Chipkarte

Dieser Text soll dem Verständnis des Themas „multifunktionale Karten und Trustcenter“ beitragen, so dass auch solche Leser, die sich nicht mit den technischen Einzelheiten auskennen, einen Einblick in das Thema bekommen können. Es werden Einsatzmöglichkeiten von multifunktionalen Karten beschrieben. Ebenso wird auf die Struktur solcher Karten eingegangen. Anschließend werden der Aufbau und die einzelnen Komponenten eines Trustcenters beschrieben und mit den multifunktionalen Karten in Verbindung gebracht. Abschließend folgt ein Beispiel für den Einsatz einer multifunktionalen Karte mit Hilfe eines Trustcenters.

Eine Vielfalt von Karten für die Nutzung von Geldautomaten, Parkhäusern, Krankenversicherung, Bibliothek oder Telephon usw. füllen derzeit statt des Geldes das Portemonnaie. Eine Reduktion dieser Kartenvielfalt könnte durch die Einführung einer Multifunktionskarte erreicht werden. Auf einer solchen Karte sind, wie der Name schon sagt, mehrere unterschiedliche Funktionen vereint. Vorstellbar wäre z.B. eine Karte, die alle oben genannten Eigenschaften in sich vereint. Sie könnte sowohl zum Ausleihen eines Buches als auch als Legitimation zur Inanspruchnahme einer Krankenversicherung bei einem Zahnarztbesuch verwendet werden. (Nach wie vor müssen aber personenbezogene Daten, wie z.B.: Wie oft und wann der Kartenbesitzer einen bestimmten Arzt besucht oder ein bestimmtes Buch ausgeliehen hat, dezentral verwaltet werden, da sonst sehr leicht die Angst vor dem „gläsernen Menschen“ Realität werden könnte [RZ99].) Bei führenden Kartenherstellern und auf dem renommierten Chipkarten-Kongress Omnicard, wird die Meinung vertreten, dass z.B. die als Karte angebotene „elektronische Geldbörse“ in ihrer Attraktivität deutlich gesteigert werden könnte, wenn anstelle der „einfachen“ Karte eine multifunktionale Karte verwendet würde.
Auch für den Einkauf im Internet eignen sich Multifunktionskarten hervorragend. Mit Hilfe eines einfachen Kartenlesegerätes können Beträge, die sich auf der Chipkarte befinden, abgebucht werden.

Die zur technischen Realisierung von Multifunktionskarten notwendigen SmartCards sind am Markt verfügbar; Beschaffung und „Programmierung“ sind kein Problem.

2 Skalierbarkeit als Vorteil multifunktionaler Karten

An welchen Stellen derzeit Bedarf an multifunktionalen Karten besteht, lässt sich aus den Gründen ersehen, zu welchem Zweck die Nutzung einer „uni-funktionalen Karte“ eingeführt wurde. Aus den Anschaffungsgründen, können die am meisten genutzten Karten abgeleitet werden und daraus eine multifunktionale Karte geschaffen werden. Diese Karte ist zunächst eine allgemeine multifunktionale Karte, für die weitere Funktionen beantragt werden können. Die Funktionen auf einer durch mehrfache Antragsstellung an den Karteninhaber angepassten individuellen multifunktionale Karte könnten sein:

- Zahlungsverkehr,
- Zutritt / sicherer Zugang,
- Anwesenheit / Benutzungskontrolle,
- tragbare Datenhaltung .

Die Abbildung auf der nächsten Seite zeigt eine mögliche Klassifikation von Anwendungsfeldern.

Die am meisten verwendete Funktion einer multifunktionalen Karte ist das Bezahlen der durch die Karte zugänglich gemachten Dienstleistungen. Die Funktion „elektronische Geldbörse“ ist demzufolge eine der Funktionen einer allgemeinen multifunktionalen Karte. Bei multifunktionalen Karten kann zwischen permanenten Funktionen und Funktionen mit bestimmter Lebensdauer unterschieden werden.

Die Anforderungen an Multifunktionalität lassen sich mit den folgenden Hypothesen zusammenfassen [Kre93]:

- *Konsumentenwunsch*: Konsumenten bevorzugen eine einzige Karte, auf welcher mehrere Leistungen sinnvoll vereint sind - im Gegensatz zu mehreren Karten, die jede für sich wieder nur die eine fast gleiche Leistung enthalten.

- *Zeitfenster*: Der Konsumentenwunsch ist technisch und organisatorisch nur während eines engen Zeitfensters erfüllbar.

Die besonderen Anforderungen des Bankensektors an multifunktionale Chipkarten sind vor allem:

- Reduzierung der operativen Kosten (so viel offline Transaktionen, wie sinnvoll und möglich)

- Erbringung von zusätzlichen Leistungen zu den eigenen Kundenkarten, um durch die hinzugefügten Eigenschaften eine Kundenbindung zu ermöglichen.

- Stufenweise Aktivierung dieser Zusatzleistungen.

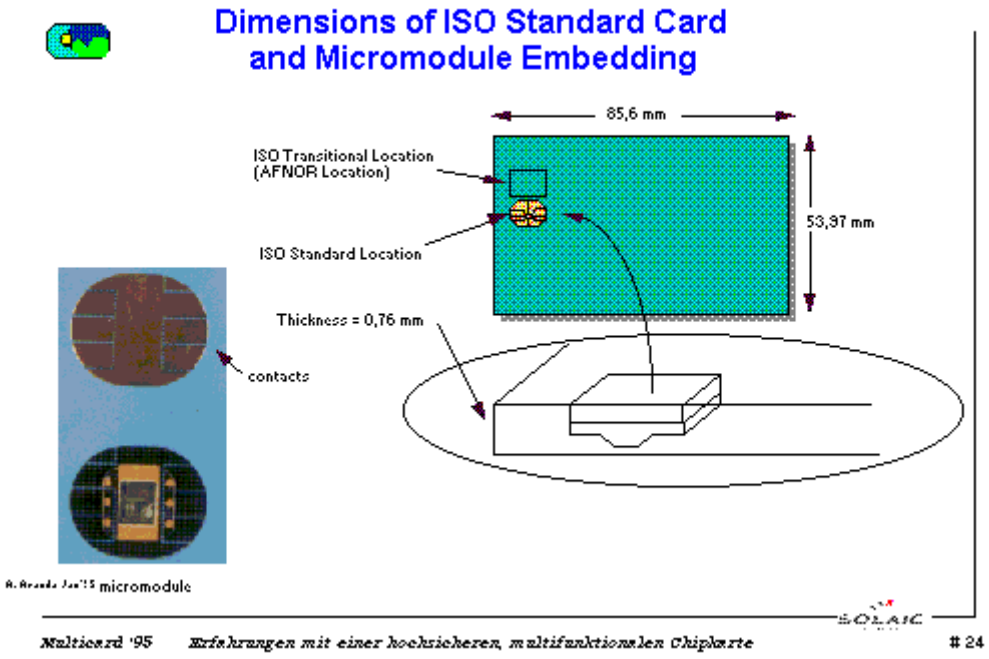
Im letzten Punkt wird ein schon erwähnter und wichtiger Aspekt betrachtet, welcher hinzuzufügende Funktionen (Zugang zu Dienstleistungen) auf multifunktionale Karten erwirkt, die sich bereits im Umlauf befinden. Für eine multifunktionale Karte sind insbesondere durch das Hinzufügen und das Entfernen des Zuganges zu

Dienstleistungen (Funktionen) besondere Sicherheitsanforderungen erforderlich. Diese Sicherheitsanforderungen an multifunktionale Chipkarten sind :

- korrekte Verarbeitung der Daten auf einer multifunktionalen Karte
- Verfügbarkeit von Kartenlesegeräten und Anwendungen sowie eine einwandfreie und funktionsfähige multifunktionale Karte
- Wiederherstellung verlorengegangener Daten (Fehlertoleranz)
- die Kartendaten dürfen nur dem Eigentümer der Karte zugänglich sein (Vertraulichkeit)
- Identifikation des Karteneigentümers als Zugangsschutz zu Anwendungen (Authentisierung)

3 Planung der Multifunktionalität

Welche Funktionen auf einer multifunktionalen Karte untergebracht werden sollen und wie diese Funktionen geschützt werden müssen erfordert eine sorgfältige Planung und Evaluierung der benötigten Funktionen. Auf den multifunktionalen Karten kann nicht alles untergebracht werden.

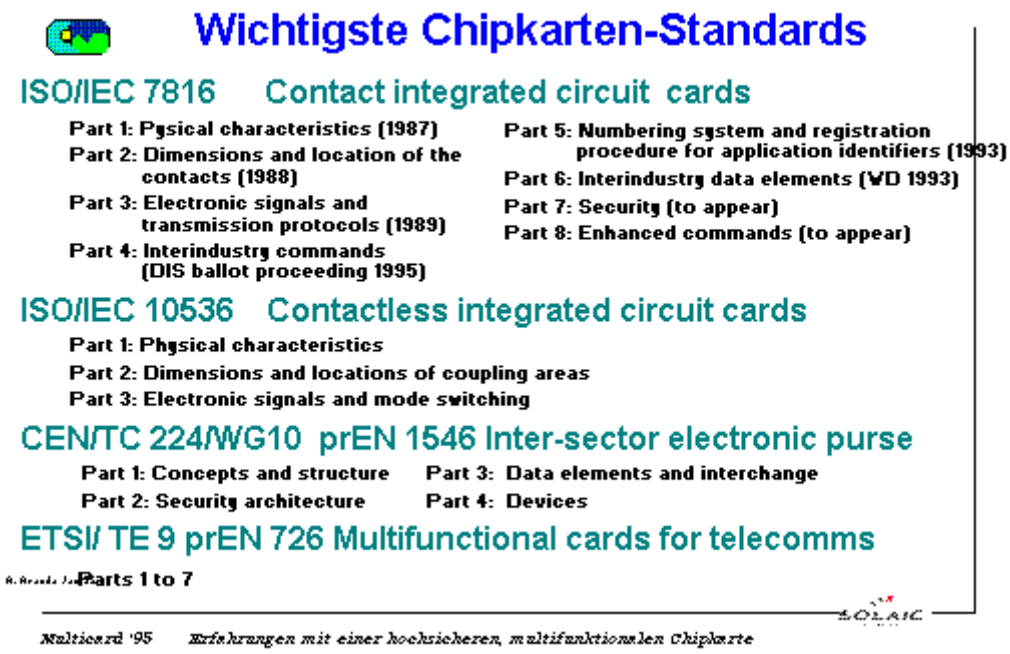


Die Idee einer nationalen, branchenübergreifenden multifunktionalen Lösung auf einem Chip wurde in den vergangenen Jahren vorgeschlagen [Kre93] und wegen organisatorischer Probleme zurückgestellt. Interessanterweise wurde 1994 ein erneuter Versuch hinsichtlich Multifunktionalität gestartet [Kre94], mit dem neuen Ansatz, mehrere Chips auf einer Karte unterzubringen, wobei jeder Chip eine eigene Anwendung kontrollieren würde. Die Idee setzte sich nicht durch. Der Ansatz, branchenübergreifende Multifunktionalität mit

mehreren dedizierten Chips auf einer Karte, die statt einem Mikrochip mehrere enthält, zu verwirklichen, wurde aufgegeben.

Deshalb muss eine Konvention im Hinblick auf die Verteilung der Daten und der Software auf multifunktionale Karte und unterstützendes System gemacht werden. Um diesen Umstand zu verdeutlichen, wurde mit Hilfe der Abbildung der vorigen Seite der Aufbau einer multifunktionale Karte dargestellt.

Aus Kompatibilitätsgründen ist eine einheitliche Dicke, Größe, Biegsamkeit, Position des Kontaktfeldes (bei kontaktbehafteten Karten) von Karten wichtig. Das Kontaktfeld dient dem Datenaustausch zwischen Kartenlesegerät und Kartenmikrochip. Bei kontaktbehafteten Karten wurde durch den Standard ISO 7816-2 (1988) die Anzahl, Form und Position der Kontakte festgelegt [mc95]. Es gibt neben kontaktbehafteten Karten noch die kontaktlosen. Diese Karten stellen den Kontakt zum Lesegerät nicht durch das Einführen der Karte in den Schlitz des Lesegerätes her. Bei dieser Art von Karten reicht es aus, dass die Karte in die Nähe des Lesegerätes gebracht wird.



Die Sicherheit kontaktloser Karten ist fraglich, da heutzutage noch keine Standards für die Verwendung von Infrarot und Hyperfrequenzen existieren, auf denen Sicherheitsanforderungen basieren könnten. Es wird also zunächst das Hauptaugenmerk auf den kontaktbehafteten Karten liegen. Die wichtigsten Chipkarten-Standards für kontaktbehaftete, kontaktlose, „elektronischer Geldbörse“ und Multifunktionalität sind auf der Abbildung dieser Seite dargestellt.

4 Einsatz multifunktionaler Karten durch Trustcenter

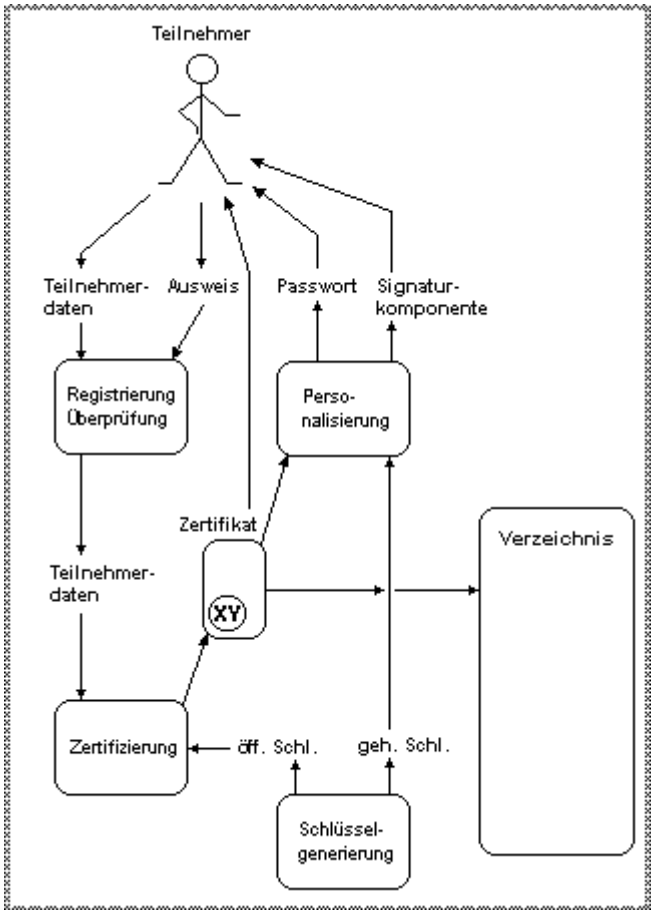
Der Einsatz von multifunktionalen Karten mit Hilfe eines Trustcenters erfordert zunächst, wie oben beschrieben, eine Planung, welche Daten auf der Karte gespeichert werden sollen und zu welchen Funktionalitäten (Dienstleistungen) die Karte Zugang ermöglichen soll. Dazu ist es wichtig zu wissen, wie ein Trustcenter aufgebaut ist und welche Rolle die Karte innerhalb eines Trustcenter spielen soll.

Ein Trustcenter [ti97], [ti98] bedient sich einer Registrierungsstelle, in der alle personenbezogenen Daten, die für den Inhalt eines Zertifikates wichtig sind aufgenommen werden (Die Abbildung auf der nächsten Seite verdeutlicht das Szenario das nun weiter beschrieben werden soll.). Die zu den Daten gehörende Person, also der Antragsteller, wird in der RA identifiziert und überprüft. Dies kann mit Hilfe seines Personalausweises geschehen oder auf andere geeignete Weise, wie z.B. werden für Mitarbeiter eines Betriebes Zertifikate ausgestellt so ist nur eine Bestätigung des Personalbüros notwendig, dass alle für ein Zertifikat notwendigen

Daten vorliegen. Der Antragsteller erhält die allgemeinen Geschäftsbedingungen sowie eine Aufklärung über einen verantwortungsvollen Umgang mit seinem Zertifikat. Als Kenntnisnahme unterschreibt der Antragsteller dann die Dokumente.

Das Trustcenter hat nun die Aufgabe einen geheimen Schlüssel zu erzeugen, den nicht einmal der Antragsteller kennen darf. Vorzugsweise geschieht die Erzeugung des geheimen Schlüssels gemeinsam mit einem dazugehörenden öffentlichen Schlüssel auf der Karte. Die Karte muss also als „Standarddienstleistung“ für die Verwendung in einem Trustcenter diese Schlüsselerzeugung bieten.

Skizzierung einer Ablauforganisation



Im weiteren Verlauf verbleibt der öffentliche Schlüssel im Trustcenter. Aus dem öffentlichen Schlüssel wird gemeinsam mit den personenbezogenen Daten des Antragstellers ein digitales Zertifikat erstellt. Dieses Zertifikat wird dem Antragsteller zugänglich gemacht, so das dieser es auf seiner Karte, auf der sich der geheime Schlüssel befindet und die ihm vorher vom Trustcenter zugestellt wurde, das Zertifikat speichern kann. Nun ist es dem Antragsteller überlassen, wer zusätzlich zum Trustcenter sein Zertifikat erhalten soll.

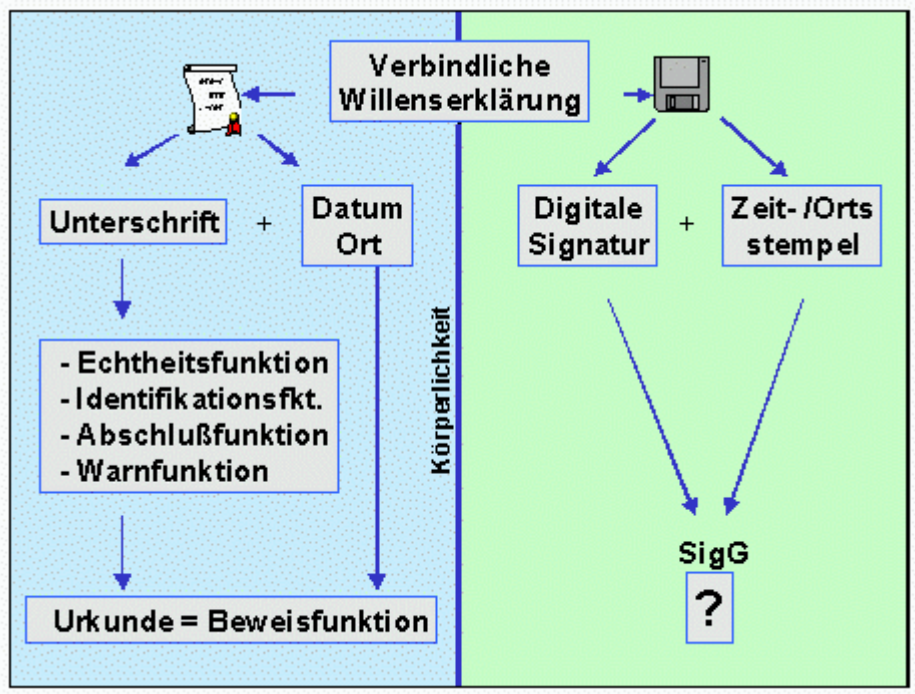
Der Antragsteller kann das Zertifikat nun zum Signieren und/oder Verschlüsseln von Daten verwenden (siehe Abbildung auf der folgenden Seite). Die Überprüfung, ob das Zertifikat gültig ist, wird vom Verzeichnisdienst

des Trustcenter übernommen, welches das Zertifikat ausgestellt hat. Im Idealfall gibt es einen weltumspannenden Verzeichnisdienst, der die Zertifizierungsinstanz (Certificate Authority) als Verzeichnis hat. Ein Zertifikat gewährt innerhalb dieses Verzeichnisses bestimmte Zugriffsrechte. In der Realität gibt es mehrere Verzeichnisbäume, die über „Crosszertifizierungen“ miteinander in Verbindung stehen. Bei „Crosszertifizierungen“ tauschen die (Policy)-Zertifizierungsinstanz der Trustcenter Zertifikate untereinander aus, um so den Zugriff auf ihre Verzeichnisse einer anderen Policy-Zertifizierungsinstanz zu gestatten und deren Verzeichnis dem eigenen hinzufügen zu können. Ein Beispiel hierfür wäre die Fusion zweier Firmen.

Es wäre denkbar, das eine Person bei unterschiedlichen Trustcentern Anträge gestellt hat. Die geheimen Schlüssel und Zertifikate könnten auf einer Karte gespeichert werden. Da „Crosszertifizierungen“ nicht die Regel sind, bieten Multifunktionskarten vorerst eine Alternative.

Um Zertifikate auf ihre Gültigkeit prüfen zu können und damit der Verzeichnisdienst der Zertifizierungsinstanz, welche das Zertifikat ausgestellt hat, nicht überlastet wird, werden Sub-Zertifizierungsinstanzen durch Zertifizierung geschaffen. Diese Sub-Zertifizierungsinstanz enthalten alle notwendigen Informationen über diejenige Benutzergruppe, welche sie verwalten müssen.

Beispiel für Antragsstellung und Nutzung von Zertifikaten



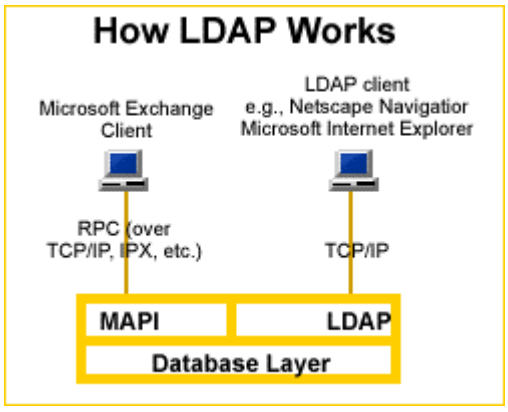
Damit die Gültigkeit eines Zertifikates geprüft werden kann wurden sogenannte Certificate Revocation Lists oder kurz CRL eingeführt.

Ein Signaturschlüssel-Zertifikat könnte folgendermaßen aussehen[taet97]:

Name des Signaturschlüssel-Inhabers	Peter Meier
öffentlicher Signaturschlüssel	jöSK9EkQPYTCjkhg8njKAAhl...
Bezeichnung der Algorithmen	RSA
laufende Nummer	4711
Beginn und Ende der Gültigkeit	gültig 01.01.98 - 31.12.2003
Name der Zertifizierungsstelle	Zertify GmbH
Angaben, ob die Nutzung des Signaturschlüssels auf bestimmte Anwendungen nach Art und Umfang beschränkt ist	keine Einschränkung

Die Idee von Browsern aus Verzeichnisdienste zu verwalten wurde durch das LDAP (Lightweight Directory Access Protokoll) begünstigt. LDAP basiert auf DAP (Directory Access Protokoll), welches wiederum eine Vereinfachung des Standards X.500 [X500] darstellt. Die folgende Abbildung zeigt an einem Beispiel, wie LDAP eingesetzt werden kann.

Beispiel für einen Verzeichnisdienst [lda98]



Durch Hinzunahme von SSL (Secure Socket Layer) basierend auf dem Standard X.509 [X509] wird für die Sicherheit der Verbindungen zwischen Client und Server garantiert. Um über Login und Passwort die Gruppenzugehörigkeit einer Person festlegen zu können, muss diese Person bei einer Zertifizierungsinstanz ein Zertifikat beantragen. Ein Beispiel für eine Zertifizierungsinstanz ist Verisign. Diese Zertifizierungsinstanz stellt für 60 Tage kostenlos ein Zertifikat zur Verfügung mit dessen Hilfe Emails signiert (digitale Unterschrift) und

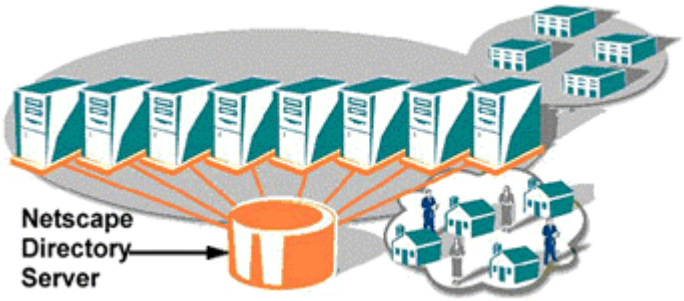
verschlüsselt werden können. Voraussetzung für eine Verschlüsselung ist der S/MIME(Secure MIME)-Mechanismus.

Die Kommunikation zwischen Server und Client über SSL geschieht folgendermaßen. Der Server schickt ein Zertifikat an den Client mit einem öffentlichen Schlüssel. Der Client verifiziert das Zertifikat bei einer Zertifizierungsinstanz und beginnt bei erfolgreicher Identifikation mit dem Transfer von mit dem öffentlichen Schlüssel verschlüsselten Daten. Der Server dekodiert die empfangenen Daten mit seinem privaten Schlüssel.

Der Client sendet nun sein Zertifikat, um sich beim Verzeichnisdienst (Server) zu authentifizieren. Der Verzeichnisdienst prüft seinerseits das Zertifikat bei einer Zertifizierungsinstanz. Bei erfolgreicher Identifikation liegen die Rechte (lesen, schreiben) und Sichten, welche der Client bei dem Verzeichnisdienst hat bereits fest. Der Client hat sich durch seine Authentifizierung in seine Rolle als Administrator, Verzeichnisbeauftragter, Leser, Verleger oder Autor begeben. Das Zertifikat des Clients enthält ebenfalls einen öffentlichen Schlüssel. Ist das Zertifikat des sich authentifizierenden Verzeichnisdienst-Nutzers akzeptiert worden, kann dieser ohne erneute Angabe von Passwort und Login den Verzeichnisdienst gemäß den ihm zugeordneten Rechten nutzen. Dieses Verfahren wird als „Einmalunterschrift“ (engl. single sign on) bezeichnet. In diesem Konzept wird die Netscape-Suite-Spot-Programmpacket als Verwaltung von LDAP, SSL und Zertifikatsmechanismus eingesetzt. In dem Packet übernimmt die Verzeichnisverwaltung des Personalbestandes der Verzeichnisdienst und die Verwaltung der Zertifikate die Zertifikatsverwaltung. Ebenso übernimmt die Zertifikatsverwaltung die Rolle einer Zertifizierungsinstanz. Die Zertifikate von Personen, Verzeichnisdienst und Zertifikatsverwaltung enthalten alle den distinguished name (dn) ihres Besitzers. Dieser dn dient der Einordnung des angemeldeten Servers oder der angemeldeten Person in die Hierarchie des Verzeichnisdienstes und setzt sich aus Knotenbezeichnern im Verzeichnisbaum zusammen. Durch den dn wird die Rolle des Besitzers des Zertifikates bestimmt.

Die Abbildung auf dieser Seite stellt den eine besondere Eigenschaft der

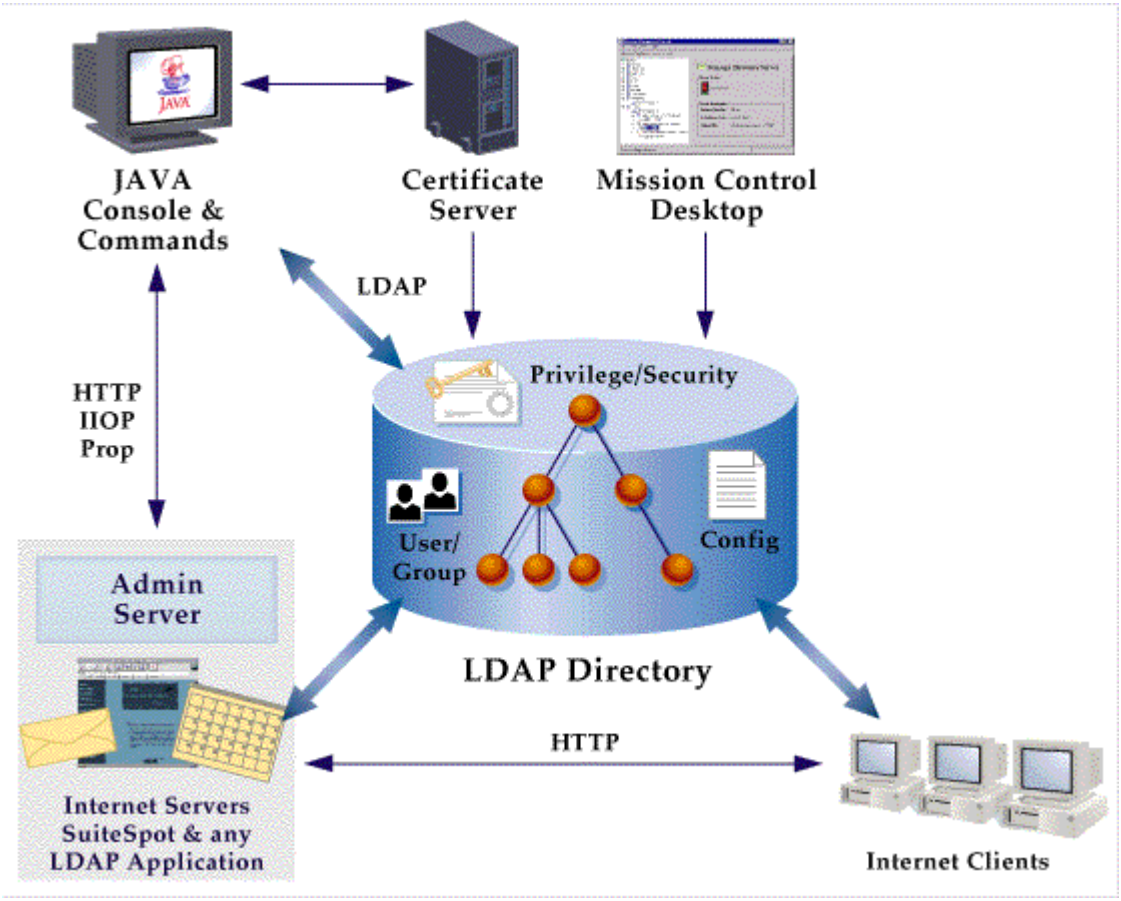
Die besondere Eigenschaft eines Verzeichnisdienstes [dir99]



In der Abbildung der nächsten Seite ist das Zusammenspiel von Zertifikatsdienst und Verzeichnisdienst. Der Verzeichnisdienst wird hier nicht allein zum Verwalten der Zertifikate genutzt, sondern zusätzlich für die Verwaltung von Benutzerrechten eingesetzt. Es wird also bei der Anmeldung mit Hilfe einer multifunktionale Karte zunächst überprüft, ob das Zertifikat, das sich auf der Karte befindet, gültig ist und danach die Resourcen freigegeben auf die der Besitzer der Karte Zugriff hat. Der in der Abbildung dargestellte Aufbau basiert auf Komponenten der Netscape Suite Spot. Für die Konfiguration in diesem System dienen die administrative

Komponente sowie eine Komponente für die Skalierung und Anpassung des Systems an einen bestimmten Verwendungszweck. Der Verzeichnisdienst verwaltet Internet Clients, die Anträge auf Ressourcenzuteilung mit Hilfe von multifunktionale Karte stellen.

Beispiel für ein Trustcenter [mc98]



5. Zusammenfassung

Mit der zunehmenden Akzeptanz von Public Key Infrastrukturen und dadurch erforderlichen Trustcentern, entstand, wie überall zunächst das Problem der eilig auf den Markt gebrachten proprietären Systeme. Eine Verbindung dieser Systeme (Trustcenter) zu einem weltumspannenden Netzwerk, wird durch die Verwendung des LDAP-Standards ermöglicht. Bis dahin ist es zumindest, was die Trustcenter angeht, noch ein weiter Weg.

Zur Zeit existieren die Trustcenter noch weitestgehend nebeneinander und bedienen sich der „Crosszertifizierung“, um eine Verbindung herzustellen. Diese Verbindungsart ist jedoch nicht immer gegeben.

Hat ein Karteninhaber Zugang zu unterschiedlichen Trustcentern, die nicht durch „Crosszertifizierung“ miteinander Verbunden sind, so ist eine Multifunktionskarte sinnvoll, da sie die Verwendung mehrerer Karten

erspart. Die technischen Eigenschaften und die Anwendungsgebiete von multifunktionalen Karten sind in [Multi99-1] und [Multi99-2] ausführlich behandelt worden. [Kry98] gibt einen umfassenden Überblick über die Struktur und Konzeption eines Trustcenters nach dem deutschen Signaturgesetz, das Richtlinien für die verwendete Soft- und Hardware, wie auch der Gebäudeinfrastruktur gibt.

6 Literatur

[dir99] **Netscape Communications Corporation**, http://developer.netscape.com/tech/directory/directory.html,1999, (letzter Zugriff Januar 2000)

[Kre93] **Kreft, H. D. (1993)**, *Zur Multiapplikation*, Vortrag in Köln beim Arbeitskreis Multiapplikationskarte am 6. Mai 1993.

[Kre94] **Kreft, H. D. (1994)**, *Combi Card am SmartCard Markt*, Vortrag in Frankfurt am 19. Juli 1994.

[Kry98] **TeleTrusT(1998)**, Kryptoreport, Kryptographische Verfahren im Gesundheits- und Sozialwesen

[Kub94] **Kubicek, H. und Klein, S. (1994)**, *Co-Organisation - Wege zur Uberwindung der Organisationslücke bei branchenübergreifenden Kartenlösungen*, Kongreßdokumentation Multicard '94, Berlin.

[lda98] **Microsoft and/or its suppliers**, http://aries.synet.edu.cn/guocj/directory/paper/corp/ms/msldap.html**,** 1998, (letzter Zugriff Januar 2000)

[mc98] **Microsoft and/or its suppliers,** http://developer.netscape.com/docs/wpapers/missionc/mcdev.html, 1998, (letzter Zugriff Januar 2000)

[Multi99-1] **Graf, H., Meinel, Ch, Engel, Th (1999),** `Multifunktionale Karten – Teil 1: Technischer Überblick‘, Studie am Institut für Telematik e.V. (Trier)

[Multi99-2] **Lüpken, B. , Meinel, Ch., Engel Th.(1999),** `Multifunktionale Karten – Teil 2: Anwendungspotentiale`, Studie am Institut für Telematik e.V. (Trier)

[Per94] **Perez Soria, J. M.. (1994)**, *The Spanish electronic purse system*, Kongreßdokumentation Smart Card Europe '94, London.

[PKI98] **TeleTrusT Deutschland e.V.** , http://www.teletrust.de/wf/pki.htm, 1998, (letzter Zugriff Januar 2000)

[Rod94] **Rodriguez Bonachera, E. (1994)**, *The SEMP multi-function card in Spain*, Kongreßdokumentation Cartes '94, Paris.

[TC98] **Security Team der TU-Berlin**, Erweiterte EMail für den Einsatz in Management und Verwaltung, http://hatch.prz.tu-berlin.de/trustcenter/TrustCenter/TAbstract/, 1998, (letzter Zugriff Januar 2000)

[X500] **Computer Networks Destinations® Home, Aloni Systems**, http://www.aloni.com/CND/CNDest.asp?TOCId=IPFamily&TopicID=X500,1999, (letzter Zugriff Januar 2000)

[X509] **R. Housley, SPYRUS, W. Ford, VeriSign, W. Polk, NIST, D. Solo, Citicorp**, Network Working Group Request for Comments: 2459, Category: Standards Track , Internet X.509 Public Key Infrastructure, Certificate and CRL Profile, http://www.cis.ohio-state.edu/htbin/rfc/rfc2459.html

[RZ99] **Rhein-Zeitung Online**, http://rhein-zeitung.de/on/99/03/04/topnews/cebcard.html, 1999, (letzter Zugriff Januar 2000)

[mc95] **A. Aranda**, **SOLAIC Smart Cards**, **Groupe SLIGOS, Frankfurt/Main**, Erfahrungen mit einer hochsicheren, multifunktionalen Chipkarte für Bankenanwendungen, http://www.winforms.phil.tu-bs.de/winforms/company/solaic/mulcar95/mulcar95.html, 1995, (letzter Zugriff Januar 2000)

[taet97] **Der Landesbeauftragte für den Datenschutz Schleswig-Holstein**, Tätigkeitsbericht, http://www.rewi.hu-berlin.de/Datenschutz/DSB/SH/material/tb/tb20/kap7.htm, 1997, (letzter Zugriff Januar 2000)

[ti97] **Hans-Jürgen Görg, Stephan Müller, Thomas Engel, Christoph Meinel,** Trust Center - Konzeption einer Zertifizierungsstelle nach Signaturgesetz und Signaturverordnung, 1997

[ti98] **Hans-Jürgen Görg, Thomas Engel, Christoph Meinel** ,TI-Trust Center - Eröffnung einer Zertifizierungsstelle in Anlehnung an das Signaturgesetz und die Signaturverordnung,1998