

Lecture 8

Smartcards and Related
Application Infrastructures

Mobile Business I (WS 2010/11)

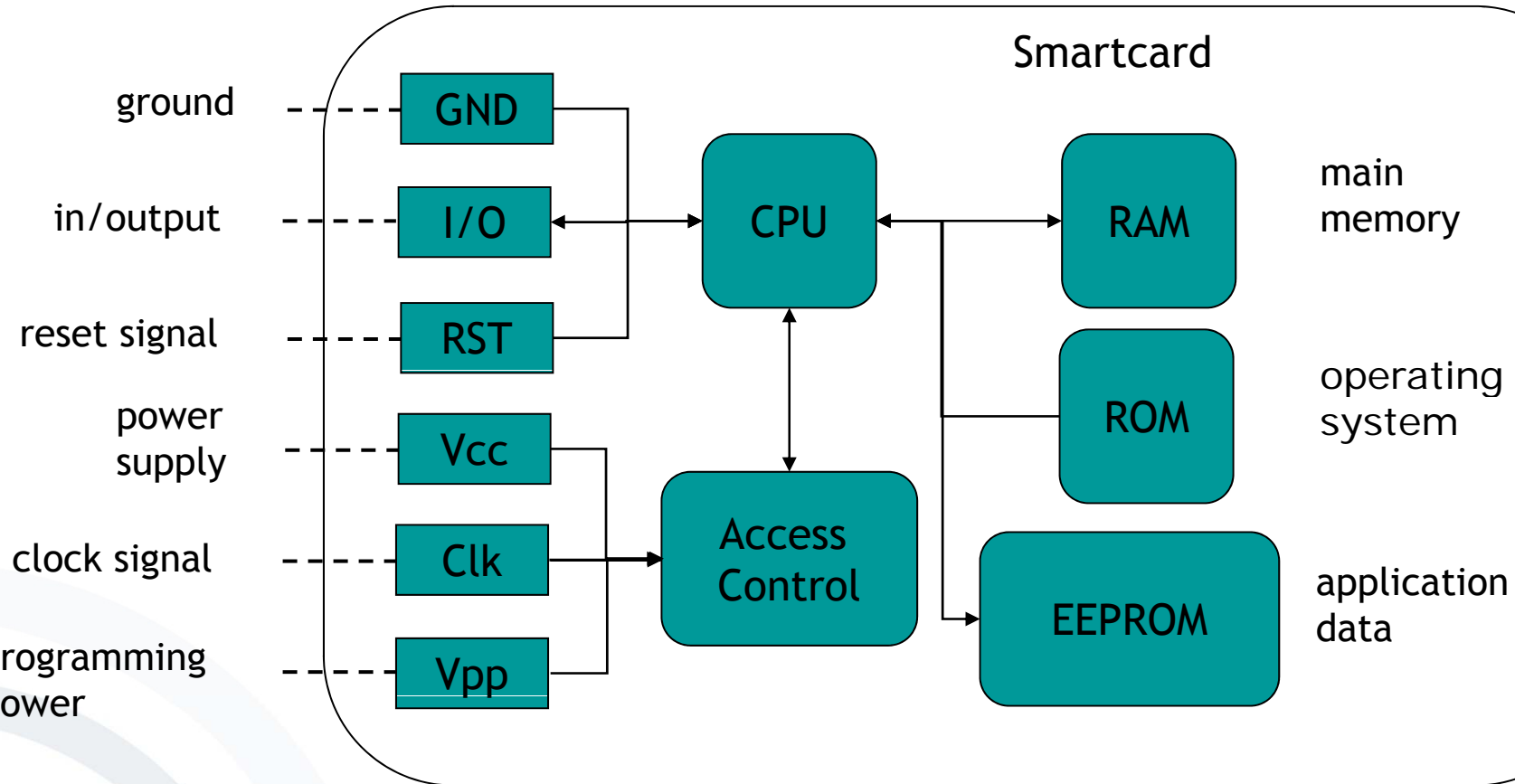
Prof. Dr. Kai Rannenber

T-Mobile Chair of Mobile Business & Multilateral Security
Johann Wolfgang Goethe University Frankfurt a. M.



- Smartcards – Introduction
- Subscriber Identity Module (SIM)
- WAP Identity Module (WIM)
- Universal SIM (USIM)
- IP Multimedia Services Identity Module (ISIM)
- New Applications – CamWebSIM

- Small computers with **memory, operating system, software, processor, I/O and access control**
- **Chip protected against manipulation**
- After being **initialised with keys and other data** smartcards are distributed to their users.



[Source: SecCommerce2002]

- Used when **security** of data (e.g. for keys, signatures, physical access control, payment) is needed in **insecure environments**
- **Examples:**
 - Phone cards of Deutsche Telekom
 - Signature cards according to German Signature Law
 - Smartcard applications for PC
 - Smartcards for mobile communication (SIMs)



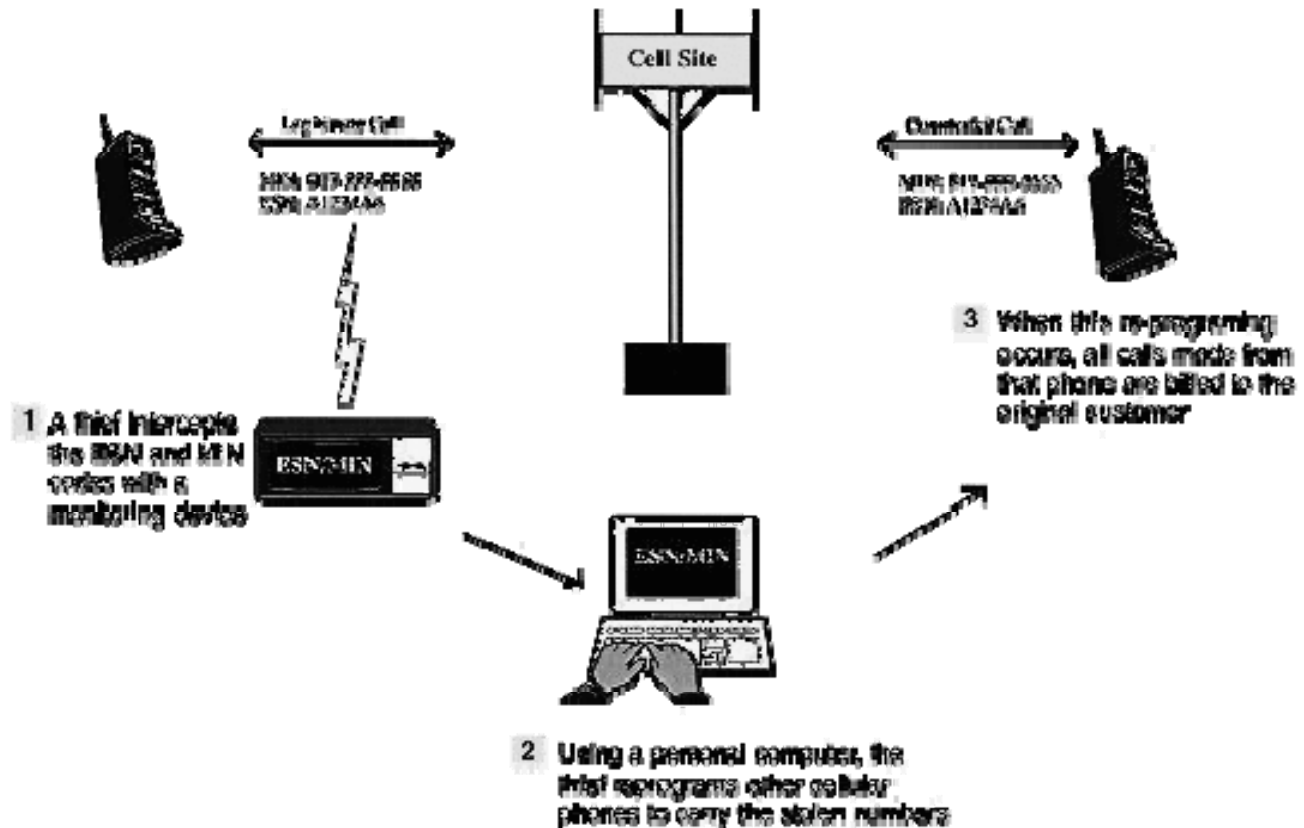
Protection needed against:

- Unauthorised usage of services through forged user data
- Duplication of a user's credentials
- „Cracking“ of credentials
- Billing fraud

CELLULAR COUNTERFEITING/CLONING FRAUD

Cellular Phone Counterfeiting

With each call made, a cellular phone transmits an Electronic Serial Number (ESN) and a Mobile Identification Number (MIN) identifying the caller. Possession of these numbers is the key to the counterfeiting.



Example for faulty system design (CDMA)

Duplication of intercepted user IDs

- Smartcards – Introduction
- Subscriber Identity Module (SIM)
 - Functionality
 - Technology
 - SIM Application Toolkit (SAT)
- WAP Identity Module (WIM)
- Universal SIM (USIM)
- IP Multimedia Services Identity Module (ISIM)
- New Applications – CamWebSIM

- In GSM and UMTS since 1991, upcoming for WLAN
- **Represents contract between subscriber & network operator**
- Authorises a “phone” to use the network by linking it to a **subscription**
- **3450 Mio** GSM subscriptions [GSM2009]
- **More** countries with **SIM** infrastructure (219, 2010-Q4) **than** with **McDonald’s** (125, 2010-Q4) and **more than UN** member states (192, 2010-Q4)

[GSM2010, McDonalds2007, Wiki2010, UN2006]



- **SIMs are Smartcards:**
 - SIM cards serve as security medium.
 - Tamper-resistance prevents counterfeiting.
 - robust design
- Contain **International Mobile Subscriber Identity (IMSI)** for subscriber identification and the key K_i provided by the mobile operator
- Reliably execute computational functions for the mobile device

cf. [EffingRankl2002]

- SIM serves as „**identity card**“ for GSM cellular phone subscribers.
- SIM identifies the **issuer of the card** – important for the **billing of roaming subscribers** by roaming partner.
- SIM allows for **secure billing of roaming subscribers** through SIM-cryptography – important for card issuer.
- SIM contains additional **configuration data** of the GSM system.

- Protected data:
 - IMSI, PIN, PUK
 - A3, A8 crypto algorithms
 - List of subscribed services
 - Language used by the subscriber
- Dynamic data:
 - Cell information
 - Frequency information
 - Dynamically generated (session) keys
 - Attributes of GSM login
 - User data (address book, telephone list, SMS memory)

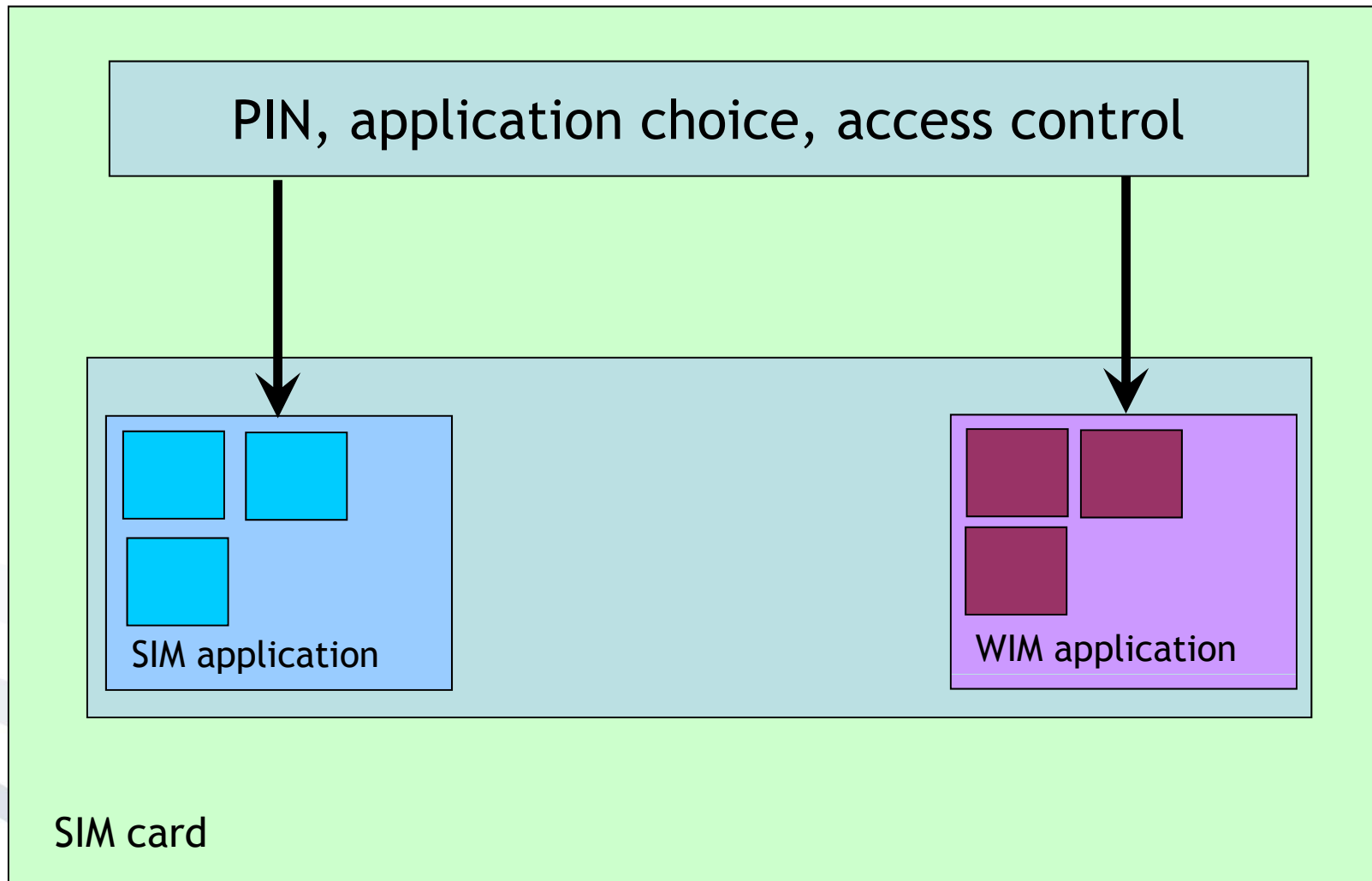
- **ETSI GSM 11.11** [GSM2006] specifies electrical as well as software interfaces between SIM and device.
- A **serial interface** is used for accessing the card.
- Communication through **SIM commands**
- Device can access **files** or execute **actions** through SIM commands.
- „SIM Application Toolkit“ allows for implementing of **additional applications** on a SIM.

- Provides an interface for **Value Added Services** implemented on **programmable SIMs** for interacting with mobile devices
- **Standardised 1996** as ETSI GSM 11.14, extended 1999 [GSM2006]
- **Controls I/O, Telephony, Download**
- Allows for **security functionality**
- „Living standard“

- **Mobile Banking and Brokerage**
 - T-Mobile and T-Online SMS banking
- **Secure payment** via cellular phone
- **Authentication** of users trying to access servers
- **Location-based services**
 - ATM search, navigation
- **Security applications in general**
 - Mobile signatures

- Smartcards – Introduction
- Subscriber Identity Module (SIM)
- WAP Identity Module (WIM)
- Universal SIM (USIM)
- IP Multimedia Services Identity Module (ISIM)
- New Applications – CamWebSIM

- **WAP** is a protocol family implementation of Client/Server applications on mobile devices.
- Originally WAP did not provide sufficient **end-to-end security** for applications.
- The **WAP Identity Module (WIM)** should solve security problems raised by WAP.
- **WIM** is implemented as an **additional application** on a SIM.

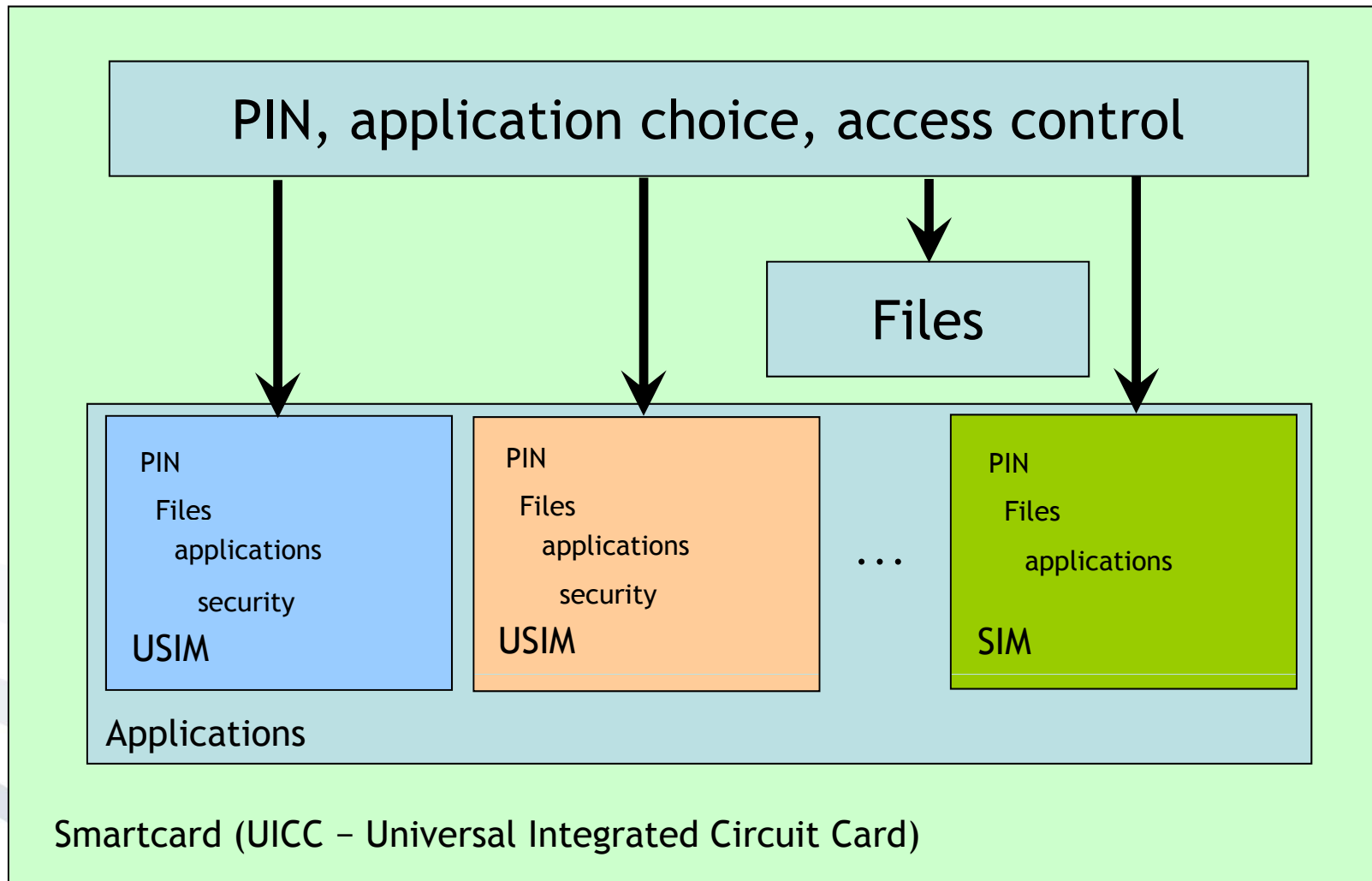


- **Secure storage** for keys and certificates
- **Tamper resistance** of SIM based crypto algorithms
- **Standardised interface** to security functions (PKCS#15)
- **RSA signatures** are implemented on WIM

- Not in widespread use
- Many demonstrations, including signature applications
- Smartcard manufacturers provide WIM as an option for SIMs (e.g. Gieseke & Devrient's StarSIM®).
- Till now no WIM has been certified as signature creation device as required by German "Signaturgesetz" (SigG).

- Smartcards – Introduction
- Subscriber Identity Module (SIM)
- WAP Identity Module (WIM)
- Universal SIM (USIM)
- IP Multimedia Services Identity Module (ISIM)
- New Applications – CamWebSIM

- **Standardised** in 3GPP TS 21.111 and 3GPP TS 31.102 [GSM2006]
- **Successor** of SIM in 3G networks (but 3G networks are downward compatible to many SIMs)
- Supports different „virtual“ **USIMs** and **SIMs** on one cards – i.e. multifunctional smartcard
- Specified as „**UMTS-SIM**“, to support authentication, authorisation and computation of future services



- **Support for multiple applications**
- **End-to-end security** from the USIM to the application
- **Authentication of the network** towards the USIM via cryptography
 - ➔ **Multilateral Security** is possible!
- **Downward compatible** to SIM
- **Extended phone book** on card:
 - Email addresses
 - Multiple names & numbers for each entry
 - More memory
 - Standardised entries

- **Market entry of USIM „disguised“ as SIM**
 - ➔ UMTS activated by operator
- **Multiple USIMs – possibly from competing providers – can technically coexist on one card. Selection via menu on mobile device**
 - ➔ Reduction of operator switching cost
- **Switching to anonymous prepaid USIM as a privacy option when using privacy sensitive services?**

- Smartcards – Introduction
- Subscriber Identity Module (SIM)
- WAP Identity Module (WIM)
- Universal SIM (USIM)
- IP Multimedia Services Identity Module (ISIM)
- New Applications – CamWebSIM

- An **IP Multimedia Services Identity Module (ISIM)** is an application running on a UICC smart card in a 3G mobile telephone in the IP Multimedia Subsystem (IMS).
- It contains parameters for identifying and authenticating the user to the IMS.
- The ISIM application can co-exist with SIM and USIM on the same UICC making it possible to use the same smartcard in both GSM networks and earlier releases of UMTS.
- It is specified in 3GPP TS 31.103 [GSM2006] and described in e.g. [G&D2006].

- The ISIM contains:
 - One **private user identity** (username@operator.com)
 - One or more **public user identities** (user@operator.com, or tel:+1-212-555-12345)
 - A long-term secret used to authenticate and calculate cipher keys

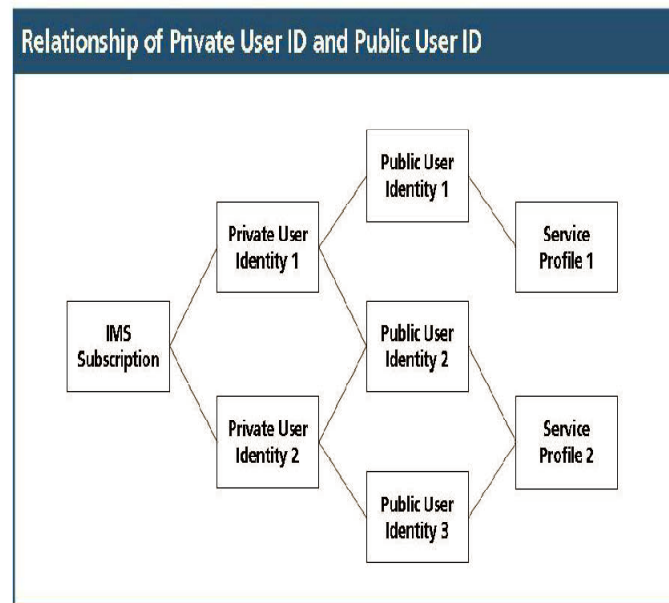
- The **Private User Identity**
 - A unique global identity assigned by the home network operator and used for example for registration, authorisation, administration, and billing purposes
 - not accessible to the user
 - only visible to control nodes inside the IMS
 - One ISIM application includes only one private user identity - but an IMS user may have several UICC cards carrying an ISIM application or a UICC card with several different ISIM applications.

- **Public User Identities**
 - Every IMS subscriber has one or more Public User Identities.
 - The Public User Identity is used for requesting communications to other users.
 - This identity is visible to the outside and can for example be included on a business card.

- Service Profile
 - identifies the services a user may currently use such as video telephony, VoIP, Presence
 - defined and maintained in the Home Subscriber Server (HSS) of the subscriber's home network

- Home domain name
 - The ISIM application stores the home domain name of the subscriber securely.
 - This can not be changed or modified.

- In case of more than one IMS subscription, there may be a many-to-many mapping of Private User Identities to Public Users IDs.
- Each Public User Identity is assigned exactly one Service Profile but a Service Profile may be assigned to more than one Public User ID.



- Smartcards – Introduction
- Subscriber Identity Module (SIM)
- WAP Identity Module (WIM)
- Universal SIM (USIM)
- IP Multimedia Services Identity Module (ISIM)
- New Applications – CamWebSIM

- A smaller personal security device

HTTP server (!) in the GSM SIM card

- A SIM based on the MS Smart Card can be programmed

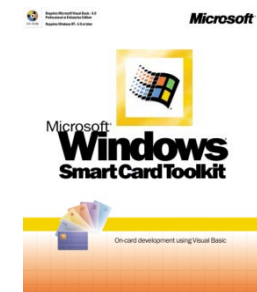


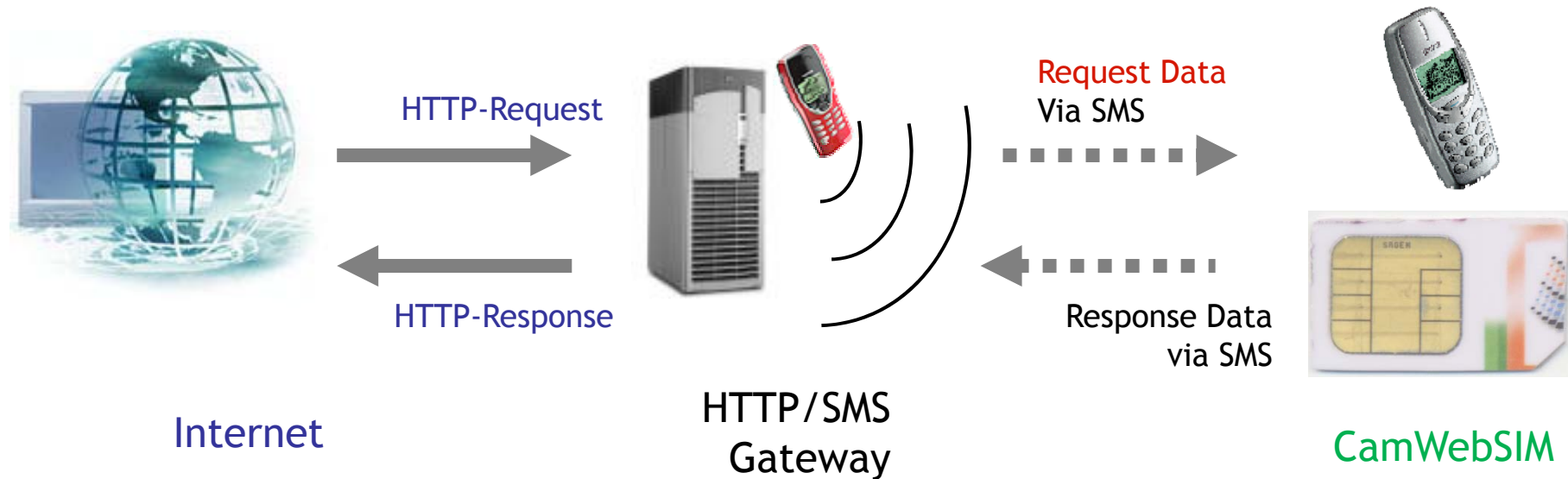
Connection between GSM and Internet

- HTTP Requests via HTTP/SMS Gateway to mobile phone

More than a cool demo ...

- Explore the relation between PDAs and Smart Cards
 - What can really be done on the Smart Card?
 - Can Smart Card encrypt info to be stored in the PDA?
- Explore the possibilities of extra interaction channels
 - SMS in parallel to Internet
- Research Authorisation vs. Authentication vs. Identification





[http://www.camwebsim.telco.com/+14253334711/dt=\(Hello World\)](http://www.camwebsim.telco.com/+14253334711/dt=(Hello World))

- Website
 - <http://www.camwebsim.telco.com/>
- Tel-No.
 - [+14253334711/](tel:+14253334711)
- Command (SIM AT V 2.0 ++)
 - `dt=(Hello World!)`
 - `LOCATION INFO info`
 - `SELECT ITEM si=(title,item1,item2,...)`
 - `DISPLAY TEXT dt=(text)`
 - `GET INPUT gi=(text)`
 - `MAIL NOTIFICATION mail=(who,subj,phone)`
 - `SIGN CHEQUE cq=(who,amount)`

Website

Tel.-No.

Command

.com.

WELCOME ADDRESS ITEMS WRAP SHIP  PAY CONFIRM

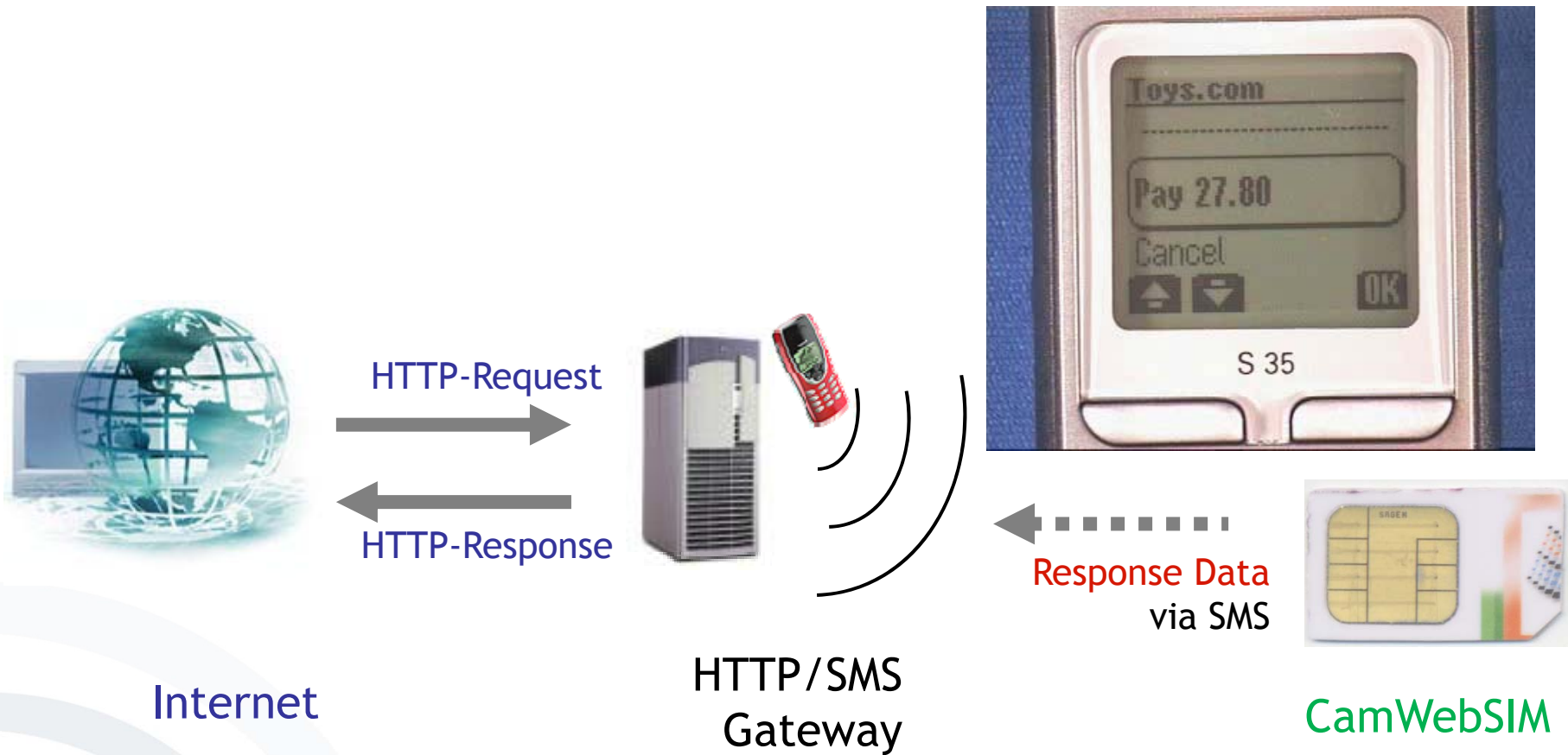
■ More Payment Channels

- Telephone Bill
- ...

Toys.com
3 Gimmicks
▶ Pay \$ 27.80
Cancel
Help



si=(Toys.com 3 Gimmicks, Pay \$ 27.80, Cancel, Help)



www.camwebsim.telco.com/+14253334711/
si=(Toys.com 3 Gimmicks, Pay 27.80, Cancel, Help)

- Technologywise

- Connected a smart card to the Internet

Goal: transparent, uniform access to smart card services

- Used the mobile phone as a trusted device

Assumed a secure path between SIM and display/keyboard

! This might be (more) dangerous with more complex phones

- Used the existing GSM infrastructure and security model for payment authorisation

User authentication key is stored in the SIM

- ...

- Applicationwise

- ...
- Used the existing GSM infrastructure and security model for payment authorisation
User authentication key is stored in the SIM
- *Provided a telecom with a new revenue channel based on an existing process*
Telecoms as payment servers (the Teletext model)
- *Enabled cash-like payment for Internet services*
In countries where one does not need to register a name with a prepaid GSM account



ATMEL 3232/ ... 8 bit CPU
5 MHz, 32K Flash, 32K EEPROM,
1K RAM
9600 Bit/s serial I/O

Sagem Smart Card

SMS limits

- No guaranteed delivery times
- 140 “real” Bytes just cover a 128 Bytes signed message ...
- ... and sometimes not even that
- We look forward to GPRS.

Space limits

- More than 32K in the chip would be helpful.

Phone capability limits

- SIM Application Toolkit Support is being interpreted widely ...

- Website
 - <http://www.camwebsim.telco.com/>
- Tel-No.
 - [+14253334711/](tel:+14253334711)
- Command (SIM AT V 2.0 ++)
 - `dt=(Hello World!)`
 - `LOCATION INFO info`
 - `SELECT ITEM si=(title,item1,item2,...)`
 - `DISPLAY TEXT dt=(text)`
 - `GET INPUT gi=(text)`
 - `MAIL NOTIFICATION mail=(who,subj,phone)`
 - `SIGN CHEQUE cq=(who,amount)`

Website

Tel.-No.

Command

- [GSM2006] GSM Specification, www.3gpp.org/ftp/Specs/archive; accessed 2006-11-03.
- [EffingRankl2002] Effing, Wolfgang and Rankl, Wolfgang (2002) Handbuch der Chipkarten, Hanser-Verlag
- [GSM2009] GSM Association (2009), Market Data Summary (Q2 2009) - Connections by Bearer Technology, http://www.gsmworld.com/newsroom/market-data/market_data_summary.htm, accessed 2010-10-10.
- [GSM2010] GSM Association (2010), GSM Technology, <http://www.gsmworld.com/technology/index.htm>, accessed 2010-11-24.
- [G&D2006] Giesecke & Devrient GmbH (2006), White Paper IP Multimedia Services Identity Module (ISIM), www.gi-de.com/pls/portal/maia.display_custom_items.DOWNLOAD_SEEALSO_FILE?p_ID=6083&p_page_id=55066&p_pg_id=4; accessed 2006-11-30
- [McDonalds2007] McDonald's Corporation (2007), www.mcdonalds.ca/en/aboutus/faq.aspx, accessed 2007-09-19.

- [SecCommerce2002] SecCommerce (2002), Überblick über Smartcards, www.seccommerce.de/de/fachwissen/technologie/smartcards/smart_cards_architektur.html, accessed 2006-11-03.
- [UN2006] United Nations (2006), www.un.org/Overview/unmember.html, accessed 2010-11-24.
- [Wiki2010] Wikipedia. List of countries with McDonald's franchises, http://en.wikipedia.org/wiki/List_of_countries_with_McDonald's_franchises , accessed 2010-11-24.