



 Preprint 00-07

**Trierer Symposium
Smart Cards
Abstracts**

Herausgeber:
Lutz Gollan
Christoph Meinel

ISSN 1433-8106

Editors Lutz Gollan
Dr. iur.

Christoph Meinel
Univ.-Prof. Dr. sc.

Copyright Institut für Telematik,
Trier

Trademarks All terms that are mentioned in this paper
that are known to be trademarks or
service marks have been appropriately
capitalised. Use of a term in this paper
should not be regarded as affecting the
validity of any trademark and service
mark. The product or brand names are
trademarks of their respective owners.

Printing 2000

Printed in Germany
All rights reserved

The documentation was accomplished
through the Institut für Telematik.
The information contained in this docu-
ment represents the current view of the
authors on the issues discussed as of the
date of publication. Because the present
methodology must respond to changing
research conditions, the results of this
paper should not be interpreted to be a
commitment on the part of the authors.
Any information presented after the date
of publication are subject to change.
The right to copy this documentation is
limited by copyright law. Making unau-
thorised copies, adaptations or compila-
tion works without permission of the
authors or institutions mentioned above is
prohibited and constitutes a punishable
violation of the law.

Trierer Symposium

Smart Cards

23. - 24. November 2000

Themenschwerpunkte

Aufbau und Wirkungsweise
Smart Cards im Gesundheitswesen
Bürger- und Kundenkarte
Mobilität durch Smart Cards
Zukünftige Entwicklungen

Inhalt

1. Veranstalter: Das Institut für Telematik e.V.	3
2. Programm des Symposiums Smart Cards	4
3. Abstracts	
3.1. Dr. Thomas Engel Architektur und Betriebssysteme – Eine Einführung	6
3.2. Wim Kuling Parkinson Card	7
3.3. Dipl.-Inf. Jürgen Sembritzki ISO WG 5: Health Cards	9
3.4. Dr. Christoph Sutter Evaluierungen von Smart Cards	10
3.5. Dr. Martin Merck Java Cards	11
3.6. Hansjörg Röhrich WAYflow und MobiChip	12
3.7. Dr. Ulrich Sporn Chipkarten im Mobilfunk – Entwicklungen und Trends	13
3.8. Dipl.-Betriebswirt (FH) Joachim Keller Das MEDIA@Komm-Projekt in der Region Nürnberg: Die Entwicklung und Einführung des Anwohnerparkausweises - erste Erfahrungen aus der Praxis	14
3.9. Walter Nink, Oberamtsrat Die multifunktionale Chipkarte als Studiausweis der Universität Trier	15
3.10. Dr. Franz Weikmann Multifunktionale Chipkarten - Technik und Anwendung	16
3.11. Dr. Rainer Ulrich Flexible, drahtlose multifunktionale Chipkarten - und was dann?	17
3.12. Dr. Bernd Dusemund Smart Cards und ihre Verwendung in einem Trustcenter	18

Veranstalter

Das Institut für Telematik e.V. ist eine gemeinnützige Forschungs- und Entwicklungseinrichtung unter der Verwaltung der Fraunhofer-Management-Gesellschaft mit Sitz in Trier. Es wurde am 1. Januar 1998 gegründet und entwickelt sich zunehmend zu einem Kompetenzzentrum für Problemlösungen im Schnittbereich von Telekommunikation und Informatik. Es beschäftigt derzeit ca. 40 wissenschaftliche Mitarbeiterinnen und Mitarbeiter verschiedener Fachrichtungen und Nationalitäten.

Das Spektrum der Institutstätigkeit reicht von der anwendungsorientierten Forschung in den Bereichen Informatik und Telekommunikation bis hin zur Entwicklung maßgeschneiderter Problemlösungen und Pilotsysteme für Handel, Industrie, Medizin und Verwaltung. Darüber hinaus hat sich das Institut die Aus- und Weiterbildung im Bereich der neuen Medien sowohl von Kooperationspartnern, als auch von interessierten Mitarbeitern regionaler und überregionaler Unternehmen zur Aufgabe gemacht.

Projektpartner des Instituts sind neben High-Tech-Unternehmen und Großbetrieben vor allem auch klein- und mittelständische Firmen, in denen die wissenschaftlichen Ergebnisse in die betriebliche Praxis umgesetzt werden. Die Tätigkeitsschwerpunkte liegen insbesondere in der Entwicklung und Nutzung neuer Informations- und Kommunikationsmedien in Technik, Medizin und Gesellschaft.

Die laufenden Forschungs- und Entwicklungsprojekte sind auf die praktische Nutzbarmachung neuester wissenschaftlicher Entwicklungen in den Bereichen elektronisches Publizieren, Internet/Intranet, Telemedizin, sichere Datenübertragung, Systementwurf und -analyse gerichtet.

Das Institut für Telematik ist dabei insbesondere in folgenden Technologiebereichen tätig:

- Redaktionssysteme - Bereitstellung von Informationen im Internet/Intranet
- Navigationssysteme - Aufbereitung von Informationen im Internet/Intranet
- Multimedia - Darstellung und Transport multimedialer Daten
- Sicherheit in offenen Netzen
- Netztechnologien und Computersysteme
- Telemedizin
- Grundlagenforschung Informatik, Mathematik und Telekommunikation

Die überwiegend projektbezogene Finanzierung der Forschungs- und Entwicklungsvorhaben sichert dabei eine Erfolgskontrolle durch die Anwender.

Prof. Dr. sc. Christoph Meinel, der Leiter des Instituts und Inhaber des Lehrstuhls für Informatik an der Universität Trier, ist Direktor des Zentrums für Wissenschaftliches Elektronisches Publizieren (WEP) an der Universität Trier und Mitglied verschiedener Aufsichtsräte und Programmkomitees. Er gehört z.B. dem Aufsichtsrat des Internationalen Begegnungs- und Forschungszentrums für Informatik Schloß Dagstuhl an und ist Sprecher der Fachgruppe "Komplexität" der deutschen Gesellschaft für Informatik (GI). Er ist als Veranstalter verschiedener wissenschaftlicher Symposien und als Mitglied verschiedener Programmkomitees internationaler Tagungen in Erscheinung getreten.

Tagungsleitung

Prof. Dr. sc. nat. Christoph Meinel
Institut für Telematik e.V.
Bahnhofstr. 30-32
D-54292 Trier

Kontakt

Dr. iur. Lutz Gollan
Institut für Telematik e.V.
Bahnhofstr. 30-32
D-54292 Trier
Tel: 0651 97551-20
Fax: 0651 97551-12
E-mail: gollan@ti.fhg.de

Programm

Trierer Symposium Smart Cards

am 23. und 24. November 2000
im Institut für Telematik e.V., Trier

Donnerstag, 23. November 2000		
14:00 – 14:15	Univ.-Prof. Dr. Christoph Meinel Institut für Telematik e.V., Trier	Begrüßung und Vorstellung des Instituts für Telematik
Einführung		
14:15 – 14:45	Dr. Thomas Engel Institut für Telematik e.V., Trier	Architektur und Betriebssysteme – Eine Einführung
Karten im Gesundheitswesen		
14:45 – 15:15	Wim Kuling Zorg en Zekerheid, Leiden/Niederlande	Parkinson Card
15:15 – 15:45	Dipl.-Inf. Jürgen Sembritzki ZTG, Krefeld	ISO WG 5: Health Cards
15:45 – 16:15	Pause	
Aufbau und Wirkungsweise		
16:15 – 16:45	Dr. Christoph Sutter TÜV Informationstechnik GmbH, Essen	Evaluierungen von Smart Cards
16:45 – 17:15	Dr. Martin Merck Sun Microsystems GmbH, München	Java Cards
17:15 – 17:30	Pause	
Mobilität durch Smart Cards		
17:30 – 18:00	Hansjörg Röhrich RMV, Hofheim/Ts.	WAYflow und MobiChip
18:00 – 18:30	Dr. Ulrich Sporn T-Mobil, Bonn	Chipkarten im Mobilfunk – Entwicklungen und Trends
ab 19:30	Konferenzdinner im Dorint Hotel Trier	

Freitag, 24. November 2000

Bürger- und Kundenkarte

09:00 – 09:30	Dr. Harald Ahrens Curiavant Internet GmbH, Nürnberg	Das MEDIA@Komm-Projekt in der Region Nürnberg: Die Entwicklung und Einführung des Anwohnerparkausweises - erste Erfahrungen aus der Praxis
09:30 – 10:00	Walter Nink, Oberamtsrat Universität Trier	Die multifunktionale Chipkarte als Studiausweis der Universität Trier
10:00 – 10:45	Pause	
Künftige Entwicklungen		
10:45 – 11:15	Dr. Franz Weikmann Giesecke & Devrient GmbH, München	Multifunktionale Chipkarten - Technik und Anwendungen
11:15 – 11:45	Dr. Rainer Ulrich Fraunhofer-Institut für Integrierte Schaltungen, Erlangen	Flexible, drahtlose multifunktionale Chipkarten - und was dann?
11:45 – 12:15	Dr. Bernd Dusemund Institut für Telematik e.V., Trier	SmartCards und ihre Verwendung in einem TrustCenter
12:15 – 13:00	Abschlussdiskussion	

Architektur und Betriebssysteme – Eine Einführung

Dr. rer. nat. Thomas Engel
Institut für Telematik e.V., Bahnhofstr. 30-32, D-54292 Trier
Tel.: ++49(0) 651 – 97551 – 30
mailto:engel@ti.fhg.de
http://www.ti.fhg.de

Abstract

Durch ihre einfache und praktische sowie vielseitige Verwendbarkeit finden Chipkarten immer größere Anwendungsgebiete. Chipkarten sind heutzutage Schlüssel zu vielen Dienstleistungen sowohl im Business-to-Business als auch im privaten Bereich. Während der letzten zwanzig Jahre entwickelte sich die Chipkarte - fast unbemerkt von der Informatik-Fachwelt - vom reinen Datenspeicher hin zu universell einsetzbaren Mikroprozessoren. Die heutige Leistungsfähigkeit entspricht der eines PC-Prozessors vor einigen Jahren. Die neue Generation von multifunktionalen Karten erlaubt es, mehrere Applikationen gleichzeitig auf einer Karte zu implementieren und somit verschiedene Funktionalitäten auf eine Karte zu integrieren.

Der Vortrag gibt einen Überblick über die verschiedenen Technologien multifunktionaler Karten und versucht, vorhandene Karten und ihre Leistungen gegenüberzustellen. Dabei gliedert sich der Inhalt in zwei Teile, eine grundlegende Einführung in die Basistechnologien sowie Anwendungsbereiche von multifunktionalen Karten.

Parkinson Card

Wim Kuling
Zorg en Zekerheid, Po box 400, NL- 2300 AK Leiden
Telefon: ++(31) 6 518 117 04
mailto:wkuling@sleutelnet.nl
http://www.zorgenzekerheid.nl

Abstract

- Card functionalities

In this project a health-card will be developed to fit the personal health situation of the cardholder, in this case the person with the Parkinson disease. The neurologist can make his diagnosis in a well-defined and computer aided way. The course of the disease is registered on the card. This will be followed by the registration of prescription and actual medication. Next to the medical specialist an important part is deposited with the pharmacist in registering all medication including that of other health professionals.

When the cardholder presents his card to a health-care professional a verification of the rightful claim to the insurance company can be made. Furthermore the participating Parkinson patients will be provided with a portable reader that looks like an organizer. With this reader he or she can decide to whom the health-card will be shown for retrieving information.

- Project description

The project is designed to serve as a blueprint for the development of a special patient-card, independent of the nature of the disease. This special health-card can be used by hospital, medical specialist, pharmacist and general practitioner. In due time the project will migrate to the designs that are currently developed by the ZorgPas Groep concerning the implementation of a national health-card.

For the health insurance company arises a state-of-the-art insurance-policy that provides an identification of the cardholder by means of biometric characteristics. In this project the FingerTipSensor of Siemens is selected for investigation. Apart from the use as insurance-policy the usability of the card for certainty about identification together with a survey of the current and historic medication as well as an insight view of the clinical picture of the cardholder will be the objects of this project.

- Participants and objectives

In the project a various number of parties will participate, such as associations for diseased, older and disabled persons, along with representatives for the federations of medical specialists, general practitioners and pharmacists. The Dutch Commissioner for information and privacy will regard the privacy and security aspects of the card.

Consequently the project will gain a wide range of carrying capacity. The central place however is for the person with the Parkinson disease: independence in lifestyle and simplicity in card-use will lead the way. A clear and open view is the main objective of the project. Health-care professionals will find modern facilities to get an accurate and overall picture of medication. The integrity of clinical data is warranted by the use of biometry and security measures by means of encryption.

Pilot characteristics

project phase:	design and development
selected cardholders:	the participants must be insured at Zorg en Zekerheid and treated for the Parkinson disease; participation is on a voluntary base; after the pilot the card will be further developed for other diseases
number of cardholders:	estimated number of persons with the Parkinson disease in Zorg en Zekerheid area: over 1000; estimated number of project participants at the start 200 – 300 growing to 800 - 1000

- Further comments

- 1 In this unique project will cooperate the associations of
Parkinson Patienten Vereniging
Nederlands Consumenten/Patienten Platform
Werkverband Organisaties Chronisch Zieken
HSB Card and Cardsystems
Zorg en Zekerheid
with participation of
regional patient platform
general practitioners in Leiden area
pharmacists in Leiden area
organization for disabled persons in Leiden area
organization for older people in Leiden area
EDP-auditors
- 2 Each participant to the pilot will have at his disposal a personal health-card with processor chip and FingerTip sensor by Siemens.
- 3 When visiting the neurologist diagnosis is made in a pre-defined and computer-aided way, while the clinical picture is registered according to standards that are developed by a group of neurologists. These data will be registered on the Parkinson-card in a compressed form, along with the prescription of the neurologist. These actions will be preceded by identification of the cardholder while using the fingertip sensor technology. In this process the encryption keys to further data will be released. While connecting with the network of the insurance company the rightful claim will be verified.
- 4 When visiting the pharmacist once again this claim will be verified and the identity established. The prescription will be read from the card and translated into actual medicine, which will also be registered on the health-card. The pharmacist will also register the medicine that has been prescribed by other health professionals such as the general practitioner.
- 5 In the pilot will participate two outpatients' departments, up to 150 pharmacists and 500 to 800 cardholders.
- 6 The participating cardholders will be provided with a portable card reader in which to enter the Parkinson card. It has the size and looks of an organizer and enables the following functions:
 - **help when taking medicine**
It is important for a Parkinson patient to take his medicine exactly on time and frequency. The card reader contains hard- and software that produces a signal when time is there. On the display the cardholder can read which medicine and quantity is scheduled.
 - **display chipdata**
By means of the card reader other persons (for example the health professionals) can retrieve the data registered on the chip. The cardholder decides. By handing over his card and card reader he implicitly gives permission for this retrieval. When the cardholder stays elsewhere, for example on holidays, the health professionals in this area can also can retrieve information about medicine.

ISO WG 5: Health Cards

Dipl.-Inf. Jürgen Sembritzki, Bereichsleiter
Zentrum für Telematik im Gesundheitswesen GmbH, Campus Fichtenhain 42, D-47807 Krefeld
Telefon: ++49(0) 2151 – 157 - 361
mailto:J.sembritzki@ztg-nrw.de
<http://www.ztg.de>

Abstract

Im August 1998 konstituierte sich das ISO TC 215 "Health Informatics" mit vier Arbeitsgruppen. Die Standardisierung von Karten war zunächst nicht vorgesehen, jedoch sollte der Bedarf in diesen Bereich untersucht werden. Im April 1999 wurde dann eine fünfte Arbeitsgruppe "Health Cards" gegründet, die sich erstmals im Oktober des selben Jahres traf, um über mögliche Arbeitsschwerpunkte zu beraten.

Zur Zeit besteht das Gremium aus 33 Experten aus 13 Ländern. Nach insgesamt 4 Sitzungen wird derzeit ein achteiliger Standard diskutiert, der neben medizinischen Daten auch die Definition des Inhaltes eines elektronischen Rezeptes beinhaltet.

Im einzelnen sind dies:

- Health informatics - Patient healthcard data - Part 1: General structure
- Health informatics - Patient healthcard data - Part 2: Common objects
- Health informatics - Patient healthcard data - Part 3: Limited clinical data
- Health informatics - Patient healthcard data - Part 4: Extended clinical data
- Health informatics - Patient healthcard data - Part 5: Identification data
- Health informatics - Patient healthcard data - Part 6: Administrative data
- Health informatics - Patient healthcard data – Part 7: Electronic prescription
- Health informatics - Patient healthcard data – Part 8: Links

Die ersten Teile werden bereits zur Abstimmung zirkuliert und sollen auf dem nächsten Treffen Anfang Dezember weiter diskutiert und entwickelt werden.

Evaluierungen von Smart Cards

Dr. Christoph Sutter
TÜV Informationstechnik GmbH, Am Technologiepark 1, D-45307 Essen
Telefon: ++49(0) 201 – 8999 - 582
mailto:c.sutter@tuvit.de
http://www.tuvit.de

Abstract

Wie sicher ist Ihre Smart Card?

Diese Frage kann, wenn überhaupt, nur durch eine Evaluierung der Smart Card nach anerkannten Sicherheitskriterien beantwortet werden.

Internationale Anerkennung weltweit haben zur Zeit die "*Common Criteria for Information Technology Security Evaluation*" (CC) wobei in Europa und Australien noch häufig die älteren "*Information Technology Security Evaluation Criteria*" (ITSEC) verwendet werden. Beide Kriterienwerke sind allgemein formuliert, so dass neben Smart Cards auch andere Hard- und Software evaluiert werden kann.

Der Evaluationsgegenstand, z.B. eine Smart Card, wird in den Sicherheitsvorgaben zusammen mit den zu erreichenden Sicherheitszielen festgelegt. Im Rahmen des Evaluierungsprozesses wird überprüft, in wieweit die festgelegten Sicherheitsziele erreicht werden. Die Überprüfungstiefe hängt von der Prüfstufe, auch Vertrauensniveau genannt, ab.

Smart Cards werden üblicherweise in den mittleren Prüfstufen ITSEC E3, E4 bzw. CC EAL4, EAL5 evaluiert. Die festgelegten Sicherheitsziele hängen vom genauen Einsatzgebiet, wie z.B. digitale Signatur, digitaler Ausweis, Geldkarte, ... der Smart Card ab. Gemeinsam ist allen Smart Cards ein Schutz der Integrität und Vertraulichkeit der abgelegten Programme und Daten. Die Sicherheitsziele werden mit einer Kombination von Sicherheitsmechanismen erreicht, die in der Smart Card Hard- und Software implementiert sind.

In einem Prüfschritt des Evaluierungsprozess werden vom Evaluator mit Hilfe der vorhandenen Informationen und den bekannten Angriffsszenarien die Sicherheitsmechanismen direkt attackiert, um festzustellen, ob diese zu überwinden oder zu umgehen sind. Nur wenn diese Überprüfung negativ ausfällt kann die Evaluierung erfolgreich abgeschlossen werden.

Java Cards

Dr. Martin Merck, Consultant
Sun Microsystems GmbH, Sonnenallee 1, D-85551 Heimstetten
Tel.: ++49(0) 89 - 46008 - 2115
mailto:Martin.Merck@germany.sun.com
<http://www.sun.de>

Abstract

Mit JavaCard steht erstmals eine sichere offene Chipkartenplattform zur Verfügung. Es können eigene Applikationen für Chipkarten entwickelt werden und diese auch nach Kartenherausgabe im Feld auf den Karten installiert werden. Die inhärente Sicherheit der Java Platform und das erweiterte Firewall-Konzept von JavaCard garantieren die Integrität aller Applikationen auf der Karte.

JavaCard ergänzt somit die Familie der Java-Technologien am unteren Ende und erlaubt nun erstmals eine durchgängige Programmierumgebung von der Chipkarte bis zum Server.

WAYflow und Mobichip

Hansjörg Röhrich, Projektleiter WAYFlow
Rhein-Main-Verkehrsverbund GmbH, Alte Bleiche 5, D-65719 Hofheim/Ts.
Tel.: ++49(0) 6192 – 294 – 101
mailto:h_roehrich@rmv.de
<http://www.wayflow.de>

Abstract

„WAYflow“ ist ein Forschungs- und Entwicklungsprojekt (F+E Projekt) unter Leitung der Rhein Main Verkehrsverbund GmbH, das im Rahmen des BMBF-Rahmenprogrammes „Mobilität in Ballungsräumen“ gefördert wird. Mit öffentlichen und privaten Partnern werden in einer sogenannten „public-private-partnership“ (ppp) ein marketingorientiertes Mobilitätsmanagement, kundenfreundliche Informationsdienste und intermodale integrierte Serviceangebote erarbeitet. Kernprodukte in WAYflow werden eine Informationsplattform und ein MobilitätsChip als Zugang zu individuellen Informationsdiensten und Leistungen sein. Die Leistungsfähigkeit der Chipkarte ermöglicht dem Nutzer neben der Information die Planung, die Buchung und die Zahlung der Reise bzw. des gewünschten Leistungspaketes.

In einem ersten Feldversuch im Frühjahr 2001 werden die im F+E Projekt WAYflow entwickelten Techniken und Dienste (WAYflow-Produkte) einer beschränkten Nutzergruppe zugänglich gemacht und einem Akzeptanz-, Gebrauchs- und Alltagstest unterzogen. Dabei ist die Erprobung der WAYflow-Produkte „Intermodales Routing“, „Freizeitberater“, „Dienstreiseberater“, „Alltagsführer“ und „Reisekorb“ in einem Zweistufenmodell primäres Ziel des Feldversuches. Das WAYflow-Produkt „MobiChip“ (Basischip: MIFARE Pro) dient als personalisierte Kundenschnittstelle. Mit dessen Hilfe erhalten die Probanden an Terminals im halböffentlichen Raum und an privaten PC Zugang zu den o.g. WAYflow Informations- und Beratungsdiensten.

Im Rahmen des RMV WAYflow Feldversuches werden neue Möglichkeiten der Mobilitätsinformation sowie -beratung für den Kunden getestet. Dabei erfolgt die schrittweise Integration vorhandener Plattformen in ein zukunftsorientiertes System, das den gewachsenen Anforderungen und Bedürfnissen des Kunden, der Technik und der Logistik entspricht.

Mit dem RMV WAYflow Feldversuch werden die kommunikativen, organisatorischen, und technischen Voraussetzungen für die Überführung der o.g. WAYflow-Produkte in den Produktivbetrieb geschaffen. Dabei werden die Ergebnisse aus dem F+E Projekt WAYflow konsequent zur Umsetzung gebracht, evaluiert, ausgebaut und weiterentwickelt. Neben der Schaffung der für den Produktivbetrieb notwendigen Infrastruktur ist das im RMV WAYflow Feldversuch getestete Informations- und Beratungssystem der Grundstein für ein späteres Reservierungs- und Buchungssystem von Mobilitätsdienstleistungen.

Chipkarten im Mobilfunk – Entwicklungen und Trends

Dr.-Ing. Ulrich Sporn, Leitung SIM Security, Mobile Commerce
T-Mobil, Karl-Duwe-Str. 31, D-53227 Bonn
Tel.: ++49(0) 221 – 936 – 1253
mailto:Ulrich.Sporn@t-mobil.de
<http://www.t-mobil.de>

Abstract

In einer kurzen Einführung werden die Hauptfunktionen der SmartCard (Teilnehmer-Authentikation, kryptographische Algorithmen, Speicherung von Secret Keys, individueller Konfiguration) im GSM-Netz erläutert.

Mit der Weiterentwicklung des Mobilfunks in Richtung 3. Generation kommen neue Funktionen z.B. Server-Authentikation hinzu, die anhand der 3GPP Standards (USIM) dargestellt werden.

Mit den GSM Standards 11.11 und 11.14 für SIM Application Toolkit (SAT) stehen dem Netzbetreiber Möglichkeiten zur Verfügung, eigene Applikationen für sogenannte Mehrwertdienste auf die Karte zu bringen. Diese Applikationen sind Over the Air (OTA) auf die Karte ladbar.

Es wird ein kurzer Einblick über Möglichkeiten und Grenzen von SAT und OTA an real existierenden Applikationen gegeben.

Die Entwicklung von SAT-Applikationen ist derzeit proprietär und an spezielle SIM-Plattformen gebunden. Ansätze zur Lösung dieses Problems sind die Java-Card bzw. die Standardisierung eines Browsers auf der SIM, der neben dem aus WAP bekannten Content-Browsing weitere Funktionen für Location Based Services sowie den Zugriff auf Verschlüsselungs- und Signaturfunktionen erlaubt.

Das MEDIA@Komm-Projekt in der Region Nürnberg: Die Entwicklung und Einführung des Anwohnerparkausweises – erste Erfahrungen aus der Praxis

Dr. Harald Ahrens, Projektleiter "Digitale Signatur"
Curiavant Internet GmbH, Am Hauptmarkt 17, 90403 Nürnberg
Tel.: ++49(0) 911 – 231 - 8600
mailto:harald.Ahrens@curiavant.de
http://www.curiant.de

Abstract

Ziel des MEDIA@Komm-Projektes des Städteverbundes Nürnberg (eine Kooperation der Städte Nürnberg, Fürth, Erlangen, Schwabach und Bayreuth) ist die Erforschung, Entwicklung und Implementierung eines integrativen Konzepts für multimediale Dienste in Kommunen unter Nutzung der digitalen Signatur, des Spektrums ihrer Möglichkeiten und ihrer wirtschaftlichen Potentiale.

Zielgruppen des Projektes sind vor allem:

- Kommunen als Anbieter öffentlicher Dienste für Bürger und private Unternehmen sowie als Anwender der digitalen Signatur in internen Geschäftsprozessen,
- rechtsfähige Bürger als Nutzer öffentlicher Dienste sowie der Angebote privater Unternehmen,
- private Unternehmen und Kammern als Nutzer der öffentlichen Dienste, als Anbieter eigener Dienste und als Anwender der digitalen Signatur.

Im Verlauf des Projektes wird eine regionale Kommunikationsplattform aufgebaut, deren Ziel die sichere Kommunikation zwischen Bürgern, Unternehmen und Kommunen ist. Zu Beginn werden Lösungen zu technischen Querschnittsprojekten entwickelt wie Identifikation/Authentifizierung, Signatur, Bezahlung, Archivierung und Stadtkarte. Die erarbeiteten Lösungen werden in attraktive Anwendungen umgesetzt, getestet und implementiert, um eine medienbruchfreie und damit effiziente und schnelle Kommunikation zwischen Unternehmen, Bürgern und Kommunen zu ermöglichen.

Als Schnittstelle zwischen dem Internetzugang des Bürgers (Frontend) mit den bestehenden DV-Systemen der Verwaltung (Backend) dient die technische Plattform. Wichtigstes Element ist dabei die digitale Signatur, eine Plastikkarte im EC-Kartenformat mit integriertem Prozessor-Chip, die eine rechtsverbindliche Unterschrift im Netz ermöglicht.

Als erste Anwendung steht den Bürgerinnen und Bürgern der Stadt Nürnberg seit dem 17. Oktober die Anwendung „Anwohnerparkausweis“ zur Verfügung. Erstmals können sich Bürgerinnen und Bürger mit der multifunktionalen Chipkarte online im Tiefbauamt einen Anwohnerparkausweis ausstellen lassen. Sie identifizieren sich hierzu, indem sie ihre Signaturkarte in das Lesegerät stecken. Dann können sie die angeforderten Informationen abrufen, das Formular ausfüllen und abschicken. Erstmals jedoch ist dank der integrierten Geldkarten-Funktion auch die Bezahlung online möglich. Diese Multifunktion ist bisher einzigartig und wurde von Curiavant entwickelt, produziert und gemeinsam mit Partnerunternehmen in die Praxis umgesetzt.

Die multifunktionale Chipkarte als Studenausweis der Universität Trier

Oberamtsrat Walter Nink
Universität Trier, Universitätsring 15, D-54286 Trier
Tel.: ++49(0) 651 – 201 – 4223
mailto:nink@uni-trier.de
http://www.uni-trier.de

Abstract

- a) **Ziele des Projektes**
Gründe für die Einführung einer multifunktionalen Chipkarte
- b) **Kartenauswahl**
Gegenüberstellung der Vor- und Nachteile einer Bankenkarte bzw. einer hochschuleigenen Karte
- c) **Funktionen des Studenausweises**
Universitäts- und Zahlungsfunktionen
- d) **Allgemeine Informationen zur Chipkarte**
Freiwilligkeit der Anwendungen, Erläuterungen zu Fragen des Datenschutzes und der bestehenden Vertragsverhältnisse
- e) **Erfahrungen mit der neuen Technologie**
Bisherige Erfahrungen mit dem System, Akzeptanz durch die Studierenden, Probleme mit Karten und/oder Geräten
- f) **Zukünftige Anwendungen**
Erläuterungen zu einem Ausweis für die Bediensteten der Universität mit den angedachten Anwendungen

Multifunktionale Chipkarten - Technik und Anwendung

Dr.-Ing. Franz Weikmann, Head of Technology Center
Giesecke & Devrient GmbH, Prinzregentenstr. 159, D-81677 München
Tel.: ++49(0) 89 - 41 19 19 03
mailto:franz.weikmann@gdm.de
http://www.gdm.de

Abstract

Multifunktionskarten - Vielkänner

Multifunktionskarten vereinen verschiedene Anwendungen. Ein typisches Beispiel für eine Multifunktionskarte ist ein Betriebs- oder Studentenausweis, der neben der Zugangskontrolle Zugriff auf Datenbanken oder Bibliotheken erlaubt und eine elektronische Börse für Kantine oder Mensa enthält, alles in einem Chip. Zusätzlich kann solch eine Karte über klassische Ausweismerkmale - etwa ein Lichtbild – verfügen. Während derartige Anwendungen die verschiedenen Applikationen in einem Chip vereinen, haben die Airplus-Karten der Deutschen Lufthansa alle nur denkbaren Schnittstellen für die verschiedenen Anwendungen: Magnetstreifen und Hochprägung für Kreditkartenanwendungen, eine Kontaktfläche mit Speicherchip für das öffentliche Telefonnetz der Deutschen Telekom sowie die kontaktlose Übertragung für das „Fliegen ohne Ticket“ der Deutschen Lufthansa. (Lexikon der Chipkarte von Giesecke & Devrient).

Multifunktionale Chipkarten können mehr als eine Anwendung sicher verwalten. Das Betriebssystem unterstützt somit nicht nur den Card Life Cycle sondern auch den Application Life Cycle mit den folgenden Funktionen:

- Selektionsmechanismen für mehrere Anwendungen
- Abschottung der Applikationen (Firewall)
- Aktivierung und Deaktivierung von Anwendungen
- Nachladen und Löschen von Anwendungen (auch Funktionalitäten).

Während heute die herstellereigene (native) Betriebssysteme mit Marktanteilen >90% dominieren, werden in Zukunft die offenen Betriebssysteme (Java, MULTOS, Windows for Smart Cards) stark an Bedeutung gewinnen. Vorteile der offenen Plattformen sind vor allem die Entwicklung von Applikationen, die nicht mehr herstellerabhängig sind, sondern aufgrund der Plattformstandardisierung kann die einmal entwickelte Anwendung auf Produkte verschiedener Hersteller geladen werden (write once run every-where). Um dieses Ziel zu erreichen und zur Gewährleistung der Sicherheit werden bei den z.Z. existierenden Betriebssystemen Interpreterkonzepte eingesetzt. Nachteile ergeben sich durch die verminderte Performance, bedingt durch die virtuelle Maschine, besonders bei kontaktlosen Karten. Als typische Beispiele für multifunktionale Chipkarten werden die ec-Karte mit Chip (electronic cash, Geldkarte, Loyalty), die GSM-Karte (GSM 11.11, SIM Toolkit, Browser) und Office-ID-Karte (digitale Signatur, Verschlüsselung, Client Server Authentisierung, Logon) vorgestellt.

Flexible, drahtlose multifunktionale Chipkarten - und was dann?

Dr.-Ing. Rainer Ulrich, Bereich Angewandte Elektronik
Fraunhofer Institut für Integrierte Schaltungen, Am Weichselgarten 3, D-91058 Erlangen
Tel.: ++49(0) 9131 – 776 – 660
mailto:ulr@iis.fhg.de
http://www.iis.fhg.de

Abstract

25 mm² - auf etwa dieser Fläche müssen alle Funktionen einer Chipkarte untergebracht werden. Größere Chips wären zu steif und würden brechen. Auf dieser Fläche finden heute typischerweise Platz: Ein 8- oder 16-bit-Microcontroller, 32 KByte ROM, 2 KByte RAM, 16 KByte EEPROM, ein Krypto-Coprozessor und ein Interface zum drahtlosen Datenaustausch im 13,56 MHz-Band.

Vielfältige, in Java programmierte Anwendungen für multifunktionale Chipkarten benötigen immer mehr Speicher. Die beim Einsatz von passiver Transpondertechnik auf etwa 10 cm begrenzte Entfernung beim Datenaustausch ist zu gering, deshalb werden zukünftige Karten integrierte Akkumulatoren besitzen. Sinnvoll wären auch ein Display und eine numerische Tastatur. Und statt der Eingabe einer PIN identifiziert sich der Benutzer über einen integrierten Fingerabdrucksensor.

Möglich werden diese Karten der Zukunft durch den Einsatz polymerbasierter elektronischen Komponenten für Displays, Batterien und den integrierten Schaltungen selbst.

Polymere lassen sich im Prinzip ohne die aufwendige Verfahren der Halbleitertechnologie verarbeiten. Man geht davon aus, dass die Herstellung von integrierten Schaltkreisen einst auf beliebigen, auch flexiblen Substraten mit Hilfe von einfachen Drucktechniken möglich sein wird. Speziell im Bereich der billigsten Massenelektronik, zu der ja auch die Chipkarte gehört, verspricht die Polymertechnologie neben mechanischen Vorteilen auch preislich interessante Lösungen.

Bis es soweit ist, müssen jedoch noch etliche Probleme gelöst werden: Die Leistungsfähigkeit einer Polymerelektronik ist erst auf dem Stand der Mikroelektronik Ende der fünfziger Jahre. Zudem sind Lebensdauerfragen zu klären und billigere, besser geeignete Produktionstechnik zu entwickeln.

Eigentlich gibt es dann auch keinen Grund mehr, die gewohnte Form beizubehalten: Unsere heutige Chipkarte hat morgen vielleicht die Form eines Armreifs oder ist in die Armbanduhr integriert.

Smart Cards und ihre Verwendung in einem Trustcenter

Dr. rer.nat. Bernd Dusemund
Institut für Telematik e.V., Bahnhofstr. 30-32, D-54292 Trier
Tel.: ++49(0) 651 – 97551 – 44
mailto:dusemund@ti.fhg.de
<http://www.ti.fhg.de>

Abstract

Der Zusammenhang zwischen Einsatz einer Smartcard und einem Trustcenter in einer PKI wird dargestellt. Ein Trustcenter übernimmt die Funktion des vertrauenswürdigen Dritten, bei der Zuordnung von Schlüsselhaber und Schlüsselpaar. Diese elektronischen Schlüssel dienen zu Signieren und Verschlüsseln von elektronischen Dokumenten. Solch ein Verfahren wird mehr und mehr notwendig, da sich die traditionell am Schriftverkehr ausgerichtete Kommunikation zunehmend elektronisch und über offene, das heißt leicht einsehbare Netze, vollzieht. Im Vortrag wird die Funktionsweise der digitalen Signatur erläutert und die zentrale Rolle eines Trustcenters dargestellt. Die Smartcard als sichere Aufbewahrungsort des privaten Schlüssels, auf der selber der Verschlüsselungsprozess ausgeführt wird, besitzt eine zentrale Bedeutung.

In einer Demonstration wird das Signieren einer e-mail mit einer Smartcard vorgeführt. Dies geschieht unter Verwendung eines jedem zugänglichen Standard Browsers dem Netscape Communicator.