mobile business

Lecture 8

Smartcards and Related Application Infrastructures

Mobile Business I (WS 2016/17)

Prof. Dr. Kai Rannenberg

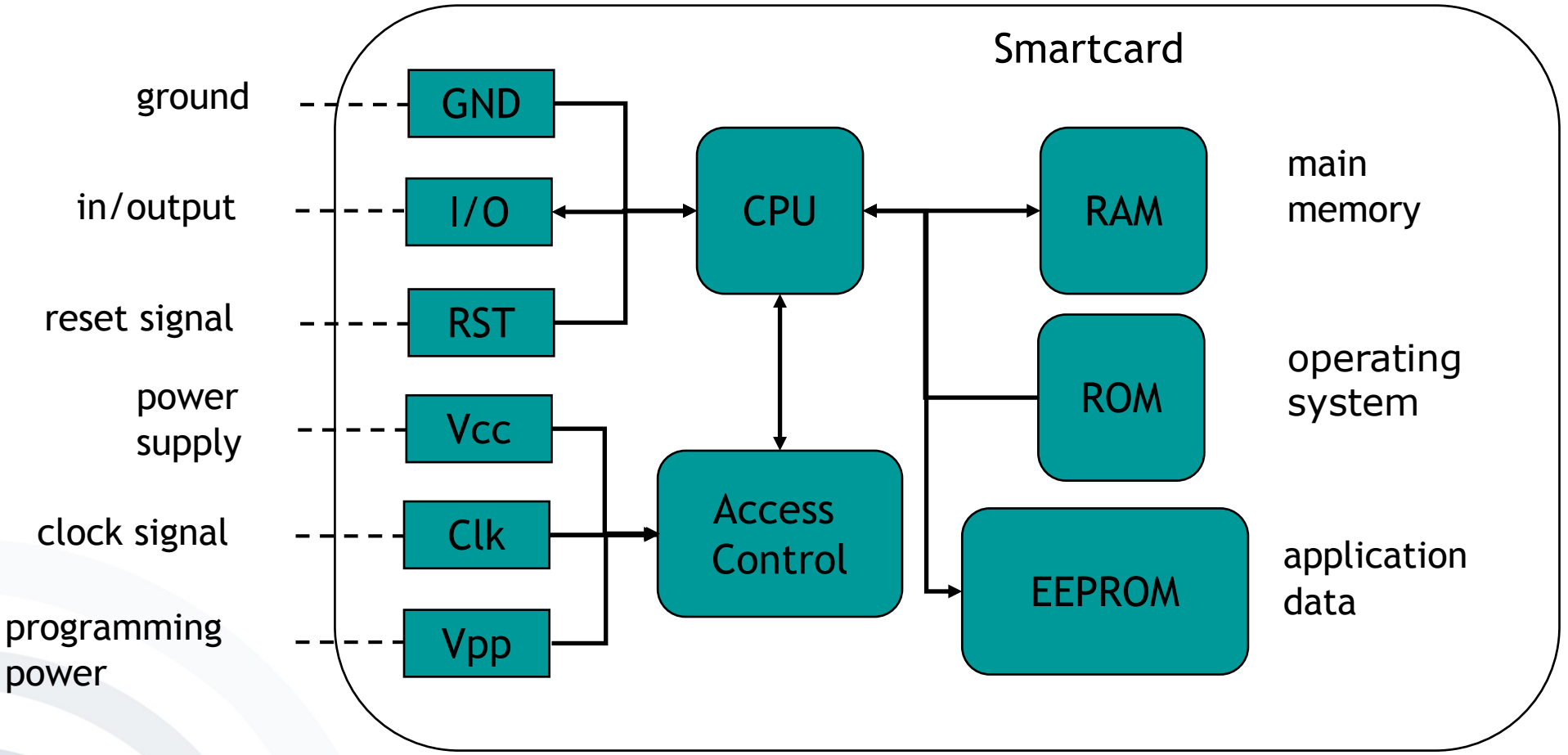
Deutsche Telekom Chair of Mobile Business & Multilateral Security
Johann Wolfgang Goethe University Frankfurt a. M.

- Smartcards – Introduction
- Subscriber Identity Module (SIM)
- WAP Identity Module (WIM)
- Universal SIM (USIM) and UICC
- IP Multimedia Services Identity Module (ISIM)
- Apple SIM
- Google Fi Project
- eSIM
- New Applications — CamWebSIM

Smartcards

- 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.

Smartcards



[Source: SecCommerce2013]

Smartcards

- 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)

mobile business

Smartcards – Examples

Why Smartcards?

Protection needed against:

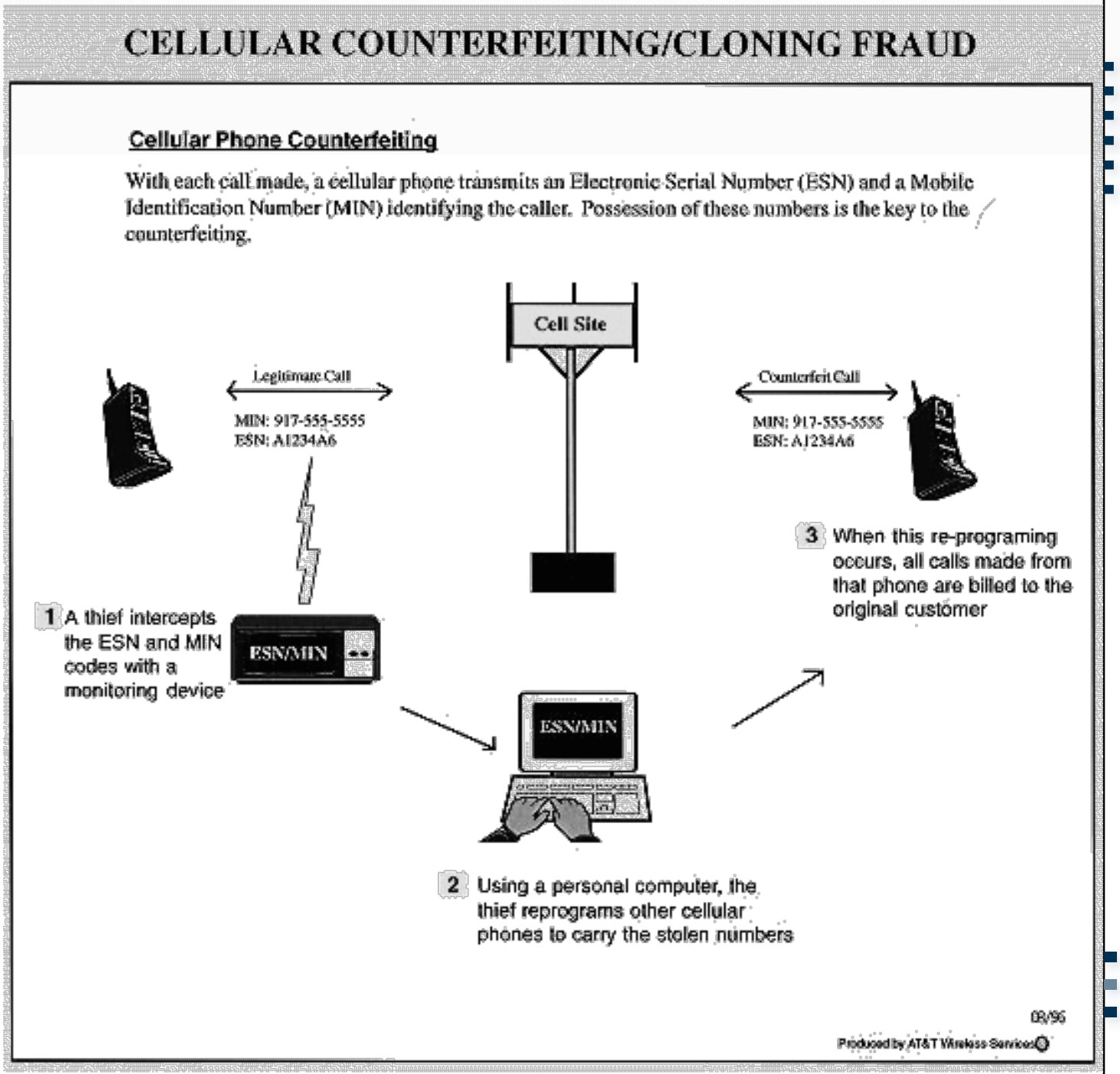
- Unauthorised usage of services through forged user data
- Duplication of a user's credentials
- „Cracking" of credentials
- Billing fraud

mobile business

Example for faulty system design (CDMA)

Duplication of intercepted user IDs

CDMA2000 overcame this by introducing the CSIM.



- Smartcards – Introduction
- Subscriber Identity Module (SIM)
  - Functionality
  - Technology
  - SIM Application Toolkit (SAT)
- WAP Identity Module (WIM)
- Universal SIM (USIM) and UICC
- IP Multimedia Services Identity Module (ISIM)
- Apple SIM
- Google Fi Project
- eSIM
- Applications — CamWebSIM

mobile business

The Subscriber Identity Module (SIM)

- 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**
- By November 2016 around **7.9 billion** mobile-cellular subscriptions (forecast to grow to **10 billion** by 2020) [GSMAI2016] vs. **3,9 billion** mobile broadband subscriptions [ITU2016]
- More countries with SIM infrastructure (ca. 239, 2016-Q3) than McDonalds (118, 2016-Q3) and UN-members (193, 2016-Q3) [GSM2016, Wiki2016, UN2016]
- More and more called "Subscriber **Identification** Module" to reflect progress in the general field of **Identity Management**

Smartcards for Mobile Communication

- **SIM**s 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 $\mathbf{K_i}$ provided by the mobile operator
- Reliably execute computational functions for the mobile device

cf. [EffingRankl2008]

SIM Functionality

- 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.

SIM Card Content (Extract)

- (Rather) static data:
  - IMSI, PIN, PUK
  - A3, A8 crypto algorithms
  - List of allocated (subscribed) services
  - Language preferred 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)

SIM
Integration into Mobile Phones

- **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.
- Meanwhile SIMs are available in different **form factors**
  - Same size as 'regular' smart cards (Full-size, FF).
  - Mini-SIM (2FF) introduced circa 1996
  - Micro-SIM (3FF) introduced in 2010
  - Nano-SIM (4FF) introduced in 2012

[Wiki2014]

SIM Application Toolkit – SAT

- 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“

SAT – Application Examples

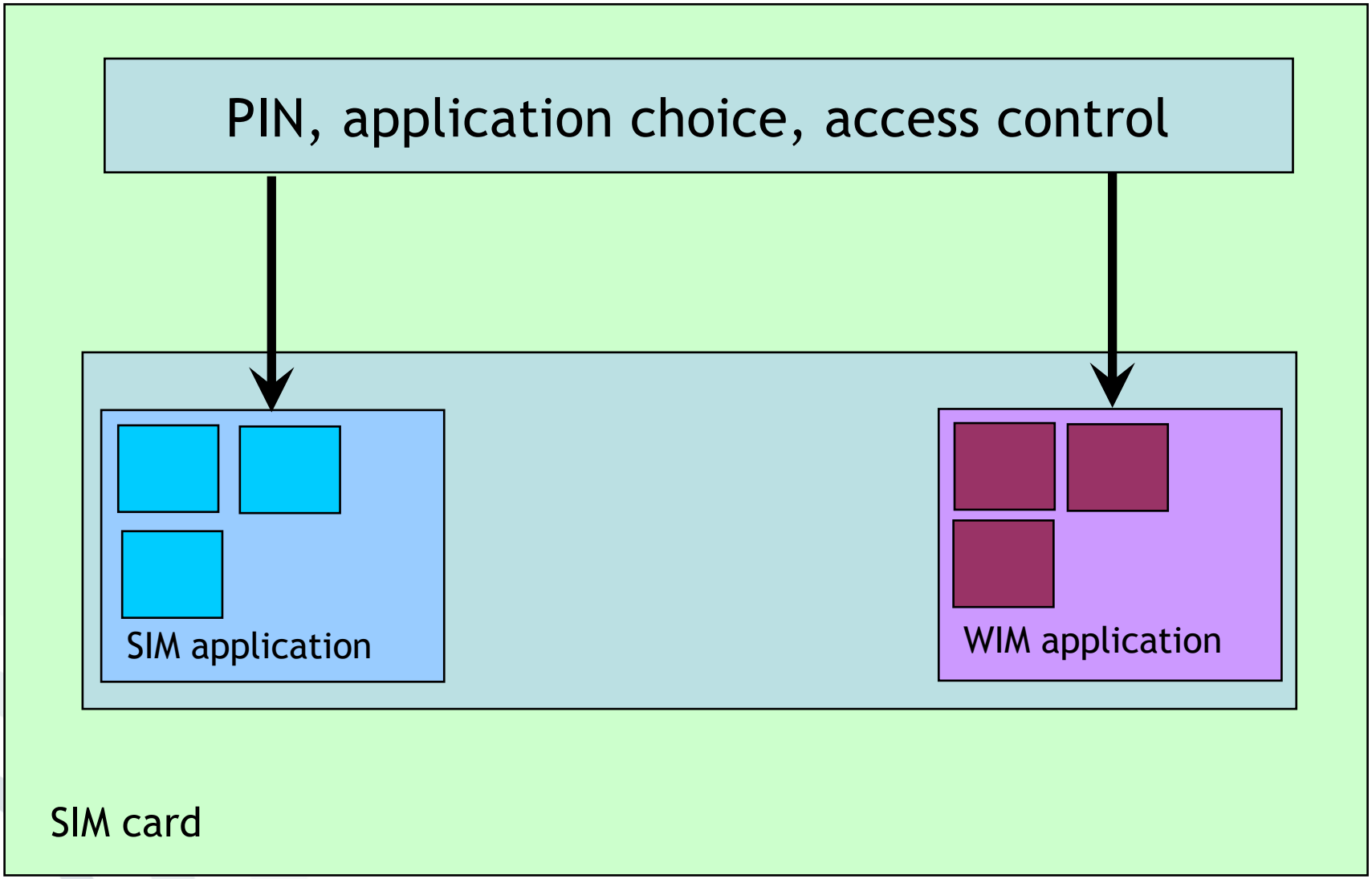
- **Mobile Banking** and **Brokerage**
  - T-Mobile and T-Online SMS banking
- **Secure payment** via cellular phone
- **Authentication** of users trying to access servers
- **Location-based services**
  - ATM search, navigation
- **Security applications in general**
  - Mobile signatures

- Smartcards – Introduction
- Subscriber Identity Module (SIM)
- WAP Identity Module (WIM)
- Universal SIM (USIM) and UICC
- IP Multimedia Services Identity Module (ISIM)
- Apple SIM
- Google Fi Project
- eSIM
- Applications — CamWebSIM

WIM – WAP Identity Module

- **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.
- More and more called "**Wireless Identification** Module" to reflect progress in the general field of **Identity Management**

SIM / WIM – Structure



WIM – Security Functionality

- **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

WIM in Real Life

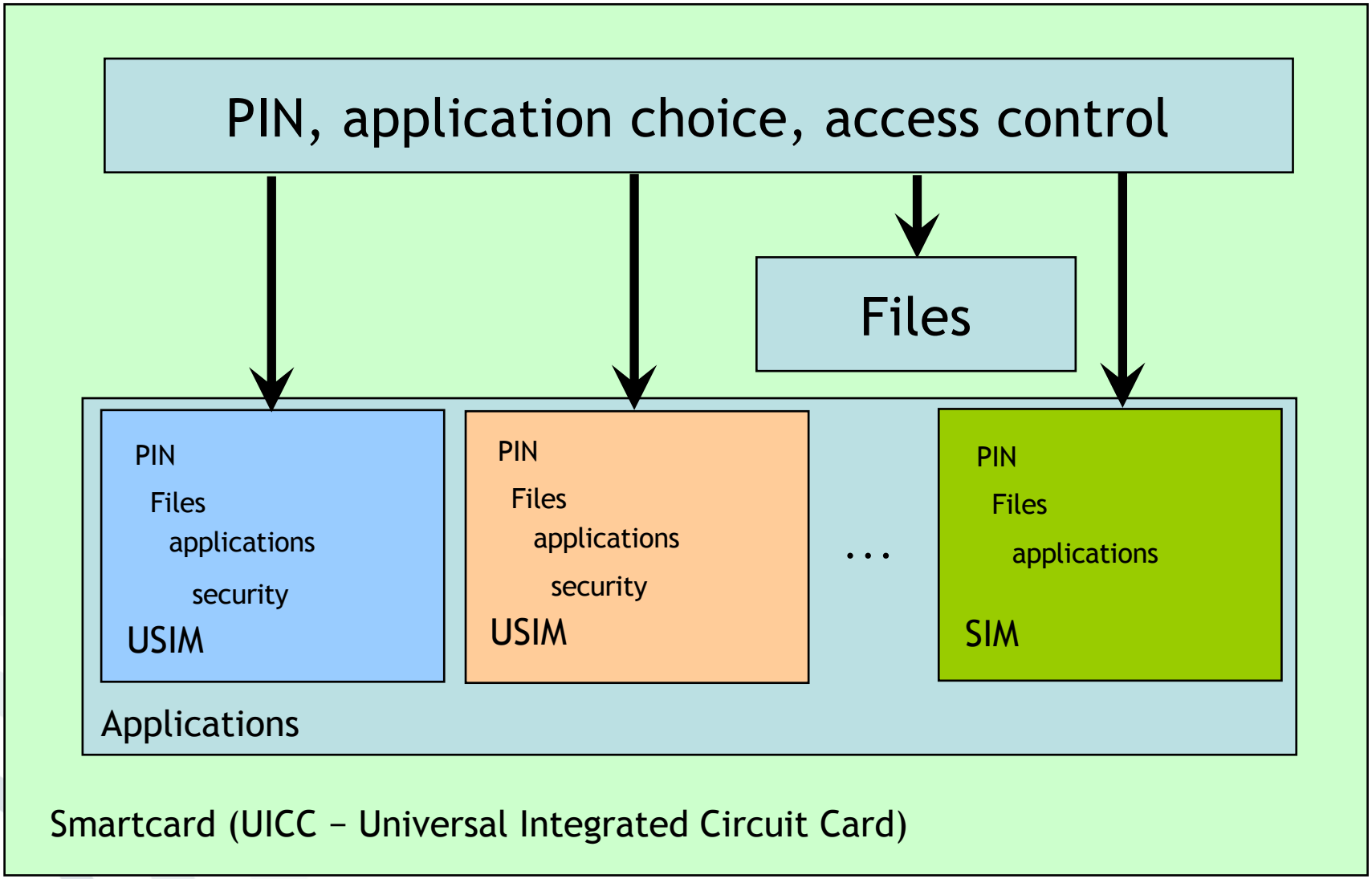
- Not in widespread use
- Many demonstrations, including signature applications
- Smartcard manufacturers provide WIM as an option for SIMs (e.g. Gieseke & Devrient's StarSIM®).
- Till now no WIM has been certified as signature creation device as required by German "Signaturgesetz" (SigG).

- Smartcards – Introduction
- Subscriber Identity Module (SIM)
- WAP Identity Module (WIM)
- Universal SIM (USIM) and UICC
- IP Multimedia Services Identity Module (ISIM)
- Apple SIM
- Google Fi Project
- eSIM
- Applications — CamWebSIM

Universal SIM – USIM

- **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 card – i.e. multifunctional smartcard
- Specified as **„UMTS-SIM“**, to support authentication, authorisation and computation of future services

USIM on UICC – Structure



USIM – Features

- **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

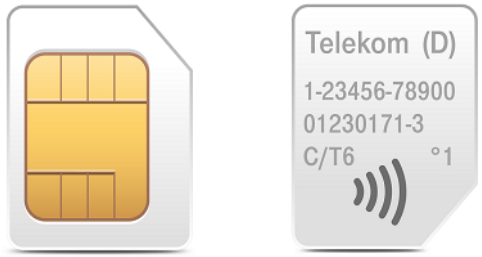
USIM – Visions of new Opportunities

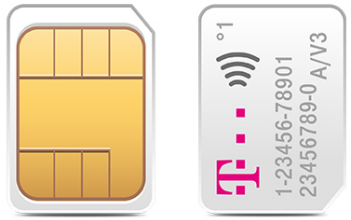
- **Market entry** of USIM „disguised“ **as SIM**
  ➲ UMTS activated by operator
- **Multiple USIMs** – possibly **from competing providers** – can technically coexist on one card. Selection via menu on mobile device
  ➲ Reduction of operator switching cost

- Switching to anonymous prepaid USIM as a privacy option when using privacy sensitive services?

UICCs as Secure Elements

- Secure Elements (SE) are hardware tokens, that offer secure services, e.g. tamper-proof storage and cryptographic operations (cf. Lecture 12).
- UICCs are one form factor of a Secure Element (SE), enabling secure mobile applications and services.





[DTAG2014]

- Smartcards – Introduction
- Subscriber Identity Module (SIM)
- WAP Identity Module (WIM)
- Universal SIM (USIM) and UICC
- IP Multimedia Services Identity Module (ISIM)
- Apple SIM
- Google Fi Project
- eSIM
- 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 [3GPP2016] and described in e.g. [GSM2006].

ISIM

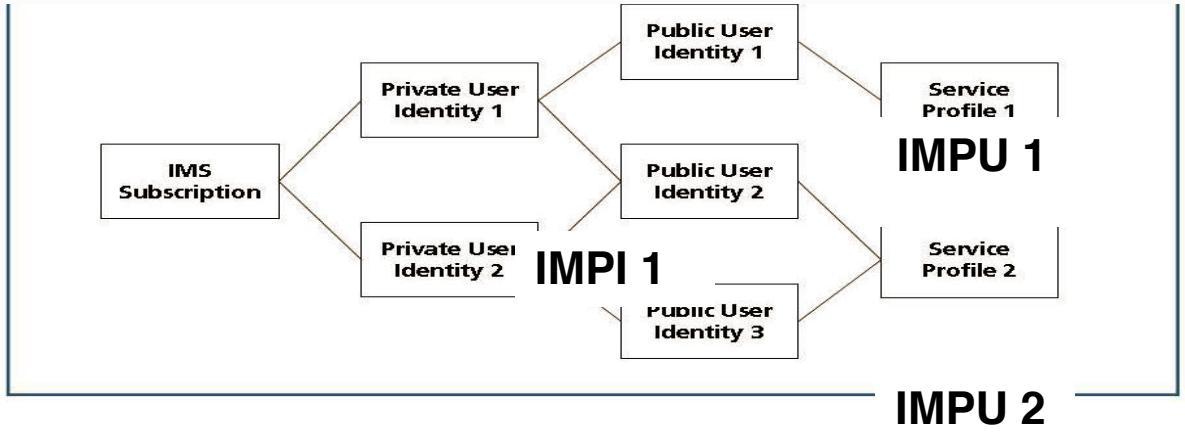
User Identifiers ("Identities") and Secret

- The ISIM contains:
  - One "IM Private Identity"
  - One or more "IM PUblic Identities"
  - A long-term secret used to authenticate and calculate cipher keys
- The IM **Private** Identity (IMPI)
  - Unique global identifier per IMS subscriber: username@operator.com
  - Assigned by the home network operator
  - Used for e.g. registration, authorisation, administration, and billing
  - Not accessible to the user
  - Only visible to control nodes inside the IMS
  - One ISIM application includes only one IMPI – but an IMS user may have several UICC cards carrying an ISIM application or a UICC card with several different ISIM applications.
- IM **PUblic** Identities (IMPUs)
  - Every IMS subscriber has one or more IMPUs, e.g. user@operator.com, or tel:+1-212-555-12345.
  - Used for requesting communications to other users
  - Visible to the outside, e.g. to be shown 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.

ISIM

IMPIs, IMPUs, and Service Profiles



- In case of more than one IMS subscription, there may be a many-to-many mapping of IMPIs to IMPUs.
- Each IMPU is assigned exactly one Service Profile, but a Service Profile may be assigned to more than one IMPU.

- Smartcards – Introduction
- Subscriber Identity Module (SIM)
- WAP Identity Module (WIM)
- Universal SIM (USIM) and UICC
- IP Multimedia Services Identity Module (ISIM)
- Apple SIM
- Google Fi Project
- eSIM
- Applications — CamWebSIM

iPad Apple SIM

- Apple SIM is available for purchase in Australia, Canada, France, Germany, Italy, the Netherlands, Spain, Sweden, Switzerland, Turkey, the UK, and the US.
- SIM contains credentials for several networks.
- The customer must “activate” the desired network, which may dedicate the SIM to that network allowing no further change with that SIM.
- When travelling abroad, the customer can use the same SIM card for a chosen mobile data tariff from “selected” operators in 90 countries worldwide.
- Available since October 2014.
- Costs in Germany:
  - SIM card for 5 EUR
  - 1 GB of data for a month for 50 EUR.
- In November 2016 supported by in cellular-enabled versions of its iPad Air 2, iPad mini 3, iPad mini 4, and iPad Pro tablets in Apple Retail Stores in Australia, Canada, France, Germany, Italy, Japan, the Netherlands, Spain, Sweden, Switzerland, Turkey, the United Kingdom, and the United States.

Source: http://www.apple.com/ipad/LTE/

- Smartcards – Introduction
- Subscriber Identity Module (SIM)
- WAP Identity Module (WIM)
- Universal SIM (USIM) and UICC
- IP Multimedia Services Identity Module (ISIM)
- Apple SIM
- Google Fi Project
- eSIM
- Applications — CamWebSIM

Google's Fi Project

- Connectivity through different operators (since April 2015)
  - In cooperation with Sprint and T-Mobile in the US (joint SIM card)
  - Google is the contract partner to the subscriber.
  - Currently supported by Google's Pixel, Nexus 6P, Nexus 5X and Nexus 6 phones
  - Seamless switch between available Wi-Fi hotspots and the mobile network
- Simple price tariffs starting from $20 per month
  - All 135+ countries in Project Fi's network include the same great benefits, such as:
    - same rate pricing,
    - high speed data at the same $10/GB,
    - unlimited domestic SMS and calls
    - Unlimited "roaming" SMS and calls for 20¢ / minute.
  - Data tariff available in 120+ countries
  - Refund for the unused data each month
  - Group plans available, friends and family for additional $15 per month each

https://fi.google.com/about/rates/

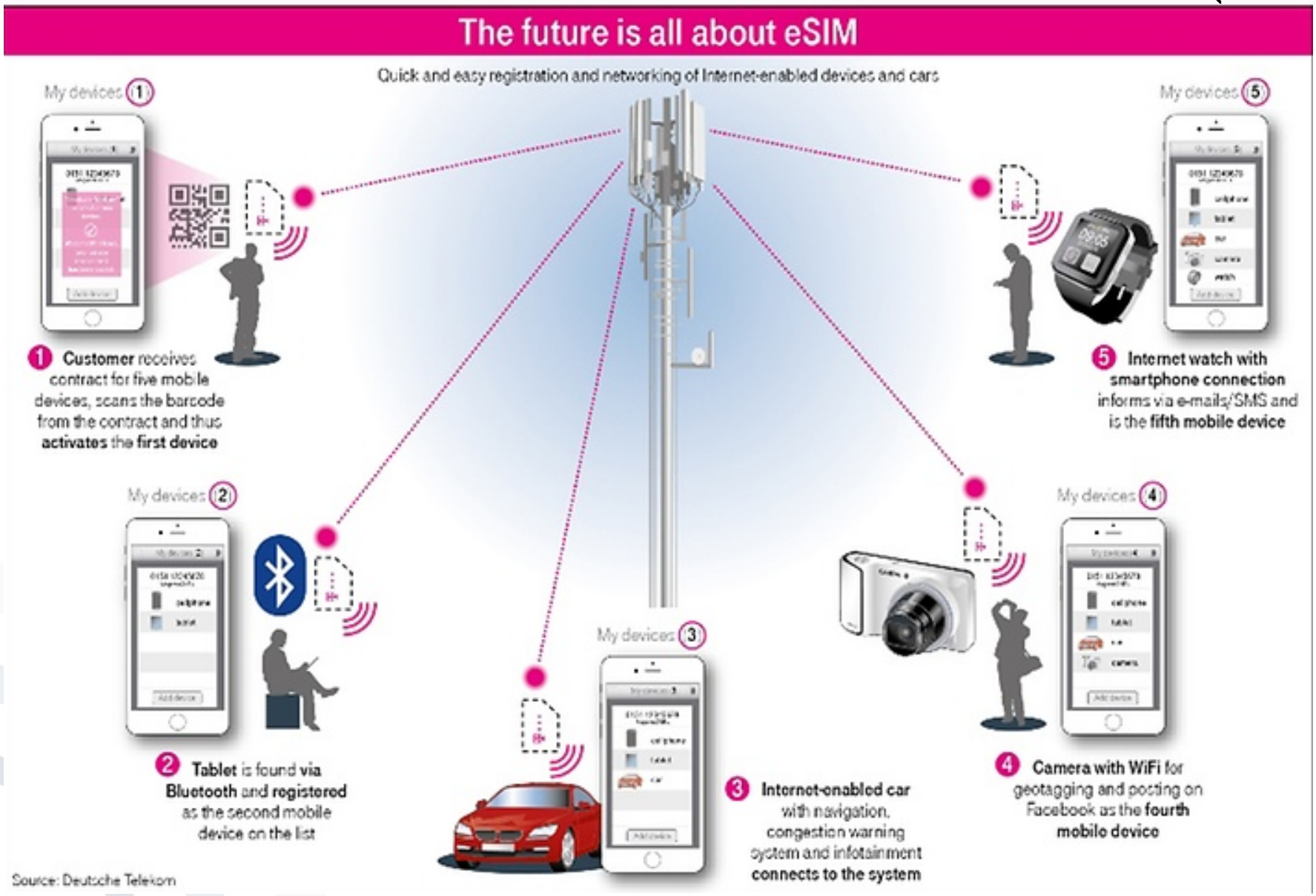
- Smartcards – Introduction
- Subscriber Identity Module (SIM)
- WAP Identity Module (WIM)
- Universal SIM (USIM) and UICC
- IP Multimedia Services Identity Module (ISIM)
- Apple SIM
- Google Fi Project
- eSIM
- Applications — CamWebSIM

eSIM
Embedded SIM (1)

- Characteristics of the embedded SIM (eSIM)
  - Embedded as a secure element in hardware (mobile devices, cars, household devices – to enable the deployment of IoT)
  - Likely implemented with a programmable ROM
  - Probably a “game changer”
    - Easy to switch providers/operators
    - Tariffs can be programmed/limited programmatically to devices, e.g. a 2-year contract can limit update to the card until the end of contract.
- Global standard being drafted by the GSMA, will require new terminal hardware

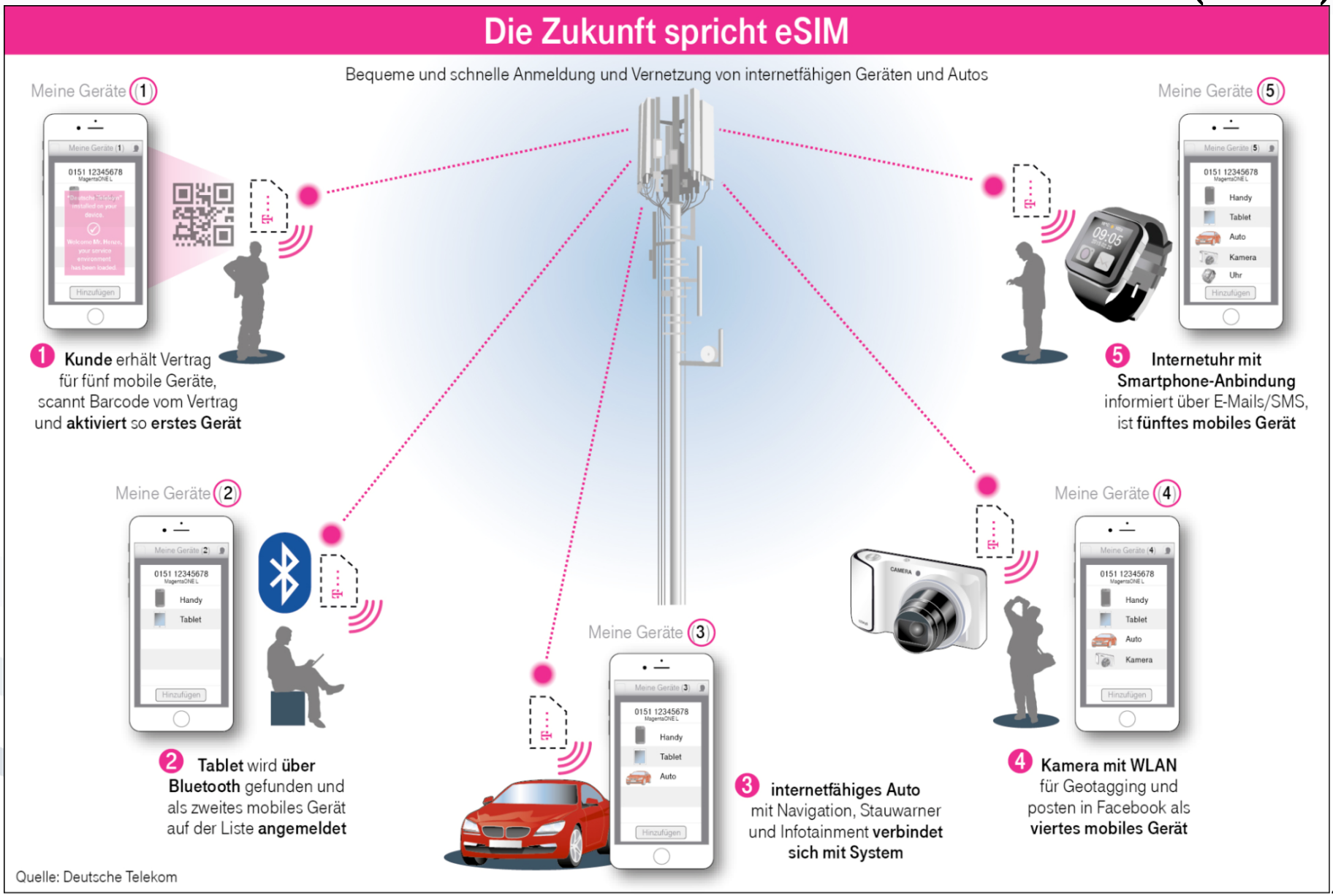
[Heise2015, T3n2015]

eSIM
Embedded SIM (2en)



[Telekom2015]

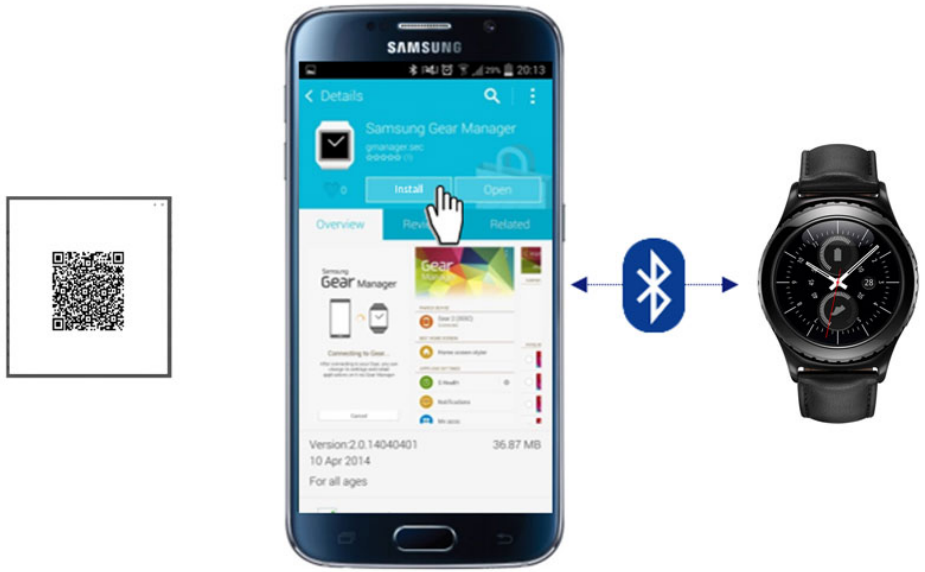
eSIM
Embedded SIM (2de)



[Heise2015]

eSIM
Embedded SIM (3)

- German market situation
  - Vodafone and O2 provide the first product/tariff with eSIM [Telefonica2016, Vodafone2016].
  - Telekom announced plan to introduce eSIM in 2016.
- Uncertainties
  - Fears of limited customer choice of operator/tariff (preselected list of operators)
  - Business models (shifting the power from the network operators to device vendors)



- Smartcards – Introduction
- Subscriber Identity Module (SIM)
- WAP Identity Module (WIM)
- Universal SIM (USIM) and UICC
- IP Multimedia Services Identity Module (ISIM)
- Apple SIM
- Google Fi Project
- eSIM
- 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

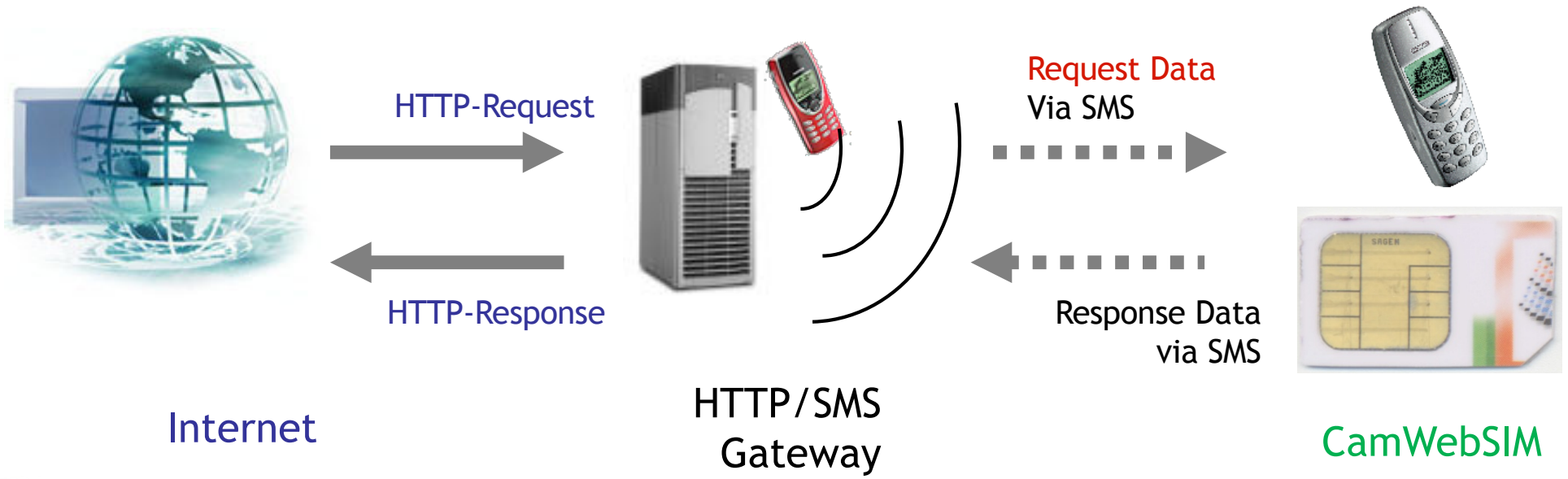
More than a cool demo …

- 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

mobile business

CamWebSIM

Combine Infrastructures



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

SIM Addressing via HTTP

- Website
  - http://www.camwebsim.telco.com/
- Tel-No.
  - +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

mobile business

SIM based Payment Authorisation

.com.

WELCOME ADDRESS ITEMS WRAP SHIP PAY CONFIRM

- More Payment Channels
  - Telephone Bill
  - …

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

Payment Authorisation live

HTTP-Request

HTTP-Response

Response Data
via SMS

Internet

HTTP/SMS
Gateway

CamWebSIM

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

What have we done in this example?

- 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
  - …

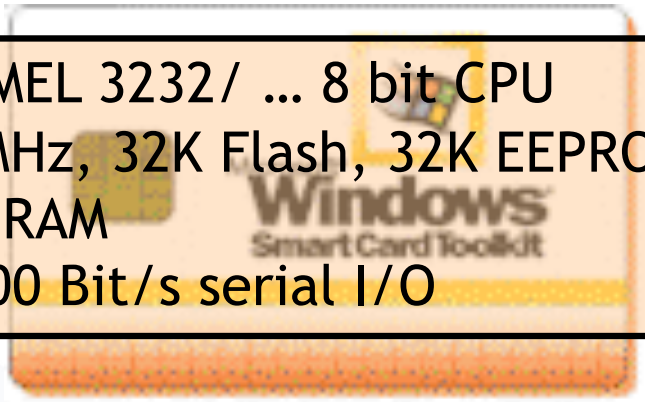
mobile business

What have we done in this example?

- 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

Technical Details and Issues (in 2001)

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 …

SIM Addressing via HTTP indication application areas

- Website
  - http://www.camwebsim.telco.com/
- Tel-No.
  - +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

Literature

- [3GPP2016] 3GPP (2013), https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=1804, accessed 2016-11-17
- [DTAG2014] Deutsche Telekom: SIM-Kartenformate, www.t-mobile.de/sim-kartenformate/0,27115,28905-_,00.html, accessed 2014-11-05.
- [EffingRankl2008] Effing, Wolfgang and Rankl, Wolfgang (2008) Handbuch der Chipkarten: Aufbau – Funktionsweise – Einsatz von Smart cards, Hanser-Verlag
- [GSM2006] GSM Specification, www.3gpp.org/ftp/Specs/archive, accessed 2013-10-03
- [GSM2013] GSM Association (2013), GSM Technology, www.gsma.com/aboutus/gsm-technology/gsm, accessed 2014-09-03
- [GSM2015] GSM Association (2015), GSM Technology, www.gsma.com/aboutus/gsm-technology/gsm, accessed 2015-11-02
- [GSMA2016] Definitive data and analysis for the mobile industry, http://gsmaintelligence.com (accessed 2016-11-30)
- [GSMAI2016] ONE BILLION NEW UNIQUE MOBILE SUBSCRIBERS BY 2020, FINDS NEW GSMA STUDY, May 2, 2015. http://www.gsma.com/newsroom/press-release/one-billion-new-unique-mobile-subscribers-by-2020-gsma/ (accessed 2016-11-30)
- [Heise2015] Heise.de (2015), “Deutsche Telekom: eSIM soll 2016 kommen”, http://www.heise.de/newsticker/meldung/Deutsche-Telekom-eSIM-soll-2016-kommen-2921732.html, accessed 2016-11-28
- [Investopadia2016] 10 Countries With the Most McDonald's Locations (MCD), http://www.investopedia.com/articles/markets-economy/091716/10-countries-most-mcdonalds-locations-mcd.asp (accessed on 2016-11-30)
- [ITU2016] International Telecommunication Union, ICT Facts and Figures 2016, http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2016.pdf, accessed 2014-09-03
- [McDonalds2016] McDonald’s Corporation (2016), http://www.aboutmcdonalds.com/mcd/our_company.html, accessed 2016-11-30

Literature

- [SecCommerce2013] SecCommerce (2013), Überblick über Smartcards, www.seccommerce.de/de/component/content/article/39-root-de/knowledge/technology/122-smartcard-architecture.html, accessed 2013-10-10
- [T3n2015] T3n.de (2015), "Warum die eSim von Apple und Samsung eine Katastrophe für Nutzer und Netzbetreiber ist [Kommentar]", http://t3n.de/news/esim-apple-samsung-katastrophe-624523/, accessed 2015-11-18
- [Telefonica2016] Erste Smartwatch mit eSIM bei O2, 2016-02-18, https://blog.telefonica.de/2016/02/mobile-world-congress-2016-erste-smartwatch-mit-esim-bei-o2/, accessed 2016-11-28
- [Telekom2015] The future speaks eSIM, 2015-11-19, https://www.telekom.com/en/blog/group/article/the-future-speaks-esim-62202, accessed 2016-11-28
- [UN2016] Growth in United Nations membership, 1945-present. http://www.un.org/en/sections/member-states/growth-united-nations-membership-1945-present/index.html, accessed 2016-11-17
- [Vodafone2016] eSIM technology will extend the mobile ecosystem, 2016-02-19, http://www.vodafone.com/content/index/what/technology-blog/esim-technology.html, accessed 2016-11-28
- [Wiki2014] Subscriber identity module, en.wikipedia.org/wiki/Subscriber_identity_module#Formats, accessed 2014-11-06
- [Wiki2016] Wikipedia, List of countries with McDonald's restaurants, https://en.wikipedia.org/wiki/List_of_countries_with_McDonald's_restaurants accessed 2016-12-01