World Class Standards

The SIM

Dr. Klaus Vedder
Chairman ETSI TC SCP

GSM…younger than ever

Lemesos, Cyprus
15 – 16 March 2007

ETSI TC SCP, the Smart Card Committee

- **19 Years of Dedication and Real-life Experience**
  - Founded in March 2000 as the successor of SMG9, the SIM-people, which specified the SIM for GSM, the most successful smart card application ever with over 2.3 billion subscribers and more than 6 billion SIMs and R-UIMs deployed

- **The Mission**
  - Create a series of specifications for a smart card platform, based on real-life (outside) requirements, on which other bodies can base their system specific applications to achieve compatibility between all applications resident on the smart card

The SIM

"A SIM is the physically secured module which contains the IMSI, an authentication algorithm, the authentication key and other (security related) information and functions. The basic function of the SIM is to authenticate the subscriber identity in order to prevent misuse of the MS (Mobile Station) and the network."

From the report of SIMEG#1 in January 1988

Plug-in SIM carrier
Telemig, Brazil, 2005

The SIM in 1988

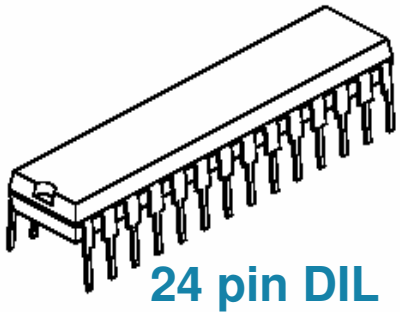
The ID-1 card used by Deutsche Telekom in their analogue network

Option 1:
"IC card"

Option 2:
"Fixed"

Software SIM fully incorporated into the handset OS
Rejected due to security concerns and less flexibility

Option 3:
"Removable"



24 pin DIL with 8 pins connected

vs

The SIM - A Removable Security Module

- The SIM: Providing the security
  - issuer specific authentication algorithm
  - issuer specific algorithm for cipher key generation
  - security management specified by issuer
- The SIM: Providing universal plastic roaming
  - keeping your identity when changing terminal or technology
- The SIM: Freeing the mobile of the burden of the subscription
  - terminal does not contain any subscription data
  - creating a global terminal market
  - bigger choice for the customer through more competition

The SIM became the driver of smart card technology

Any Doubts ?

Some (Early) Firsts

- The SIM - leading to a new generation of micro-controllers
  - The world's first low voltage smart card specs (3V in 95; 1.8 Volt in 99)
  - Memory requirements for smart cards were driven solely by GSM
- The Proactive SIM or the SIM leaving the role of the slave
  - 1991, the first proposal: the SIM should refuse to work if the counter in the SIM for the Advice of Charge charges had an overflow
- Data Download
  - Downloading data into the SIM and managing data fields in the SIM were already practised by the PCN operators in the early 90s

Both features were merged in April 1996 to the *SIM Application Toolkit* the world's first global platform for secure Value Added Services

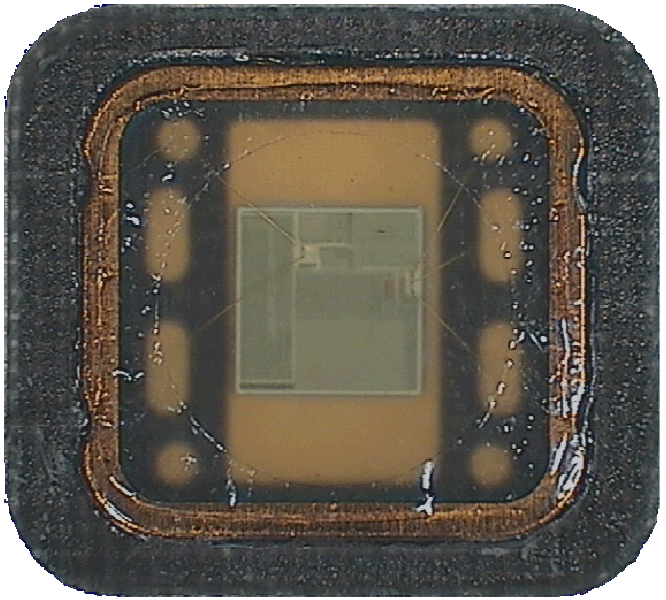
GSM 11.11, 11.14, ...

The world's first global (and most successful) smart card specification

Proactivity - The Old-fashioned Way

Smart Card Chip Evolution

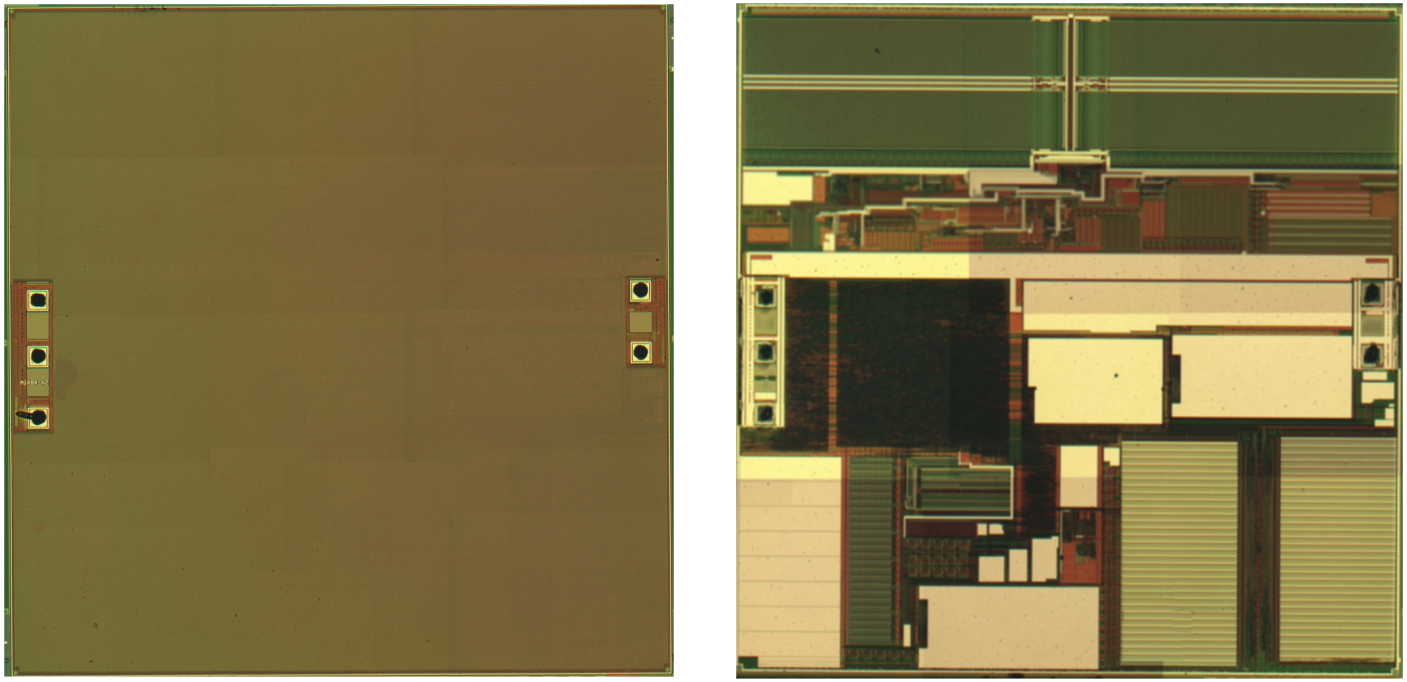
1990	8 Bit CPU
	7 kB ROM
	3 kB EEPROM
	128 Byte RAM
2007	32 Bit CPU
	500 kB ROM
	512kB EEPROM
	16kB RAM
	or
	400 kB Flash memory
	In addition: 1GB Flash



1996

- CPU, RAM, ROM, EEPROM, Crypto-unit on a single piece of silicon
- Crypto-unit for digital signatures, ciphering and other security functions
- Structure ~1990: 1,5 µm; today: ≤ 0,15 µm; metallised surface
- Sensors for Low Voltage, Frequency, Passivation Layer, Light, …..
- Evaluation of HW and SW against Common Criteria (CC)

The Chip Today

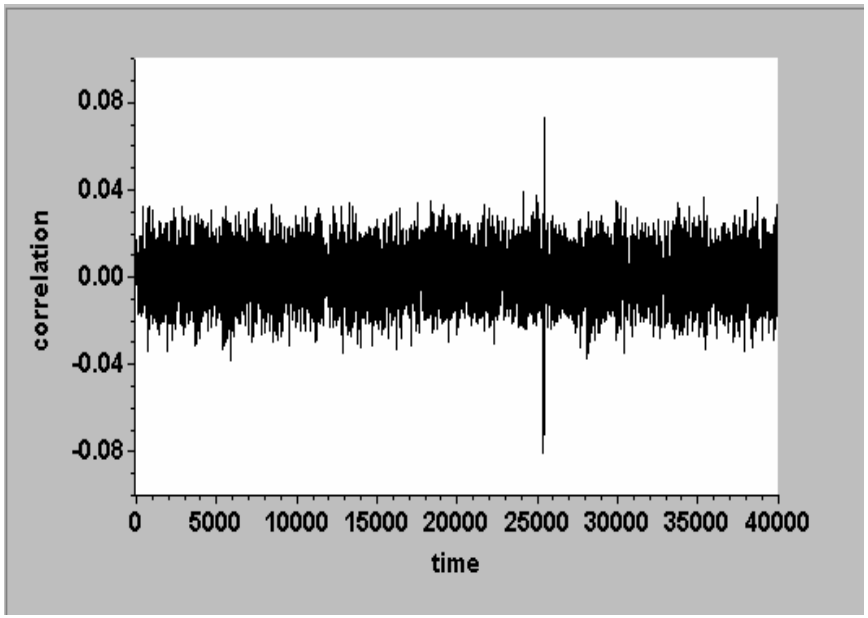


Infineon Technologies SLE66CX322P with Active Shield against state of the art physical attacks: Top view (left) and underlying circuits (right)

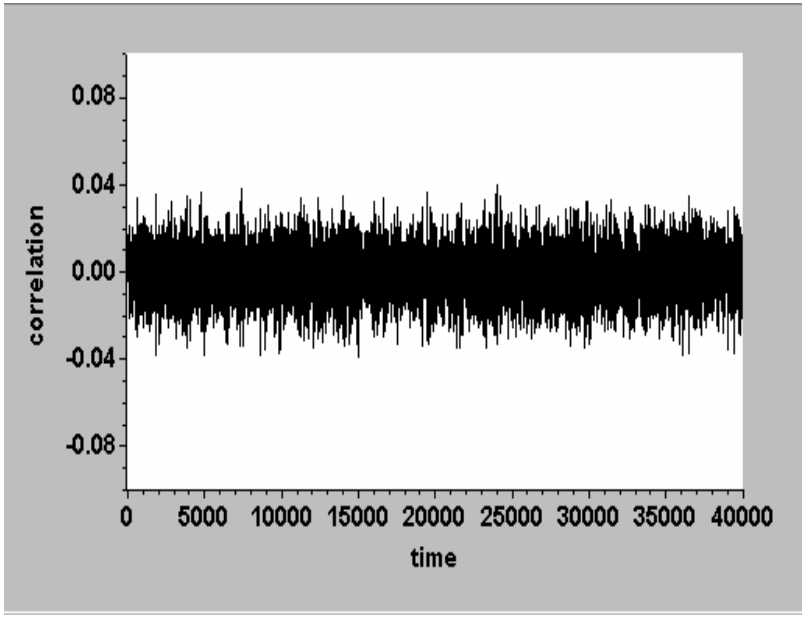
SIM Security - a Function of Hardware and Software

Calculating the secret key from hundreds of power consumption measurings using statistical methods (DPA attacks)

Correlation on output S-box with usage of the right key



Straightforward implementation



Implementation with countermeasures

SIM Broken ?

1998: Comp 128-1 (A3/A8) successfully attacked

- **black box attack against the GSM-MoU example algorithm**
  - **does not utilise any hardware or software property of the SIM**
  - **attack against just one card, not against the system itself**
- **chosen plaintext-ciphertext attack**
  - **approximately 160.000 - 200.000 very specific challenges were *then* required to calculate the secret, subscription specific key Ki**
  - **PIN has to be known or PIN-check disabled**

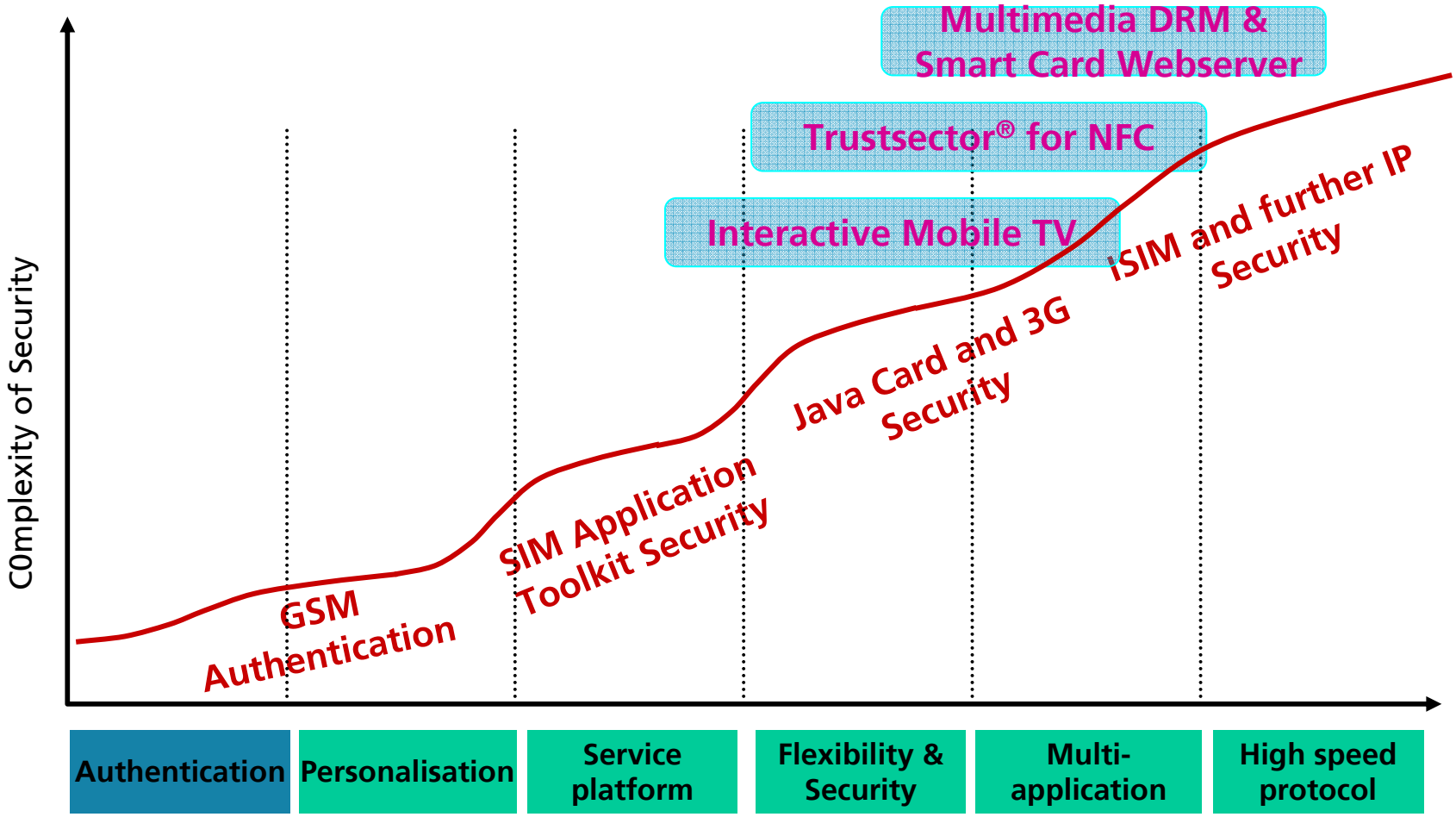
authentication counter with "automatic silencing" of the SIM is no longer a valid countermeasure

- **only 3.000 to 36.000 challenges to calculate Ki needed now**

The answer is: NO

The SIM has successfully stood the test of time

Evolution of Functionality and Security



Mobile TV - Additional Services

- **Concept**
  - During the mobile TV service the subscriber can request additional services such as more information, ringtones or MP3
    - Music files are directly downloaded to the (Multi-Megabyte) (U)SIM
    - Linked right objects will also be sent to the subscriber and used by the DRM client
- **Security**
  - Conditional Access applet on (U)SIM to access Pay-TV content
  - DRM client on (U)SIM to securely store rights for pictures, videos, sounds,…
  - OTA key exchange during mobile TV session

From the SIM to the UICC

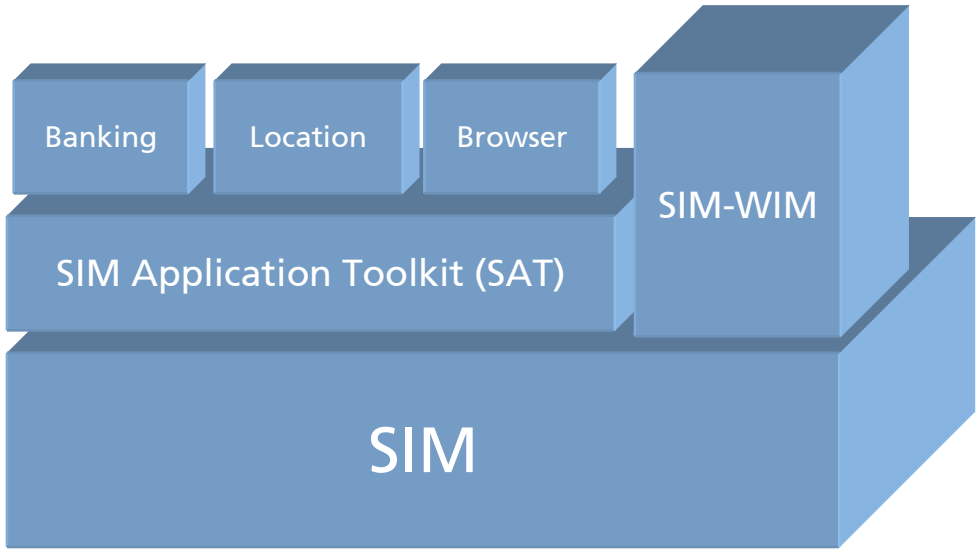
From a
standardised application
offering secure value added services

to a

true multi-application
security platform
providing the user
with a wealth of opportunities

The SIM - a "Mono-application" Smart Card

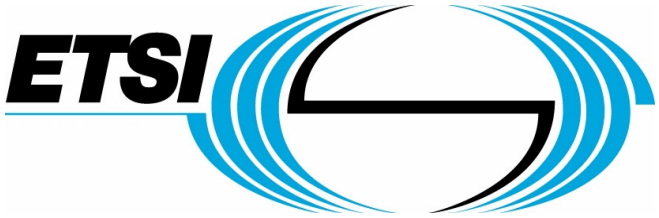
- SIM according to GSM 11.11
  - Additional applications based on SIM Application Toolkit
  - WIM as exception (own command set and triggered by WAP browser)



Where shall we going ?

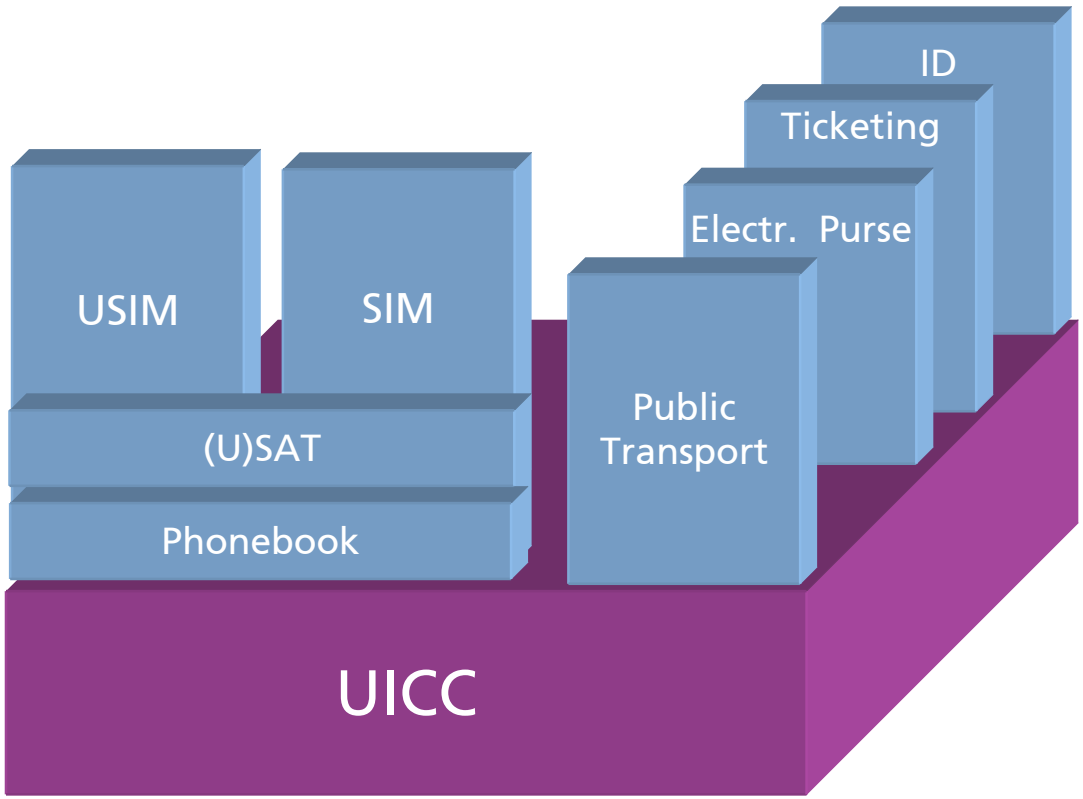
Harmonisation of IC Card Work - The New Role of SMG9

In March 2000 the ETSI Project *Smart Card Platform* (EP SCP) succeeds ETSI SMG9 to provide the smart card platform for all telecommunication systems



The UICC - the Multi-application Platform

- The UICC consists of (all) application independent functions and features
  - clear separation of lower layers and applications
  - up to 20 logical channels to run applications in parallel



Specified by TC SCP

Fire walls between applications provided by smart card (USIM) supplier

High Speed and Contactless

- Current UICC-Terminal interface protocol is not appropriate for graphical user interface and bulk data
- USB – the new high speed interface
  - SCP Plenary selected in November 2006 after a long discussion USB to be the basis for the new high speed protocol
  - This will transform the (U)SIM into a real Internet device and allow the efficient use of large SIMs in the MB and GB range
- The new contactless interface for the (U)SIM will create a wealth of new opportunities
  - Mobile phone works like a contactless card for payment, ticketing, access control, ….
  - Mobile phone works as a card reader for the (U)SIM
  - Selection and specification to be completed this summer

The “Contactless” USIM

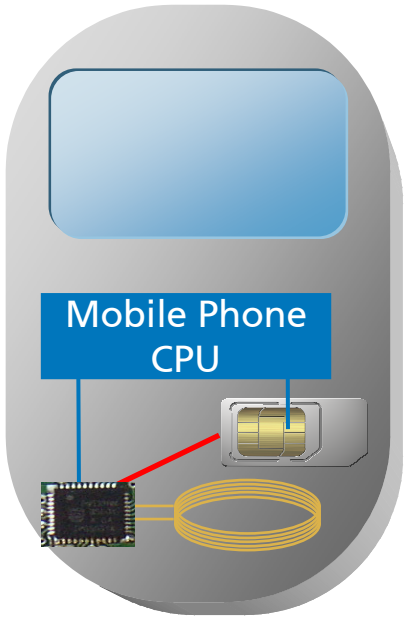
❑Mobile Phones
- High penetration
- Personal device

❑Contactless Cards
- Ease-of-use, convenient
- Infrastructure increasing

perfect match

NFC chip for contactless transmission

Interface between NFC controller and USIM to be finalise this summer



Contactless applications are stored and executed on the mobile or on the USIM

(U)SIM and NFC

- **NFC controller**
  - Responsible for contactless communication
  - Some applications (e.g. ticketing) require a direct connection between the (U)SIM and the NFC controller
- **Management of Applications**
  - Secure environment on the (U)SIM dedicated to different service providers such as banks, public transport companies, ….
  - Encapsulated storage area (Trustsector®) on the (U)SIM for secure execution of applications
  - OTA administration such as activation / de-activation or personalisation of the individual Trustsectors® via a Trusted Third Party (TTP)
  - TTP can act as a trusted “estate agent” and a broker for the memory of the (U)SIM card provided by the operator - (U)SIM becomes a piece of real estate

Web Server and GB SIM

- The Gigabyte SIM
  - First SIMs with 1GB additional memory now used in trials
    - Branding of the device - when inserted the operator branding will be downloaded to the handset and used
    - Storage of Operator specific MMI for the handset, parameter settings
    - Secure DRM, pre-loaded multi-media content
- SIM Web Server
  - Web Server application on (U)SIM utilises execution environment of mobile services
  - Easy to use GUI for services
    - Web look and feel of information loaded on the (U)SIM
    - From SIM Toolkit to SIM Web Server : from MS DOS™ to Windows™
  - (U)SIM is the secure interface to the Internet for the MS
  - A use case: Web Pages with FAQ to save calls to the Operator hotline

The Vision

To turn today's mobile phone into a multipurpose terminal, lifestyle tool, and personal security device

by

establishing a second, contactless communication channel and using the new High Speed Protocol for the (U)SIM

Dr. Klaus Vedder

Head of Telecommunications
Giesecke & Devrient GmbH
Prinzregentenstr. 159
81607 Munich
Germany

klaus.vedder@gi-de.com

ETSI SCP website

http://portal.etsi.org/scp/summary.asp

Next SCP Requirement WG / Plenary Meeting
Madrid 16-18 / 18-20 April 2007