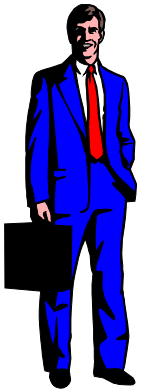
Alles einfach ?

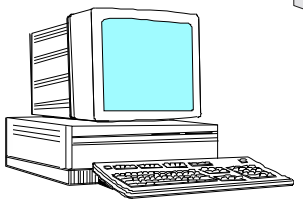
Vor- und Nachteile der Uni-Chipkarte

Mögliche Funktionen einer Uni-Chipkarten

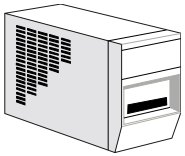
- Bezahlfunktion: Mensa, Drucker, Kopierer, Kostenstellen
- Studierendenausweis mit Studienfach, Fachsemester, Studiendauer
- Bibliotheksausweis
- Schliessfächer
- Semesterticket mit Foto
- Signatur, Authentifizierung, Zertifikate
- Zugangskontrollen, Parkplätze, Gebäude, Räume
- Zeiterfassung
- Dienstausweis
- Wahlausweis
- SAP-Karte
- Internetzugang

Anwendungsumgebungen



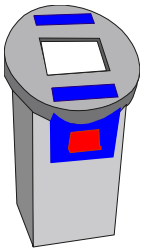


HIS
Studierendenverwaltung



Drucker

Digitale Kamera



Service-Station

1. Der/Die Studierende wird „Online“ personalisiert

2. Er/Sie erhält einen Studienausweis (Chipkarte)
mit persönlichen Daten (z.B. Name / Matrikel-Nr.)
„Semester-Stempel“

3. Der Studierende kann nun alle Applikationen der Chipkarte nutzen

Kantine / Cafeteria

Kopieren/Drucken

Bisheriger Einsatz von Chipkarten an der TUBS

- Bezahlfunktion: Mensa, Drucker, Kopierer, Kostenstellen
- Studierendenausweis mit Studienfach, Fachsemester, Studiendauer
- Bibliotheksausweis
- Schliessfächer
- Semesterticket
- Signatur, Authentifizierung, Zertifikate
- Zugangskontrollen, Parkplätze, Gebäude, Räume
- Zeiterfassung
- Dienstausweis
- Wahlausweis
- SAP-Karte
- Internetzugang

Chipkarte

Historie

1. Magnetstereifenkarten
   - nur ca. 150 Zeichen
   - jährlich derzeit mehrere Milliarden Stück
   - Scheck- und Kreditkarten
   - 1991 entstanden den Banken Verluste in 2-stelliger Millionenhöhe
   - Verlust der Information durch äußeres Magnetfeld
   - Kratzer und Hitze machen Karten unbrauchbar

2. Optische Speicherkarten
   - mehrere MByte
   - arbeiten wie CD´s
   - Inhalt nicht änderbar ⇨ fälschungssicher, schwer zerstörbar
   - relativ teuer
   - „dumme“ Karte (ohne Chip)

Chipkarte

Historie

3. Chipkarten

1983: erste Telefonkarte
1984: Bankkarte
Erste Massenanwendung: Telefonkarte, weltweit rund 8 Mill. Karten
Zweite Massenanwendung: Krankenversicherungskarte

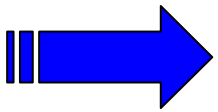
Smart-Cards (SIM-Karte) für Mobiltelefone weltweit millionenfach
Signaturkarten in Deutschland: mal gerade etwa 10.000 Nutzer

Heise.de/security/news/meldung/126956

Bauformen der Smart-Chipkarte

Kontakt behaftete Chipkarten (Goldkontakte)
Kontaklose Chipkarten (elektromagnetische Felder)

Chipkarte

Mono  Multifunktion

- Einfache Speicherkarten
- Speicherkarten mit Schreib/Lesefunktion
- Karte mit Speicher und Prozessor
- Karte mit Betriebssystem und Programmen

SmartCard

SmartCard werden ubiquitär

Internet SmartCard
mit kompletten Webserver, fester IP-Adresse, Sicherheitszertifikationen

Super SmartCards

verfügen nicht nur über ein Display, sondern auch über aufgedruckte Mikrofone und Lautsprecher oder numerische Tastaturen

www.heise.de/security/news/meldung/85075

Statt einer Chipkarte:
elektronisches Gerät (z.B.: iPod touch)

Chipkartentechnologien

Einfache Speicherkarte

- Typisch für monofunktionale Anwendungen

  z.B. Krankenversichertenkarte (personengebundene Nutzung)

- Keine logische Sicherheit

  z.B. Telefonkarte

  Bits werden „zerstört“

  Einmalanwendung (anonyme Nutzung)

Klassen von Chipkarten

Einfache Speicherkarten (z.B. Kankenversicherungskarte)
Chipkarte mit Schutzfunktion (z.B. Telefonkarte)
Prozessor-Chipkarte
Prozessor-Chipkarte mit Krypto-Controller
(zum Verschlüsseln und Entschlüsseln, komplexe Operationen)

Speicheraufteilung

Herstellerbereich (u.a. Hersteller, Typ, Version, Herstellungsdatum)
Personalisierungsbereich (u.a. Serien-Nr., Personendaten)
Anwendungsbereiche
Sicherheitsbereiche (u.a. PIN, Fehlerzähler, Systemdaten, Schlüssel)

Radio-Frequency Identification

Funkfrequenz-Identifizierung:

Kontaktfreies Erfassen der so ausgestatteten Chip-Karte

Zwei unterschiedliche Systeme:

a) Aktives System mit eigener Energiequelle

b) Passives System, das Lesegerät stellt die Energie zur Verfügung

1.) Backscatter-System im elektromagnetischen Fernfeld und UHF-Frequenz
2.) Lastmodulations-System im elektromagnetischen Nahfeld
Abstand bis zu 10 cm, Lesegrät sendet relativ starkes elektromagnetisches Feld mit einer Frequenz von 13,56 MHz (± 7 kHz), Karte ist induktiv angekoppelt
3.) Nachbarschafts-Ankopplung mit einer Reichweite von mehreren Metern

Sicherheit heißt Verschlüsselung

- Nur offene oder asymmetrische Schlüsselsysteme sind tragfähig
- Smartcard enthält geheimen Schlüssel und Krytoprozessor
- verschlüsselte Daten gelangen in Smartcard
  werden dort entschlüsselt oder verifiziert
  gelangen unverschlüsselt über sicheren Kanal zu Datenbanken

Sicherheit

- Geheimer Schlüssel verläßt Smartcard nie
- leistungsfähiger Kryptoprozessor
- Smartcard muß gegen Angriffe geschützt werden

Challenge-Response-Verfahren

- Frage-Anwort-Verfahren: kryptographische Verfahren zum Identitäts-Nachweis

Zu identifizierende **Nutzer besitzt geheimen Schlüssel**, auf den eine kryptographische Operation ausgeführt wird. In der Regel wird von dem System (Server, Firewall), an dem sich der Nutzer authentisieren möchte, eine Zufallszahl o.ä. generiert und an den Client des Nutzers gesendet.

- Diese Zahl wird anschließend vom Nutzer mit seinem geheimen Schlüssel signiert. Hierzu fordert die Authentisierungs-Software im Client den Nutzer auf, seine Chipkarte in das Lesegerät einzuführen und seine PIN einzugeben.

- Die signierte Zahl wird an den Server zurückgesandt, der mit Hilfe des **öffentlichen Schlüssels des Nutzers die Echtheit verifiziert**.

- Bei erfolgreicher Verifikation ist der Nachweis der Nutzeridentität erbracht, weil davon auszugehen ist, dass nur dieser den geheimen Schlüssel besitzt, mit dem die Signatur gebildet wurde.

Challenge-Response-Verfahren

- Grundsätzlicher Nachteil des Challenge-Response-Verfahrens:

Notwendigkeit der nutzerseitigen Authentisierung an jedem einzelnen Dienst.

Hierzu müssen die betroffenen Dienste Zugriff auf die öffentlichen Schlüssel sämtlicher Nutzer haben, um diese verifizieren zu können, wodurch ein beträchtlicher Verwaltungsaufwand entsteht, insbesondere wenn man die Fluktuation der Berechtigten bedenkt.

- Gängige Lösung: **Einbeziehung eines Trustcenters**, das ein zentrales z.B. LDAP- basiertes Verzeichnis vorhält, in dem sämtliche Nutzerzertifikate gespeichert sind. Die authentisierenden Dienste benötigen nur den Zugriff auf das Zertifikatverzeichnis sowie den öffentlichen Schlüssel der zertifizierenden Instanz zur Verifizierung der Signaturen.

Befürchtungen

- Überfrachtung der Anwendungen
- Verlust der Karte / Kostenübernahme der Ersatzkarte?
- Unerlaubtes Auslesen
- Erstellung von Bewegungsprofilen
- Mangelhafte Datensicherung
- Diverse Missbrauchsmöglichkeiten
- Benutzung der Chipkarte durch Unberechtigte

Schutzmaßnahmen der Chips

- Stochastische Verteilung der Adressleitung über mehrere Ebenen
- Blindzellen
- Spezielle Sensoren registrieren Licht ⇨ Löschung des Chips
- Schutz vor Messung des Versorgungsstromes (Blindzellen, gemischt)
- Schutz vor Einzelschrittbetrieb (mind. 1 MHz Takt)
- Speicherschutz (z.B. nach Transport- und Personalisierungsphase)

Schutzmaßnahmen des Plastikkörpers

- Hologramm
- Unterschrift
- Lichtbild
- Aufdruck (z.B. Name, Anschrift)
- Echtheitsmerkmal
- Multiple Laser Image

Erwünschte Sicherheit

- Fälschungssicher
- Nicht beschreibbar
- Schutz vor unberechtigtem Auslesen
- „Schalter“ (Hülle) vor unberechtigtem Auslesen
- Keine Verknüpfung der Anwendungen untereinander
- Sichere Verschlüsselung

Notwendige Infrastruktur

- Kartenschreiber
- Kartenleser
- Aufladestationen
- Personalisierungsstationen
- Abhörgeschützte Verbindungen zwischen diesen verschieden Geräten

Mangelhafte Verschlüsselung bei vielen RFID-Karten

Bei Mifare-Classic-Karten* ist die Krypto-Implementierung durch sogenannte Proxy- oder Relay-Attacken kompromittierbar !

*: Mifare (Mikron Fare System, „Mikron Fahrgeld-System) wurde Anfang bis Mitte der 1990 Jahre von der „Mikron Gesellschaft für Integrierte Mikroelektronik“ in Gratkorn, Österreich entwickelt

Plötz, Henryk (2008) Mifare Classic – Eine Analyse der Implementierung, Diplomarbeit, HU-Berlin
www.heise.de/security/news/meldung/117074
www.heise.de/security/news/meldung/121028

Gehackt:

ePass-Hack im niederländischen TV demonstriert

heise.de/newsticker/meldung/69127

Biometrische Gesichtserkennung in Laptops

heise.de/ix/news/meldung/132781

Erstes RFID-Virus

heise.de/tp/r4/artikel/22/22252/1.html

RFID-Freischaltung eines verschlüsselten USB-Festplattengehäuse

heise.de/security/news//meldung/119781

Funk-Schließsystem für Autos – *Hack den BMW*

http://www.heise.de/autos/Forscher-knacken-verbreitetes-Funk-Schliesssystem-fuer-Autos--/artikel/s/5492

heise.de/tp/54/artikel/22/22645/1.html

Verschlüsselung des RFID-Chip „Mifare Classic“

Henryk Plötz, Diplomarbeit, HU-Berlin 2008

heise.de/security/news//meldung/117074

Alternative Chips, z.B.: DESfire8*

Funktion:

Kontaklos zwischen der Schreib-/Leseeinheit und Mifare-Chip im Ausweis (13,56 MHz), passiv, max. Abstand 10 cm

Enthält 16 (32 bei 4KB) voneinander unabhängige Sektoren, Speicher-kapazität von bis zu 8 KByte, flexible Dateistruktur erlaubt die Implemen-tierung von bis zu 28 Applikationen

Jeder Sektor ist durch zwei verschiedene Schlüssel vor unberechtigtem Zugriff geschützt (Advanced Encryption Standard [AES], unterstützt ebenso gängige Kryptographie-verfahren DES und 3DES bei hoher Datentransferrate)

Hybridmedien (Mehrfachtechnologien):

Der Mifare kann durchaus mit anderen Technologien in einem Medium vereint werden. **Es ist jedoch zu beachten, dass gleiche Frequenzen die Funktionsfähigkeit der einzelnen Technologien stören oder komplett aufheben. Daher sind Mehrfachtechnologien in einem Medium mit gleichen Frequenzen nicht zu empfehlen.**

***:** Hergestellt von der Firma NXP (für **N**ext e**XP**erience) ist ein von der niederländischen Firma Philips 2006 gegründetes Halbleiterunternehmen

Bedrohte Privatspähre

Wenn Miniaturisierung von Elektronik mit einer immer stärkeren Vernetzung von Informationssystemen und einer stetig leistungsfähigeren Umfelderkennung zusammen kommt, dann entsteht etwas völlig Neues.

Intelligente Objekte im wirtschaftlichen und privaten Alltag bedrohen Privatsphäre.

Schaffung geeigneter Rahmenbedingungen, um die wirtschaftlichen Potenziale dieses Technologiebereiches auszuschöpfen, ohne dass individuelle Freiheiten und das Grundrecht auf informationelle Selbstbestimmung in Gefahr geraten.

Dies erfordert drei Schritte:

- systematische Nutzereinbindung in die Entwicklungsprozesse
- verstärkte Anstrengungen bei der Gestaltung der Benutzerschnittstellen
- eine Modernisierung des Datenschutzrechts.

heise.de/newsticker/meldung/139651

http://www.acatech.de/fileadmin/user_upload/Baumstruktur_nach_Website/Acatech/root/de/Publikationen/Stellungnahmen/acatech_bezieht_Position_intelligente_Objekte_web.pdf

EU empfiehlt RFID-Anwendern die Achtung der Privatsphäre

- Verbraucher sollten wissen, welche Artikel mit RFID-Chips enthalten
- Unternehmen und Behörden sollten die auf RFID-Chips gespeicherten Daten bekannt geben
- Einzelhandelsverbände und –organisationen sollten ein europaweit einheitliches Zeichen über die Päsenz von RFID-Chips an Produkten informieren
- Unternehmen und Behörden sollten VOR der Verwendung von RFID-Chips Folgeabschätzungen zum Datenschutz durchführen

heise.de/newsticker/meldung/137705

Empfehlungen zum Einsatz von Chipkarten - Grundschutz

- Fälschungssichere Authentifizierungsmerkmale
- Steuerung der Zugriffsrechte durch die Chipkarte selbst
- Sicherung gegen unbefugte Analyse der Chipinhalte
- Verschlüsselungs- und Signaturfunktionen mit anerkannten Algorithmen
- Sicherung der Kommunikation durch starke kryptographische Maßnahmen
- Abschottung der unterschiedlichen Chipanwendungen
- Gegenseitige Authentifizierung durch Challenge-Response-Verfahren

Empfehlungen zum Einsatz von Chipkarten - Erweitert

- I/O-Kontrolle aller Schnittstellen, Interferenzfreiheit der einzelnen Anwendungen, Verzicht auf Trace- und Debug-Funktionen
- Auslagerung von Teilen der Sicherheitsfunktionen des Betriebssystems in dynamisch bei der Initialisierung bzw. Personalisierung zuladbare Tabellen
- Anonyme Chipbenutzung sollte möglich
- Dateninhalte und Funktionalität in neutraler, zertifizierter Systemumgebung durch den Karteninhaber kontrollierbar

Kontrollfragen zum Datenschutz

- Wann und wie kommt es zum Personenbezug
- Auf welcher Rechtsgrundlage sollen die Daten verarbeitet werden
- Ist der Datenvermeidungs-/Erforderlichkeitsgrundsatz erfüllt
- Wer kann wie auf welche Daten zugreifen
- Wie wird ein unbefugter Zugriff auf Daten verhindert
- Sind die Sicherheitsmaßnahmen geeignet und angemessen, um unbefugte Zugriffe zu verhindern
- Ist die Anwendung für den Betroffen transparent
- Wie kann der Betroffene seine Auskunftsrechte geltend machen
- Sind Kommunikationsvorgänge, die auf einem RFID-Tag eine Verarbeitung personenbezogener Daten auslösen, für den Betroffenen eindeutig erkennbar

Meine Empfehlung

- Nicht alle Anwendungen auf nur einer Chip-Karte platzieren
- Chip-Karte mit sowenig wie möglich, besser: KEINEN, personenbezogen Daten einsetzen
- Alle für unterschiedliche Anwendungen notwendigen Daten sollten in Datenbanken gespeichert sein, auf die mit der Chip-Karte zugegriffen werden kann
- Implementierung aktualisierter Software (Anwendung, Sicherheit)
- Kommunikation zwischen Chip-Karte und Datenbanken (gegenseitige Authentifizierungen) sollten mittels Challenge-Response-Verfahren erfolgen
- Dafür zuvor notwendigerweise einzurichten:
  ein Authentifizierungs-System an der TU Braunschweig

Unterlagen: Empfehlungen zum Einsatz von Chipkarten

- **Empfehlungen zum Einsatz von Chipkarten**

  lfd.niedersachsen.de

- **Orientierungshilfe „Datenschutzgerechter Einsatz von RFID“**

  Herausgegeben vom Arbeitskreis „Technische und organisatorische Fatenschutzfragen“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, 14.12.2006

Praktische Regelungen

- **§ 17 NHG: … „Durch Ordnungen der Hochschulen kann die Pflicht zur Verwendung von mobilen Speichermedien begründet werden, die der automatischen Datenerfassung oder –verarbeitung insbesondere für Zwecke der Zutrittskontrolle, Identitäts-feststellung, Zeiterfasssung, Abrechnung oder Bezahlung dienen.“**

- Regulierungsbehörde für Telekommunikation und Post ist zuständig
- Hat mit Stand 15.7.1998 Maßnahmenkatalog für Zertifizierungsstellen für technische Komponenten herausgegeben

Chipkarte
Wichtige URL‘s

- **Datenschutz**: www.lfd.niedersachsen.de
- **Regulierungsbehörde:** www.regtp.de
- **BSI:** www.bsi.de
- **Frauenhofer:**
  http://sit.sit.fraunhofer.de/_veranstaltungen/smartcard-ws/index.php
- **Hardware:** www.gi-de.com

Datenschutz als werbewirksames Aushängeschild: Eine Vision!?

Vielen Dank für Ihre Aufmerksamkeit !

Prof. Dr. Michael Wettern
Tel 0531 / 391 5886
Fax 0531 / 391 8208
eMail m.wettern@tu-braunschweig.de