Modell für den Einsatz von JavaCards im Gesundheitswesen

L. Vorwerk, B. Lüpken, F. Losemann, T. Engel, Ch. Meinel

Institut für Telematik

Zusammenfassung

In dem folgenden Text werden Public Key Infrastrukturen (PKI) diskutiert, die benutzt werden, um dem Public Key Benutzerinformationen zuzuordnen. Patientenkarten dienen hierbei als Aufbewahrungsort für Schlüssel (Private Key). Zu einer PKI gehören Einrichtungen, die Organisation, Verwaltung und Pflege von Schlüsselpaaren (pubic und private key), bzw. damit direkt verbundenen Gegenständen, Diensten und Dienstleistungen zur Verfügung stellen. Ebenfalls müssen Protokolle und Standards entwickelt werden, bevor die Infrastruktur stabil funktionieren kann. Das Einsatzgebiet für Patientenkarten in Verbindung mit einer PKI ist die Entwicklung von Multimediale, elektronische Patientenakten.

Multimediale, elektronische Patientenakten sind Teil eines patientenorientierten Gesundheitsmodells. Die Verbindung dieses Modells zu einer Patientenkarte, genauer einer multifunktionalen Karte, soll näher betrachtet werden. Diese Art der Patientenkarte wird benutzt, um bestimmte Informationen verschlüsselt zu speichern und kann als Health Professional JavaCard (HPJC), die vom JavaCard Forum entworfen wurde, implementiert werden. Diese HPJC ist konfigurierbar und wurde an das Gesundheitsmodell, das im folgenden Text besprochen wird, angepasst. Eine multifunktionale JavaCard kann verschiedene Applikationen ausführen [3]. Die JavaCard API 2.1 [2] wurde eingesetzt [4], um die HPJC zu implementieren [1]. Der folgende Text wird eine Patientenkarte behandeln, die von dem Institut für Telematik vorgeschlagen wurde, um in bestimmten Testfällen eingesetzt werden zu können. Multifunktionale Patientenkarten und das Übertragen von Rezepten wurden hierbei berücksichtigt. In dem Szenario befindet sich der Public Key des Arztes auf der Patientenkarte. Der Patient kann den symmetrischen Schlüssel des Arztes mit dessen Public Key entschlüsseln und auf diese Weise den Arzt identifizieren. Der Patient entschlüsselt jetzt den entstandenen symmetrischen Schlüssel mit seinem Public Key. Der Apotheker benutzt seine JavaCard gemeinsam mit dem symmetrischen Schlüssel, um das Rezept zu überprüfen.

Wichtige Begriffe

Java, Applets, Health Professional Card, World Wide Web, JavaCard API

1. Einführung

Der vermehrte Gebrauch von Internet-Applikationen, die für das Übertragen von privaten medizinischen Daten entwickelt werden, erfordert noch hohe Sicherheitsmechanismen, welche die übertragenen Daten schützen. Infrastrukturen - speziell entwickelt, um Authentisierungs- und Authorisierungsmechnismen zur Verfügung zu stellen - werden ebenfalls benötigt. Public Key Infrastrukturen werden benutzt, um einen Public Key des Benutzers mit individuellen Informationen zu versehen. Der Public Key, zusammen mit der Benutzerinformation, repräsentiert ein digitales Zertifikat oder kurz: ein Zertifikat. Zertifikate werden in einer Zertifikatsdatenbank verwaltet, die Dienste anbietet, wie z.B. Zertifikatsüberprüfung, -anträge, -registrierung und –verwaltung. Vorzugsweise wird der Private Key auf der Chipkarte des Benutzers gehalten. Dieser Private Key kann nicht von dem Public Key konstruiert werden, jedoch kann der Public Key von dem Private Key konstruiert werden. Dies liegt an der Tatsache, dass Schlüssel dieser Art asymmetrisch sind. Bei einer Verifikation wird immer als erstes überprüft, ob der Public Key zum Private Key gehört.

Der Authentisierungsprozess wird als sehr wichtiger Teil in einer PKI betrachtet, weil die Verifizierung einer Personenkennung ein Prozess ist, in dem entschieden wird, welche Zugriffsrechte einer Person zugeordnet werden, und ob es dieser Person gestattet ist, eine Komponente der PKI zu nutzen. Die beste Methode, eine Authentisierung durchzuführen, ist eine Chipkarte zu benutzen, wie z. B. eine JavaCard.

In diesem Text wird eine neue Art der Health Professional Card vorgestellt, die durch eine multifuktionale JavaCard[12],[13],[14] mit einer flexiblen Verifikationsmöglichkeit für verteilte Systeme eines vernetzten Gesundheitssystems repräsentiert wird. Die flexible Verifikation wird durch einen Prozess erlangt, in dem der Sender einer signierten Nachricht automatisch identifiziert werden kann, wobei unterschiedliche

Zertifikatsdatenbanken gescannt werden, die in voneinander unabhängigen Gesundheitssystemen genutzt werden.

Das Institut für Telematik entwickelte ein Konzept für eine Anwendung, welche den JavaCard 2.1 Standard [1] für Patienten nutzt, um als elektronisches Rezept zu fungieren. Es ist wichtig, eine standardisierte elektronische Patientenakte zu nutzen, die in unterschiedlichen nationalen Gesundheitssystemen in der ganzen Welt verwendet werden kann. Zur Zeit gibt es unterschiedliche, auf dem Markt existierende Kartensysteme. Fast alle Chipkarten verwenden Software, repräsentiert durch Bibliotheken, implementiert in der Programmiersprache C. Es sollte jedoch die JavaCard als Alternative in Betracht gezogen werden. Mit der Hilfe einer JavaCard für mehrere Anwendungen ist es möglich, unterschiedliche Anwendungen auf einer Karte zu speichern. Ein Applet auf der Patientenkarte kann Informationen entweder von der Karte oder vom World Wide Web lesen. Eine Patientenkarte stellt eine mögliche Lösung für spezielle Anwendungsfälle dar.

Es gibt unterschiedliche Patientenkarten, die im deutschen Gesundheitssystem eingesetzt werden.. Zieht man ganz Europa in Betracht, resultiert daraus ein hoher Bedarf an Patientenkarten. Das derzeit existierende Modell für Gesundheitssysteme in Europa besteht aus drei Ebenen: Die erste Ebene wird durch die Ärzte repräsentiert, die zweite setzt sich aus Spezialisten zusammen und die dritte Ebene besteht aus Krankenhäusern und Kliniken [2]. Die Kommunikation dieser Ebenen wurde weder in dem nationalen noch in dem internationalen Modell der Gesundheitssysteme standardisiert. Die Kommunikation richtet sich auf den Austausch von Briefen mit Hilfe der Post aus. Elektronische Kommunikationsmittel werden weniger genutzt. Auch Patientenkarten werden nur in wenigen Bereichen genutzt. Ein Beispiel für das Einsatzgebiet von Patientenkarten ist sie als Ersatz für den Krankenschein einer Krankenversicherung zu nutzen [3]. Zur Zeit werden unterschiedliche Karten für Versicherung und Krankenhäuser genutzt. Patienten erhalten zu einer privaten Krankenversicherung auch eine Krankenhausversicherungskarte. Diese Karten werden jedoch nur für administrative Zwecke genutzt.

Die Sicherheitsanforderungen, die Gesundheitskarten erfüllen müssen, sind von für den Schutz personenbezogener Daten von großer Bedeutung. Einige Karten haben funktionale Bedeutung, wie z. B. in dem Fall der Verschlüsselung (Kryptographie) und der digitalen Unterschrift (Signatur). Andere Karten verwenden biometrische Authentisierung, in dem eine spezielle Ausrüstung benutzt wird, um z. B. Fingerabdrücke zu prüfen und somit die lästige Eingabe eines Zugangskodes zu umgehen.

2. Multifunktionale Karte: ein vorgeschlagenes Modell für Gesundheitssysteme

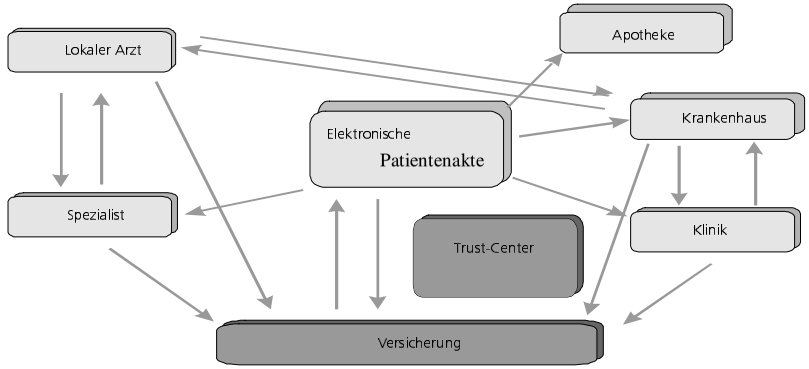

Abb. 1: Patientenorientiertes Gesundheitsmodell

Aus vielen Gründen ist ein solches Gesundheitsmodell, wie in Abbildung 1 dargestellt wird, vorteilhaft. Die standardisierte, multimediale, elektronische Patientenakte wird helfen, die Kommunikation zwischen den drei obengenannten Ebenen des Gesundheitssystems zu verbessern. Ein sicherer, elektronischer Datenaustausch zwischen den einzelnen Gruppen wird administrative Prozesse vereinfachen, die notwendig für eine solche komplexe Organisationsstruktur sind. Das vorgeschlagene Gesundheitsmodell soll Kosten reduzieren und Fehler

vermeiden, die aus falsch gesendeten Informationen resultierten. Die Infrastruktur muss durch medizinische Netzwerke und Trust Center modernisiert werden. Das medizinische Netzwerk ermöglicht die elektronische Kommunikation. Trust Center werden für sicheren Datentransfer benötigt, in dem sie Hilfsmittel zur Verfügung stellen, um eine Verwaltung der Zugriffskontrolle zu erlauben. In der Zukunft wird es für alle Mitglieder des Gesundheitssystems notwendig sein, unterschiedliche Arten eines Zertifikats, Private sowie Public Keys, eines symmetrischen Schlüssels für die Verschlüsselung und einer Funktion für die Berechnung der Signatur zu verwenden.

Für ein Modell des Gesundheitssystems ist es wichtig, eine standardisierte, multimediale, elektronische Patientenakte, die weltweit benutzt werden kann, zu verwenden. Voraussetzung für ein solches Modell ist es, eine multifunktionale Karte zu verwenden. Es gibt unterschiedliche Möglichkeiten, wie man eine Health Professional Card gemeinsam mit einer elektronischen Patientenakte nutzen kann. Einige Information kann verschlüsselt auf der Karte gespeichert werden. Andere Anwendungen werden für die Authentisierung genutzt, um elektronische Patientenakten von Krankenhäusern oder von Arztpraxen zu bekommen. Zum Beispiel: Ein Patient besucht seinen Arzt. Der Arzt sendet ein Rezept in Form einer digital signierten E-Mail an die Apotheke des Patienten. Danach besucht der Patient die Apotheke, um seine Medikamente abzuholen.

3.1 Entwurf einer Health Professional JavaCard (HPJC)

Eine Lösung für Multifunktionskarten mit Sicherheitsproblemen bietet die JavaCard. Die Software für JavaCards und die technische Spezifikation wurde durch das JavaCard Forum konzipiert. Dieses Forum wurde von den SmartCard-Herstellern Bull, Schlumberger und Gemplus gegründet [5]. Eine multifunktionale JavaCard kann mehrere Anwendungen auf einer Karte speichern [11]. Diese Anwendungen müssen eine Hochsicherheitsarchitektur besitzen, mit der Möglichkeit, digitale Signaturen zu verwenden. Die Java Card API 2.1 wurde in der Vergangenheit verwendet. Dieses Application Programming Interface (API) ermöglicht Kryptographie und Object Sharing zwischen Applets und Dateisystem.

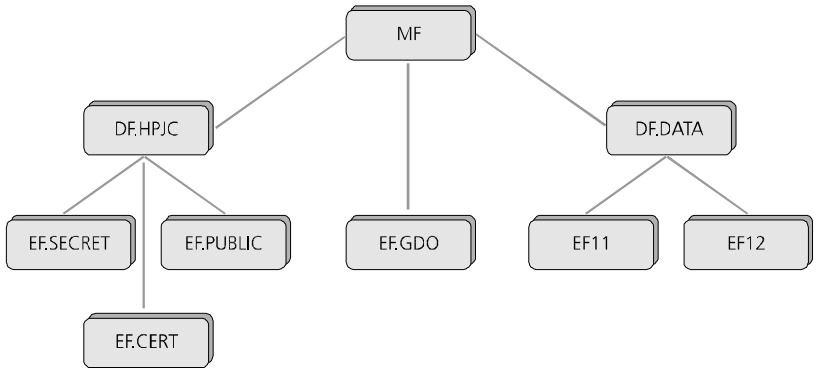

Abb. 2: Dateisystem der Patientenkarte

Eine HPJC richtet sich nach ISO/IEC 7816 (dem Standard für SmartCards) und nach DIN NI-17.4 (dem ChipCard-Standard mit elektronischer Signatur) [6], [7]. Unsere Anwendungsspezifikation sieht eine ID001 Karte vor. Das andere wichtige Kartenformat ist ID-000. Die Größe und Position der Kontakte wurden in Übereinstimmung mit ISO/IEC 7816-2 spezifiziert. Wir legten das halb-duplex asynchrone Block-Transfer-Protokoll T=1 als Übertragungsprotokoll fest. Für dieses Protokoll sollte die Node Address (NAD) auf „00“ gesetzt werden. Die Dateistruktur ist in Übereinstimmung mit ISO/IEC 7816 entwickelt worden und ist hierarchisch aufgebaut (Abb. 3). Die Wurzel ist das Master File (MF). Das MF besteht aus Elementary Files (EF) und Dedicated Files (DF). Die DF bestehen aus DF und EF, aber die DF in der letzten Ebene der Hierarchie

bestehen nur aus EF. Das MF besteht aus dem EF.GDO (GDO=Ground Data Object), mit der Seriennummer des Chips (ICCSN) und dem Namen des Kartenbesitzers. Die Anwendung für Signaturen wird innerhalb des DF.HPJC gespeichert. Alle Anwendungen haben ein DF mit einer Application Identification (AID). Das DF.HPJC besteht aus 3 Gruppen von EF: Sicherheitsdateien, öffentlichen Dateien und zertifizierten Dateien. Die PIN-Nummer und der Private Key sind in den Sicherheits-EF und der Public Key sowie die Hash-Funktion in den öffentlichen Dateien enthalten. Das Zertifikat für die Authorisierung sowie die Attributszertifikate der Krankenversicherung, der Apotheke, der Arztpraxis und des Krankenhauses sind in den zertifizierten Dateien enthalten. Sobald der Benutzer die Karte in das Kartenlesergerät steckt wird der Answer to Reset (ATR) ausgeführt und die Karte initialisiert. An dieser Stelle wird das MF ausgewählt. Auf diese Weise ermöglicht die JavaCard eine Integration unterschiedlicher Anwendungen.

Diese Methoden sind normalerweise maschinenabhängige Prozeduren oder Funktionen, so dass die Hersteller einer JavaCard ihre eigenen plattformabhängigen Bibliotheken anbieten. Für die Systeme Windows 9.x oder Windows NT sind diese Methoden in C oder C++ implementiert und in Dynamic Link Libraries (DLL) gekapselt.

Für viele Prozesse braucht man das Standardkommando SELECT FILE und READ BINARY, um auf das EF der JavaCard Zugriff zu haben. SELECT FILE findet die Datei durch den FID (File Identifier) im Dateisystem. Dies ist die einfachste Möglichkeit, Dateien auszuwählen. Danach liest das Kommando READ BINARY die Daten.

Als Hash-Algorithmus wurde der Algorithmus (SHA-1) verwendet [8]. Nur der 160-Bit Hash-Algorithmus der MD4-Familie ist in Deutschland erlaubt [9]. Zwei Bedingungen müssen erfüllt werden: Der Hash-Algorithmus muss frei von Kollisionen sein und muss aus injektiven Funktionen bestehen. Ein anderer geeigneter Algorithmus ist der RIPEMD-160 [9]. Das Kommando PSO:HASH (PERFORM SECURITY OPERATION:HASH) berechnet den Hash-Wert auf der Karte. Der nächste Schritt besteht in der Speicherung des Hash-Wertes zusammen mit dem Dokument auf der Festplatte des PCs. Der Hash-Wert wird in das EF geschrieben. Mit dem Standard Kommando SELECT FILE und READ BINARY kann der Wert auf die Festplatte übertragen werden. Der Hash-Wert eines bestimmten Dokumentes ist eine geeignete Methode, zu überprüfen, ob der Hash-Wert von einer dritten Person geändert worden ist.

Der nächste wichtige Prozess ist das Lesen öffentlicher Zertifikate und ihrer Public Keys. Diese Informationen werden in der EF.PUBLIC.x gespeichert. In vielen Fällen überprüft die Karte, ob das Rezept, die Apotheke, das Krankenhaus und die Versicherung richtig sind. Es wurde hier nur ein Prozess vorgestellt, in dem Zertifikate auf einer JavaCard gespeichert wurden. Vorbedingung ist, dass das aktuelle X.509 Zertifikat von einem X.500 Directory Server heruntergeladen wurde und in dem EF.PUBLIC.CERT.PHAR gespeichert wurde. Die Überprüfung kann auf ähnliche Weise durchgeführt werden, z. B. für Daten, die verschlüsselt an den Sender übertragen werden, der den Public Key bereitstellt.

Es ist auch möglich, neue Kommandos zu definieren. Die Kommandos müssen dem Standard ISO 7816 entsprechen.

3.2 Multifunktionale Patientenkarten und der Transfer von Rezepten

Es ist Patienten möglich, alle Ebenen des Gesundheitssystems zu nutzen. Diese unterschiedlichen Ebenen können durch Server simuliert werden, die den jeweiligen Ebenen zugeordnet wurden und sich in einem lokalen Netzwerk befinden. Die Benutzungsoberfläche wird durch die Signaturanwendung repräsentiert. Patienten können Zertifikate oder Attributszertifikate besitzen, die sie für ihre Krankenversicherung, ihre Apotheke, ihren Arzt und ihr Krankenhaus verwenden können. Wir werden den Transfer von Rezepten vorstellen, in dem eine multifunktionale Patientenkarte für den Fall, dass der Patient seine Medikamente erhält, verwendet wird. Der Arzt, der seine Patienten besucht hat führt eine Diagnose durch. Hieraus resultiert ein schriftliches Rezept. Es wird angenommen, dass der Patient dem Arzt gesagt hatte, wer sein Apotheker ist. Der Arzt nutzt einen SHA-1 Hash-Algorithmus und einen symmetrischen Schlüssel zur Verschlüsselung des Dokuments. Der symmetrische Schlüssel ist durch den asymmetrischen Schlüssel des Arztes verschlüsselt worden. An dieser Stelle gibt es verschiedene Möglichkeiten, den Transfer des Rezeptes sicher und auf elektronischem Wege dem Apotheker zukommen zu lassen. Dies setzt voraus, dass der Arzt die folgenden unterschiedlichen asymmetrischen Schlüssel verwendet:

1. Private Key des Arztes ,
2. Public Key des Patienten,
3. Private Key des Patienten,
4. Public Key des Apothekers.

Der dritte Fall setzt voraus, dass der Patient nicht anwesend ist, um die Signatur mit seiner Patientenkarte überprüfen zu können. Der Patient darf seine PIN-Nummer nicht dem Arzt geben, denn in diesem Fall wäre der Arzt in der Lage, den Private Key des Patienten zu verwenden und digitale Signaturen des Patienten zu erzeugen.

Der Patient geht zum Apotheker. Für jede der eben genannten vier Möglichkeiten hat der Patient unterschiedliche Möglichkeiten, den symmetrischen Schlüssel des Arztes zu entschlüsseln:

1. Der Patient überprüft das X.509 Zertifikat des Arztes. Das Zertifikat wird in einem LDAP Directory eines Trust Centers gespeichert. Wenn der Patient den Public Key des Arztes auf seiner Karte hat, kann er den symmetrischen Schlüssel mit dem Public Key des Arztes entschlüsseln. Wenn der Patient nicht den Public Key des Arztes besitzt, kann er den Public Key des Zertifikates, den er vom Trust Center bezog, benutzen. Jetzt kann er den symmetrischen Schlüssel mit diesem Public Key entschlüsseln.
2. Der Patient entschlüsselt den symmetrischen Schlüssel mit seinem Private Key. Er kann seinen Private Key aber erst nach Authentifikation durch die Eingabe seiner PIN benutzen.
3. Der Apotheker überprüft das Zertifikat des Patienten mit Hilfe des Directory Servers des Trust Centers. Die erste Handlung besteht darin, dass der Patient den symmetrischen Schlüssel mit seinem Public Key entschlüsselt. Sobald der Public Key auf seiner Patientenkarte ist, kann er sich mit seiner PIN authentisieren. Die andere Möglichkeit besteht darin, den Public Key des Patienten aus dessen Zertifikat zu lesen, das von dem Trust Center bezogen wurde.
4. Der Apotheker nutzt seine SmartCard, um den symmetrischen Schlüssel zu entschlüsseln. Dazu muss er seine PIN eingeben, bevor er seinen Private Key benutzt.

Nachdem der symmetrische Schlüssel entschlüsselt wurde, kann das Rezept mit dem symmetrischen Schlüssel entschlüsselt werden. Der Apotheker muss hierbei die digitale Signatur überprüfen. Der Hash-Wert wird mit dem gleichen Algorithmus berechnet, der auch in der Anwendung des Arztes verwendet wurde. Dieser Hash-Algorithmus ist SHA-1. Der Apotheker berechnet den Hash-Wert des verschlüsselten Rezeptes. Danach berechnet er den Hash-Wert und vergleicht ihn mit der gesendeten digitalen Signatur. Falls diese Werte übereinstimmen, entspricht die digitale Signatur der gesendeten digitalen Signatur.

Diese Schritte können durch Software realisiert werden, welche die digitale Signatur entschlüsselt und überprüft. Für einen auf den Patienten ausgerichtetes Netzwerk müssen dessen Prozesse und die Administration verschiedener Zertifikate standardisiert werden.

4. Bewertung und Ausblick

Im vorangegangen Text beschrieben wir nur eine mögliche Anwendung der JavaCard. Der Vorteil einer Karte dieser Art liegt jedoch darin, sie auch für andere Zwecke innerhalb von Krankenhäusern und Versicherungen einzusetzen. Es gibt einige Implementierungen, wie z. B. einen Multimedia-Editor für die Erzeugung von Befunden [10] oder eine Bildbetrachtungssoftware, die es ermöglichen, Bilder und deren Interpretationen einander zuzuordnen. Indem diese Implementierungen miteinander zu einem System verbunden werden und ein Zertifizierungsmechanismus hinzugefügt wird, entsteht ein wertvolles Hilfsmittel, das für das Management von Bildern, deren Interpretationen, sowie von Rezepten- und Patientendaten verwendet werden kann.

Literatur:

[1] *Java Card Application Programming Interface 2.1,* Version 1.0, 1999

[2] *Telematik im Gesundheitswesen - Perspektiven der Telemedizin in Deutschland -für Bundesministerium für Bildung, Wissenschaft, Forschung und Technologie und Bundesministerium für Gesundheit,* München 1997 http://www.iid.de/forschung/studien/telematik/ oder http://www.rolandberger.com

[3] *Application of Health Cards, h*ttp://www.gdm.de/index_0.htm G&D

[4] *Telematik-Anwendungen im Gesundheitswesen, Nutzungsfelder, Verbesserungspotentiale und Handlungsempfehlungen*, Schlußbericht der Arbeitsgruppe 7 des Forum Info 2000, Hrsg.: Der Bundesminister für Gesundheit, Bonn 1998

[5] Java Card Forum (JCF), *Standardization workgroup of the Java Card*. http://www.javacardforum.org

[6] *ISO7816 Standard, Teil 4 - vollständig* http://www.fh-augsburg.de/~bossekr/iso7816_4.html

[7] *Specification of chipcard interface with digital signature application/function*, DIN NI-17.4, Version 1.0, 1998

[8] B. Schneier, *Applied Cryptography,* Second Edition, 1996

[9] *Geeignete Kryptoalgorithmen gemäß § 17 (2) SigV,* Hrsg.: Bundesamt für Informationssicherheit (BSI), Bonn 1999 http://bsi.bund.de

[10] von Gehlen S., Vorwerk L., Eichelberg M. et al, A multimedia editor for radiological reports based on the DICOM Supplement Structured Reporting. In CARS `99, Computer Assisted Radiology and Surgery, Elsevier, Paris, 1999,pp 438-442.

[11] The JavaTM Virtual Machine Specification, © 1996 SunTM Microsystems, Inc.2550 Garcia Avenue, Mountain View, California 94043-1100 U.S.A.

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

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

[14] Meinel, Ch.., Vorwerk, L., Engel, T. Trustcenter und Multifunktionskarten, ONLINE'2000, Düsseldorf (Germany)