

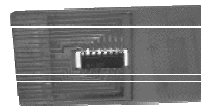
Smart Cards

- Einführung/Motivation/Anwendungsbereiche
- Arten von Smart Cards
- Aufbau/Herstellung von Smart Cards
- Smart Card Betriebssysteme
- Smart Card Software
- Kryptographie für Smart Cards
- Open Card Framework
- Kombination mit anderen Technologien
- Literatur

Folie 1

Entwicklungsgeschichte

- Frühe 50er Jahre: erste Plastikkarten (Kreditkarten von Diners Club)
- 60er Jahre: erste Magnetstreifenkarten
- 1968: Patent für eine Plastikkarte mit aufgebrachtem IC
 - Geburt der Smart Card



The first chip housed on an epoxy card.

Folie 2

Vorzüge von Smart Cards

- Smart Cards stellen portable Computer in Kreditkartengröße dar
- Smart Cards bieten einen sehr hohen Zugriffsschutz auf die dort gespeicherten Daten
- Smart Cards lassen sich mit anderen Technologien kombinieren
 - **Bio Smart Card**
 - **Contactless Smart Card**
 - **Optical Memory Card**

Folie 3

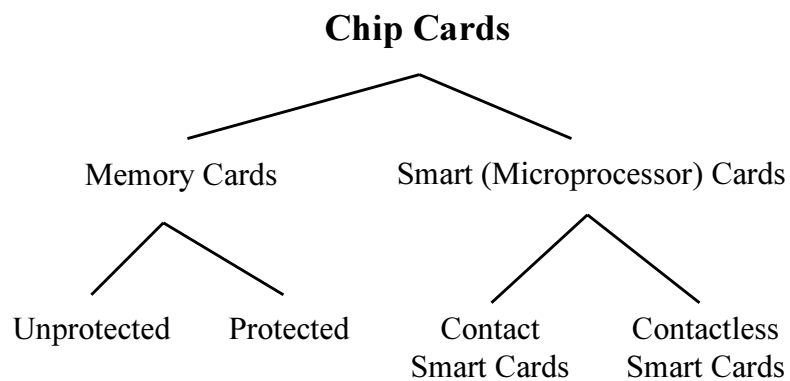
Anwendungsbereiche

The top five applications for smart cards throughout the world currently are as follows:

- **public telephony** (prepaid phone memory cards using contact technology)
- **mobile telephony** (mobile phone terminals featuring subscriber identification and directory services)
- **banking** (debit/credit payment cards and electronic purse)
- **loyalty** (storage of loyalty points in retail and gas industries)
- **pay-TV** (access key to TV broadcast services through a digital set-top box)

Folie 4

Arten von Chipkarten



Folie 5

Smart Card Standards

- Primarily, smart card standards govern physical properties and communication characteristics of the embedded chip and are covered through ISO 7816-1,2,3.
- Application-specific proprieties are being debated with many large organizations and groups proposing their standards.
- Open system card interoperability should apply at several levels
 - to the card itself
 - it's access terminals (readers)
 - the networks and the card issuers' own systems

Folie 6

Smart Card Standards

These organizations and industry initiatives are active in smart card standardization:

- **ISO (The International Standards Organization)**
 - ISO 7816: International standard for integrated-circuit cards (smart cards) that use electrical contacts
- **NIST (National Institute of Standards and Technology)**
 - Security Requirements for Cryptographic Modules
- **Europay, MasterCard and Visa**
 - Integrated Circuit Card Specifications for Payment Systems

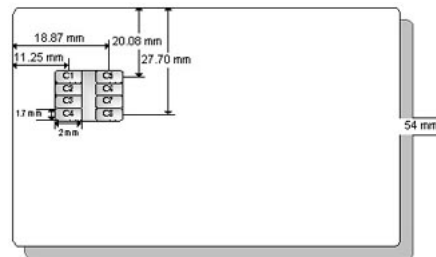
Folie 7

Smart Card Standards

- **Microsoft**
 - PC/SC specifications
- **CEN (Comite' Europe'en de Normalisation) and ETSI (European Telecommunications Standards Institute)**
 - Focused on telecommunications (smart cards in cellular telephones)
- **OpenCard Industry Consortium**
 - Open Card Framework

Folie 8

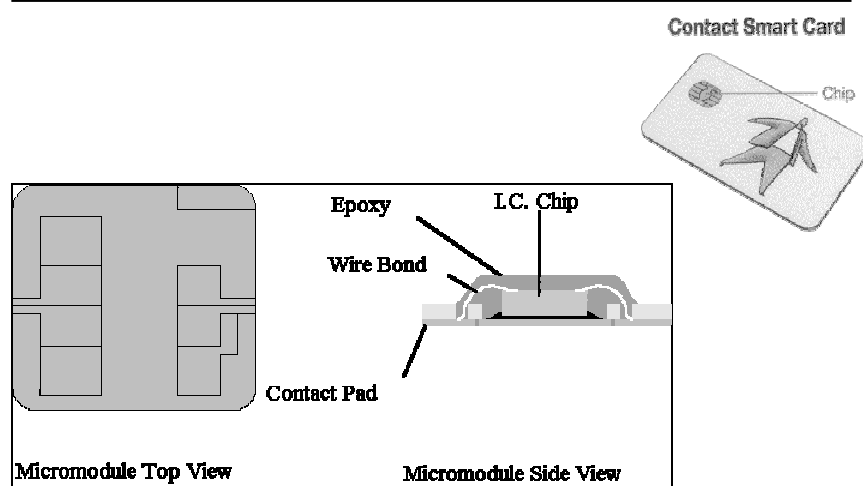
Abmessungen einer Smart Card



Schematischer Aufbau einer
Smart Card nach ISO 7810

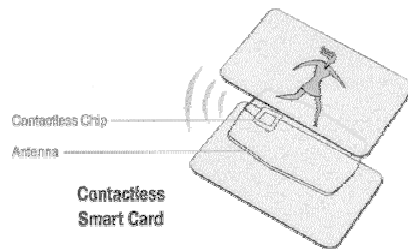
Folie 9

Aufbau einer Contact Smart Card



Folie 10

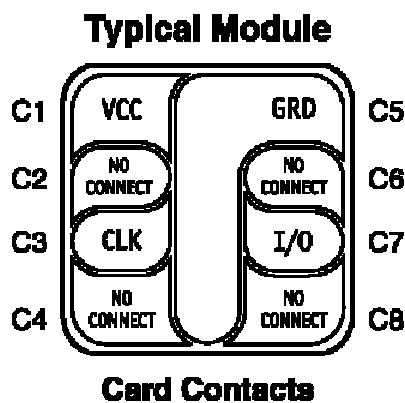
Kontaktlose Chipkarten



- The top and bottom card layers sandwich the antenna/chip module.
- The antenna is typically 3 - 5 turns of very thin wire (or conductive ink), connected to the contactless chip.

Folie 11

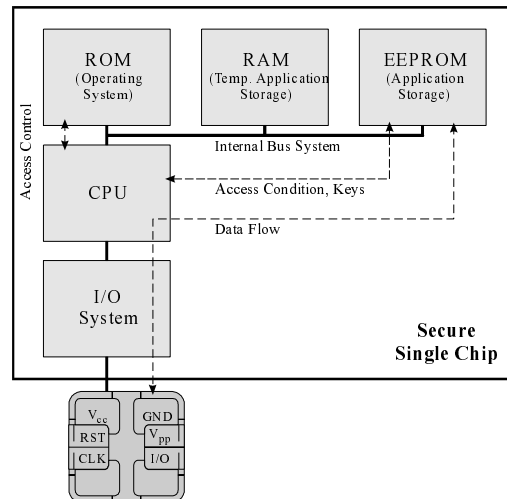
Mechanische Kontakte



- C1, C5: Versorgungsspannung
- C2: Nicht belegt oder Reset
- C3: Externer Takt
- C4, C8: Reserviert für zukünftigen Gebrauch
- C6: Nicht belegt oder Spannung zur Programmierung des EEPROMs
- C7: Datentransfer

Folie 12

Der Computer auf einer Smart Card



- RAM (4 KB)**
- ROM (16 KB)**
 - Operating System
 - Communication
 - Security (DES, RSA)
- EEPROM (16 KB)**
 - Filesystem
 - Program Files
 - Keys
 - Passwords
 - Applications
- CPU (8 Bit, 5 MHz, 5V)**
 - optional: crypto-coprocessor

Folie 13

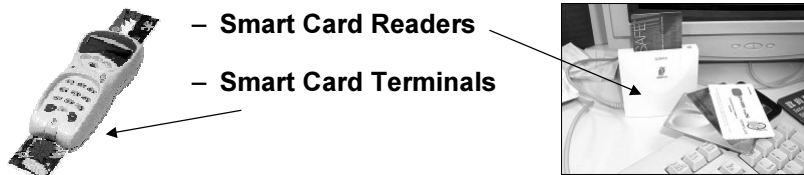
Der Herstellungsprozeß

- Herstellung des Chips
- Herstellung der Plastikkarte
- Aufbringen des Chips auf die Plastikkarte
- Initialisierung der Smart Card
 - Laden des EEPROMs mit dem Anwendungsprogramm und den allgemeinen Daten der Anwendung
- Personalisierung der Smart Card
 - Laden des EEPROMs mit Karteninhaber-spezifischen Informationen (Name, privater Schlüssel, etc.)

Folie 14

Smart Card-Readers and Terminals

- To write and read data to a smart card or to execute a command on a smart card, it is necessary to have a physical connection with the card.
- To make the connection with a contact card, it has to be inserted into a smart card acceptance device.
- There exist two groups of smart card acceptance devices:



Folie 15

Smart Card-Readers and Terminals

- The smart card reader is basically a connector between the smart card and the device communicating with the card.
- Smart card readers often have their own housing and are connected to the serial-, parallel- or USB-port of a computer.
- A reader can usually also write data to a card.
- In contrast to this, a terminal is a computer on its own which can operate stand-alone without being attached to another device.

Folie 16

Kommunikation mit der Smart Card

- Für die Kommunikation zwischen einer Smart Card und der Lesestation wird ein standardisiertes Übertragungsprotokoll (ISO 7816-4) verwendet.
- Das Protokoll unterscheidet zwischen Befehls- und Antwort APDUs (Application Protocol Data Units), wobei die Smart Card die passive (reaktive) Rolle der Kommunikationspartner einnimmt.
- Sie wartet bis sie ein Befehl von außen (command APDU) erhält und sendet nach dessen Abarbeitung eine Antwort zurück (response APDU).

Folie 17

Aufbau der Command APDU

Command APDU						
Mandatory Header				Conditional Body		
CLA	INS	P1	P2	Lc	Data field	Le

- **CLA (class byte):** Beinhaltet die Identifikation einer Applikationsklasse, die in der Smart Card implementiert ist und aktiviert werden soll

Folie 18

Aufbau der Command APDU

- **INS (instruction byte):** Byte, das die aufzurufende Instruktion bestimmt
- **P1, P2:** Übergabeparameter
- **Lc (length command):** Anzahl der Bytes im optionalen Datenfeld
- **Data field:** optionales Datenfeld
- **Le (length expected):** Erwartete Anzahl von Bytes im Datenfeld der Response APDU

Folie 19

Aufbau der Response APDU

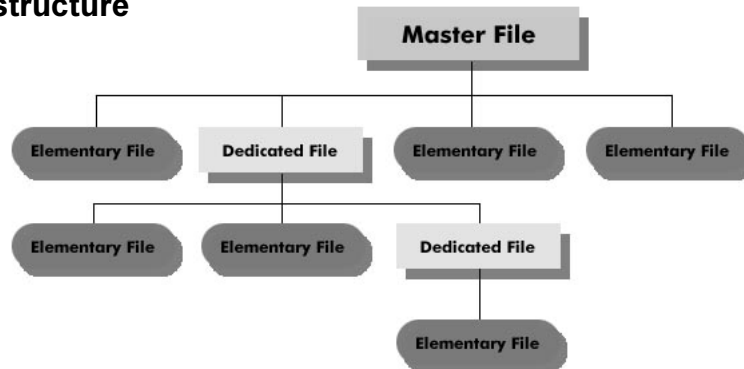
Response APDU		
Conditional Body	Mandatory Trailer	
Data field	SW1	SW2

- **Data field:** optionales Datenfeld
- **SW1, SW2 (status word):** 2 Bytes für Statusmeldungen in Bezug auf die vorhergehende Command APDU

Folie 20

The Smart Card File System

Logical file structure



Folie 21

The Smart Card File System

- The smart card file system is a tree-structured organization of directories and is similar to the file structures of MS-DOS or UNIX.
- It has a master file (MF) which is also referred to as the root directory.
- Under the master file, there are dedicated files (DF) and the elementary files (EF).
- Dedicated files contain subdirectories and the actual application with its elementary files.
- Elementary files contain the operation specific information such as data, card holder verification, cryptographic keys and application commands.

Folie 22

Access Control

- The smart card access control system controls file access.
- In order to allow data and/or objects (files and directories) to be moved to and from cards, access control lists are used to provide controlled access.
- The actions that can be performed on the file e.g. read, write, update, delete are restricted by the access control list.
- The abilities associated with a file are set with the associated access condition to provide a fine grain security.
- The levels of access conditions provided varies from smart cards depending on the application they provide.

Folie 23

Access Control

The basic access conditions of a file are:

- **Always (ALW):** Access data by a command without restriction.
- **Card Holder Verification (CHV1):** Access data is granted only when the correct CHV1 is presented by the card holder.
- **Card Holder Verification (CHV2):** Same as the above but a different CHV.
- **External Authentication (AUT):** Access to the protected data will be granted if a successful cryptographic authentication of the external device occurred previously.
- **Never (NEV):** Access of data is forbidden under any circumstances.

Folie 24

Smart Card Betriebssysteme

- **Java Card**
 - The Java Card platform allows the on-card application to be written in Java.
 - This brings the main advantages of Java to on-card software development.
 - In addition, it provides a good basis for multi-application cards, where on the same card more than one application is supported.

Folie 25

Smart Card Betriebssysteme

- **Multos**
 - Multos is a multi-application smart card operating system that allows to download or update applications on the card after it was issued.
 - Multos specifies a common operating system with an API that is called the Application Abstract Machine.
 - This ensures that after creation of a new Multos application, this application can be downloaded to every Multos smart card without any additional processing.

Folie 26

Smart Card Betriebssysteme

- **Smart Card for Windows**
 - The Microsoft Windows for Smart Cards is an 8-bit, multi-application operating system for smart cards with 8K of ROM.
 - It is designed to be a low-cost, easy-to-program platform that runs Visual Basic/C++ applications, and is designed to extend the PC environment into smart card use.
 - Smart Cards for Windows will work with the PC/SC infrastructure and thus be connected from the start to the world of PC/SC-compliant smart card applications.

Folie 27

Java Card



- The Java Card specifications enable Java technology to run on smart cards and other devices with limited memory.
- The Java Card API allows applications written for one smart card platform enabled with Java Card technology to run on any other such platform.
- The Java Card Application Environment (JCAE) is licensed on an OEM-basis to smart card manufacturers, representing more than 90 percent of the worldwide smart card manufacturing capacity.

Folie 28

Benefits of Java Card Technology

- Platform Independent - Java Card technology applets that comply with the Java Card API specification will run on cards developed using the JCAE - allowing developers to use the same Java Card technology applet to run on different vendors' cards.
- Multi-Application Capable - Multiple applications can run on a single card. In the Java programming language, the inherent design around small, downloadable code elements makes it easy to securely run multiple applications on a single card.

Folie 29

Benefits of Java Card Technology

- Post-Issuance of Applications - The installation of applications, after the card has been issued, provides card issuers with the ability to dynamically respond to their customer's changing needs.
- Flexible - The Object-Oriented methodology of the Java Card technology provides flexibility in programming smart cards.
- Compatible with Existing Smart Card Standards - The Java Card API is compatible with formal international standards, such as, ISO7816, and industry-specific standards, such as, Europay/Master Card/Visa (EMV).

Folie 30

Java Card Eigenschaften

- Aufgrund der sehr begrenzten Speicher- und Prozessorkapazitäten einer Smart Card stellt das Java Card API eine Untermenge des sehr mächtigen Standard Java API dar.
- Die wichtigsten Unterschiede sind:
 - **Kein dynamisches Laden von Klassen**
Alle Klassen werden entweder bei der Herstellung der Karte direkt ins ROM geschrieben (Klassenbibliothek) oder aber beim nachträglichen Installieren von Applets im EEPROM gespeichert. Ein dynamisches Class-Loading zur Laufzeit wird aus Sicherheits- und Performancegründen in Java Card nicht unterstützt.

Folie 31

Java Card Eigenschaften

- **Keine Threads**
Die Standard Java Schlüsselworte *synchronized* und *volatile* haben in Java Card keinerlei Bedeutung, da Java Card kein Multithreading und keine Synchronisation unterstützt. Der Grund dafür liegt in der beschränkten Prozessorleistung, die ein sinnvolles Arbeiten mit Threads nicht erlauben würde.

Folie 32

Java Card Eigenschaften

- **Keine Garbage Collection**

Die komfortable, aber rechenaufwendige automatische Speicherverwaltung ist kein Bestandteil der Java Card Spezifikation. Trotzdem sind verschiedene Smart Card – Hersteller dabei, auf ihren Java Cards auch dieses Feature zu implementieren. Java Card versteht sich als eine Mindestspezifikation, die alle Lizenznehmer erfüllen müssen. Alles was darüber hinausgeht ist zwar nicht zwingend, aber natürlich erfreulich und wünschenswert.

Folie 33

Java Card Eigenschaften

- **Keine speicherintensiven Datatypen**

Grundsätzlich unterstützt die Java Card Technologie nur die Datentypen byte, short und boolean. Mit der Verbreitung von 32 bit – Prozessoren auf smart cards wird wohl mittelfristig auch integer standardmässig unterstützt werden. Damit diese Datentypen sauber gehandelt werden können, verlangt Java Card vom Programmierer die strikte Anwendung von Cast-Anweisungen beim Umgang mit Variablen verschiedenen Typs. Nicht unterstützt werden in Java Card die Datentypen Long, Char, Float und Double.

Folie 34

Java Card Eigenschaften

- **Kein Object Cloning**

Auf die Unterstützung von Object Cloning wurde ebenfalls aus Performancegründen verzichtet, aber auch, weil die allermeisten Smart Card Anwendungen aufgrund ihrer Einfachheit dieses Konzept gar nutzen würden.

- **Keine mehrdimensionalen Arrays**

Arrays in Java Card müssen eindimensional sein und dürfen höchstens 32767 Felder beinhalten.

Folie 35

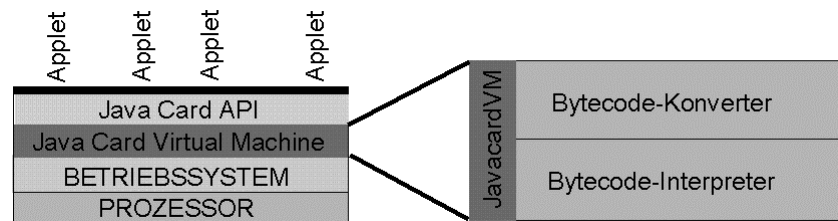
Java Card Framework

Das Java Card Framework umfasst folgende Pakete:

- javacard.framework
Hauptpaket; Definiert die wichtigen Klassen wie Applet, AID, PIN, APDU, etc.
- javacardx.framework
Dieses Paket unterstützt ein objektorientiertes Design für ein ISO 7816.4 kompatibles Dateisystem.
- javacardx.crypto, javacardx.cryptoEnc
Diese beiden Pakete ermöglichen Funktionalitäten der synchronen und asynchronen Verschlüsselung, wie sie für Smart Card gebraucht werden.

Folie 36

Java Card Architektur



Bytecode-Konverter: Befindet sich außerhalb der Karte und wird z.B. auf einem PC des Entwicklers ausgeführt. Aufgaben: Verifikation der zu ladenden Klassen und Initialisierung von statischen Variablen.

Der Bytecode-Interpreter: Ist auf der Karte implementiert und ist zuständig für die Codebearbeitung.

Folie 37

Smart Card Software

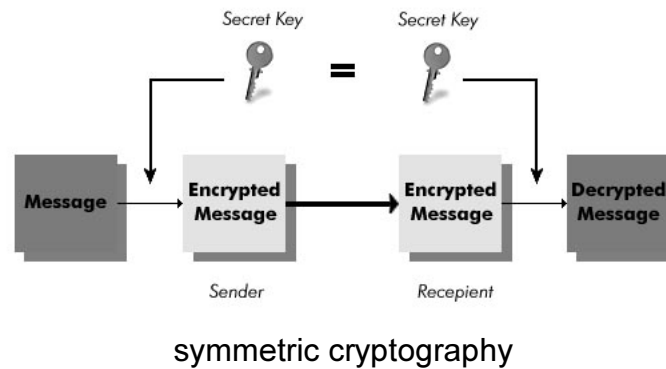
Smart Card Anwendungen setzen sich gewöhnlich aus folgenden Bestandteilen zusammen:

- Off-Card Anwendung
Teil der Anwendung, der auf dem Rechner/Terminal abläuft, an den das Smart Card Lesegerät angeschlossen ist.
- On-Card Anwendung
Teil der Anwendung, die auf dem Smart Card Chip gespeichert ist. Dabei kann es sich um Daten und/oder ausführbare Programme handeln.

Folie 38

Cryptography for Smart Cards

Secret Key Cryptography



Folie 39

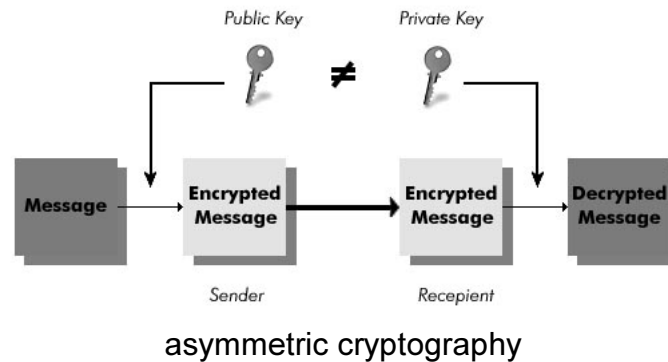
Secret Key Cryptography

- Secret key cryptography, also known as symmetric cryptography, uses one secret key.
- This key is shared by the sender and receiver of the message and the same key is used for encryption and decryption of data.
- An example is the Data Encryption Standard (DES).
- Secret key cryptography is simple and fast but the main drawback of the system is that the two parties must ensure the secret key is exchanged securely.
- Public key cryptography can avoid this problem.

Folie 40

Cryptography for Smart Cards

Public Key Cryptography



Folie 41

Public Key Cryptography

- Public key cryptography, also known as asymmetric cryptography, is based on the corresponding key pairs consisting of a public key and a private key.
- One key is used for encryption of data and the other for decryption.
- These two keys are mathematically related in such a way that the data encrypted by one key can be decrypted by the other.

Folie 42

Public Key Cryptography

- The key pair is generated by the owner.
- The private key is only known to its owner whereas the public key is given to the correspondent or published on the directory servers.
- So long as the private key is kept secret to the owner, data encrypted using the public key and sent to the owner can only be decrypted by the private key.
- The RSA Data Security's public key algorithm has become the industry standard.

Folie 43

Cryptography for Smart Cards

Digital Signatures

- Digital signatures make use of the advantages of the public key cryptography.
- A digital signature is the encrypted information generated using the private key of the sender.
- The receiver can perform the reverse process using the associated public key and confirm the identity of the sender.
- This is analogous to a handwritten signature of the physical world.

Folie 44

Digital Signatures

- The advantages of digital signatures are that they allow verification of the authenticity of information without the need of a private key.
- It ensures data has been untouched since its signing.
- It also ensures that the sender of a signed message cannot later repudiate the message since the signature is generated by his private key which is only known to him.
- For example, if someone were to send a message stating opinions, the sender cannot later deny the message was sent.

Folie 45

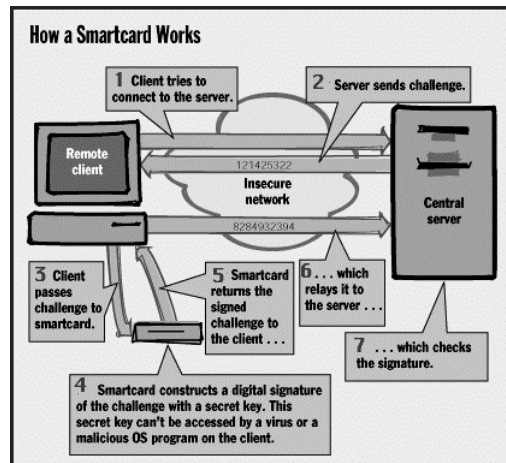
Digital Signatures

- A smart card with a crypto-coprocessor can perform full public-key generation, digital signatures, and authentication internally.
- This capability guarantees that the secret key will never be known outside the smart card and contributes to the overall security of the system.

Folie 46

Digital Signatures

Smart card using digital signatures to login to a computer network



Folie 47

Attacking Smart Cards

Logical Attacks

- Logical attacks occur when a smart card is operating under normal physical conditions, but sensitive information is gained by examining the bytes going to and from the smart card.
- One example is the so-called "timing attack". In this attack, various byte patterns are sent to the card to be signed by the private key.
- Information such as the time required to perform the operation and the number of zeroes and ones in the input bytes are used to eventually obtain the private key.

Folie 48

Attacking Smart Cards

Physical Attacks

- Physical attacks occur when normal physical conditions, such as temperature, clock frequency, voltage, etc. are altered in order to gain access to sensitive information on the smart card.
- Most smart card operating systems write sensitive data to the EEPROM area in a proprietary, encrypted manner so that it is difficult to obtain cleartext keys by directly hacking into the EEPROM.
- This type of attack can be combined with the logical attack mentioned above in order to gain knowledge of the private key.
- Most physical attacks require special equipment.

Folie 49

Attacking Smart Cards

Trojan Horse Attacks

- This attack involves a rogue, Trojan horse application that has been planted on an unsuspecting user's workstation.
- The Trojan horse waits until the user submits a valid PIN from a trusted application, thus enabling usage of the private key, and then asks the smart card to digitally sign some rogue data.
- The operation completes but the user never knows that his private key was just used against his will.

Folie 50

Attacking Smart Cards

Social Engineering Attacks

- In computer security systems, this type of attack is usually the most successful, especially when the security technology is properly implemented and configured.
- Usually, these attacks rely on the faults in human beings.
- An example of a social engineering attack has a hacker impersonating a network service technician.
- The serviceman approaches a low-level employee and requests their password for network servicing purposes.

Folie 51

Attacking Smart Cards

Conclusions

- Any security system, including smart cards, is breakable.
- However, there is usually an estimate for the cost required to break the system, which should be much greater than the value of the data being protected by the system.
- Independent security labs test for common security attacks on leading smart cards, and can usually provide an estimate of the cost in equipment and expertise of breaking the smartcard.
- When choosing a smart card for an architecture, one can ask the manufacturer for references to independent labs that have done security testing.

Folie 52

OpenCard Framework

- Standardized application platforms and standardized, easy-to-use frameworks to communicate with smart cards of any flavor and card terminals of any make are key factors for implementing smart card-enabled solutions and smart card-based services.
- The OpenCard Framework (OCF) capitalizes on the broad, cross-platform benefits of Java, providing an open architecture and a set of common *APIs* (Application Program Interfaces) geared for this purpose.

Folie 53

OpenCard Framework

- OpenCard Framework is a standard framework announced by an Industry consortium that provides for inter-operable smart cards solutions across many hardware and software platforms.
- The OpenCard Framework is an open standard providing an architecture and a set of APIs that enable application developers and service providers to build and deploy smart card aware solutions in any OpenCard-compliant environment.

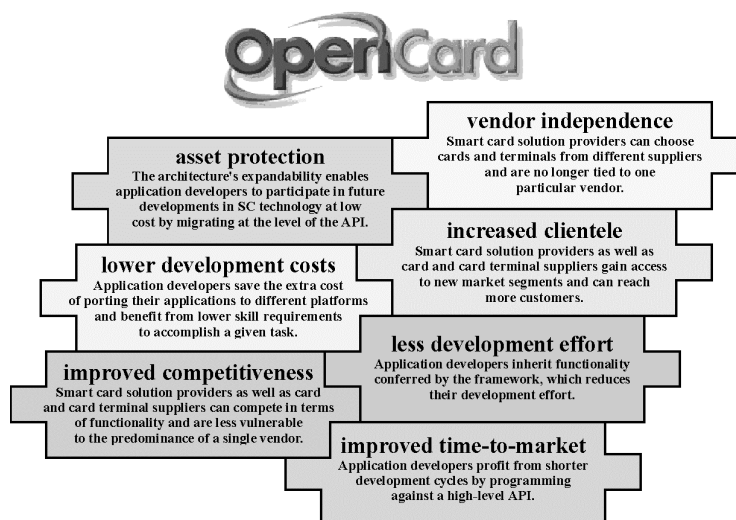
Folie 54

Some Members of the Industry Consortium



Folie 55

Benefits provided by OpenCard Framework



Folie 56

Main Parts of the OCF Architecture



Folie 57

The CardTerminal Layer

- The CardTerminal layer provides access to physical card terminals and inserted smart cards for which appropriate OCF-compliant drivers are made available by manufacturers.
- Also included are Java APIs for accessing PC/SC-supported card terminals.
- The CardTerminal layer enables OCF to handle the broad range of card terminals in use - now and in the future.

Folie 58

The CardService Layer

- The CardService layer makes it possible for the OpenCard Framework to deal with the wide variety of card operating systems in existence and the various different functions they may offer.
- Among OCF's many CardServices are the FileAccessCardService and the SignatureCardService.

Folie 59

The CardService Layer

- The FileAccessCardService provides a fairly complete set of interfaces and (abstract) classes making the ISO file system's functions available to the programmer.
- As with the rest of the framework, these classes and interfaces have been designed to fit seamlessly into the existing Java programming model.

Folie 60

The CardService Layer

- The SignatureCardService offers you methods to create and verify digital signatures based on such public key algorithms as RSA and DSA.
- Additional services allow private and public keys to be imported to the smart card or key pairs to be generated directly on the smart card.

Folie 61

The ApplicationManagement Component

- With the introduction of multiple applications which can be loaded onto a single smart card, new dependencies - such as which applications are available on the card or where an application and its data are physically located on the card - are created.
- This is where the ApplicationManagement component comes in.

Folie 62

The ApplicationManagement Component

- The ApplicationManagement component is capable of
 - **locating and selecting** card-resident applications on any given smart card,
 - **listing** the applications which a particular smart card supports,
 - **installing and uninstalling** applications on smart cards, and
 - **blocking and unblocking** applications on smart cards,
 - and thus solves the problem of card issuer dependency.

Folie 63

Scope of OCF

- OCF is perfectly suited to support all Java-enabled platforms such as
 - Personal Computers (PCs),
 - NetComputers (NCs),
 - or any type of smart card-enabled device such as automatic teller machines (*ATMs*), point-of-sales terminals, set-top boxes, and emerging hand-held devices.
- It also enables interactions with existing Personal Computer/SmartCard (PC/SC) 1.0 supported card terminal.

Folie 64

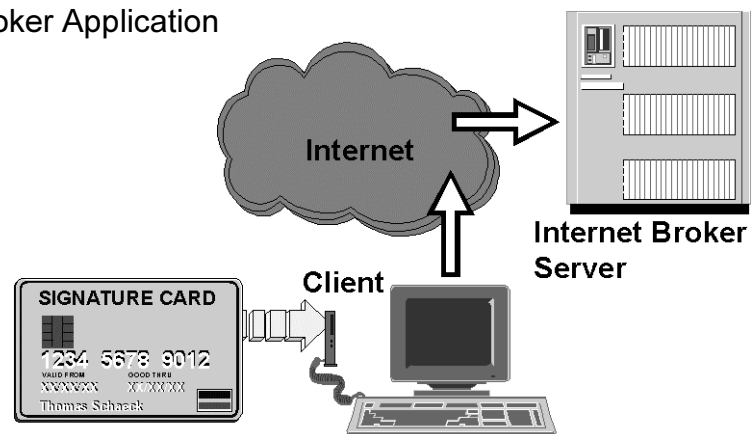
Scope of OCF

- The prerequisites for OCF are as follows:
 - Any Java 1.1 compliant platform such as AIX, LINUX, Solaris, Windows '95, and Windows NT.
 - There are no prerequisites for use with IBM NCs because OCF is delivered with the operating system.

Folie 65

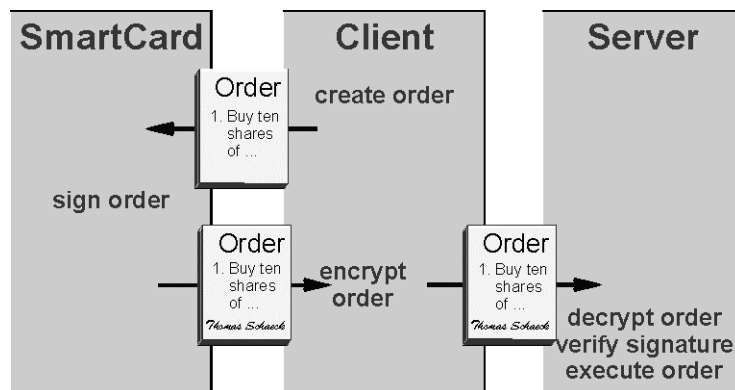
Example Application

Scenario of an Internet
Broker Application



Folie 66

Protocol used by the Internet Broker Application



Folie 67

Possible Security Breaches

The following security breaches can be carried out without the customer's knowledge or approval

- read the order data (only for non-encrypted ("clear text") transfers) - also called "interception"
- place the same order repeatedly - also called "replaying"
- change the order data (only for non-encrypted ("clear text") transfers) - also called "forgery"

Folie 68

Prevention of

- unauthorized reading of order data
 - encryption of the order data
- placing the same order repeatedly
 - internal order number

Folie 69

Prevention of Forgery

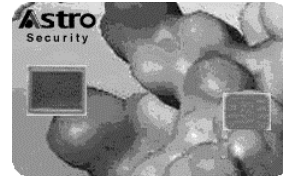
- This is possible because the "Internet Brokerage Server" used his public key and checked the digital signature generated by the smart card with the customer's private key.
- If the results don't match, the "Internet Brokerage Server" knows that he didn't receive the original message and thus doesn't process the order.

Folie 70

Kombinationen mit anderen Technologien

Bio Smart Card

- Die Bio Smart Card bietet gegenüber der herkömmlichen Smart Card ein weiteres wichtiges Feature: Einen integrierten Fingerabdruckleser.
- Durch den zusätzlichen Fingerabdruckscanner werden die Vorteile einer Smart Card Lösung mit denen der biometrischen Identifizierung vereint.
- Der totale Wegfall von Passwörtern sowie PIN Nummern rückt damit in greifbare Nähe.



Folie 71

Fingerabdruckscanner

- 65.000 Sensorelemente tasten den Finger ab und speichern die Schnittpunkte der Fingerrillen.
- Die dadurch entstehenden Muster werden zu einem eindeutigen Profil umgewandelt.
- Entsprechende Software sorgt anschließend für die genaue Auswertung des individuellen Fingerabdruckprofils.



Folie 72

Literatur

- W. Rankl, W. Effing: Smart Card Handbook; John Wiley & Sons, 2000.
- M. Hendry: Smart Card Security and Applications; Artech House Publishers, 1997.
- S. Schütt, B. Kohlgraf: Chipkarten - Technik und Anwendungen; Oldenbourg Verlag, 1996.
- F. Volpe: Chipkarten - Grundlagen, Technik, Anwendungen; Heise Verlag 1996.

Folie 73

Web-Adressen

- <http://www.javasoft.com/products/javacard/>
- <http://www.opencard.org/>
- <http://www.scia.org/default.htm>
- <http://www.smartcardforum.org/>
- <http://www.smart-card.com/>
- <http://www.visa.com/pd/smart/main.html>
- <http://www.mcard.umich.edu/otherLinks.htm>
- <http://smart.gov/>

Folie 74