

Lecture 12

Mobile Trusted Devices

Mobile Business I (WS 2011/12)

Prof. Dr. Kai Rannenber

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



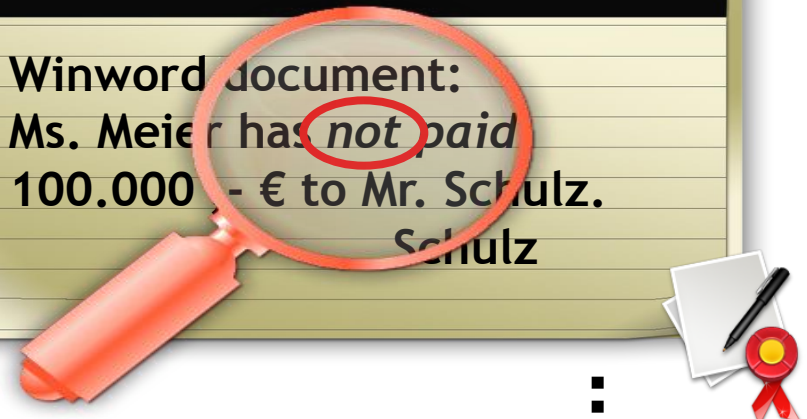
- Introduction and Motivation – Security Issues
- Security of Current Mobile Platforms
- Standardisation Activities for Trusted Mobile Platforms
- (Mobile) Equipment Identifier
- Mobile Market Players and their Interests
- Usage Scenarios for Trusted Mobile Platforms
- Matching Usage Scenarios and Players
- Conclusion and Outlook


3. Mr. Schulz

Receipt
Ms. Meier



Winword document:
Ms. Meier has not paid
100.000,- € to Mr. Schulz.
Schulz




hidden text !!!!

1. ↓

2. ✓

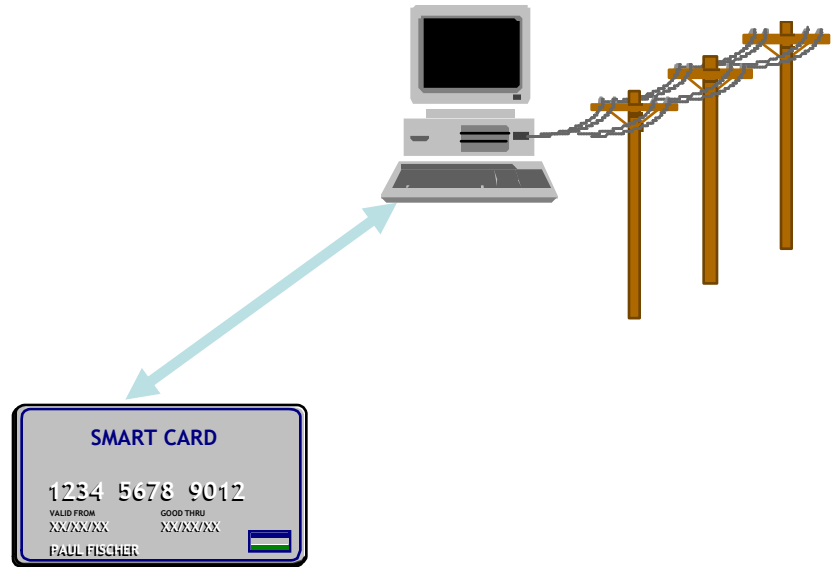
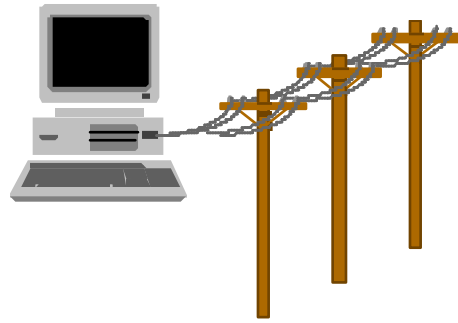
Winword document:
Ms. Meier has paid
100.000,- € to Mr. Schulz.
Schulz




Mrs. Meier

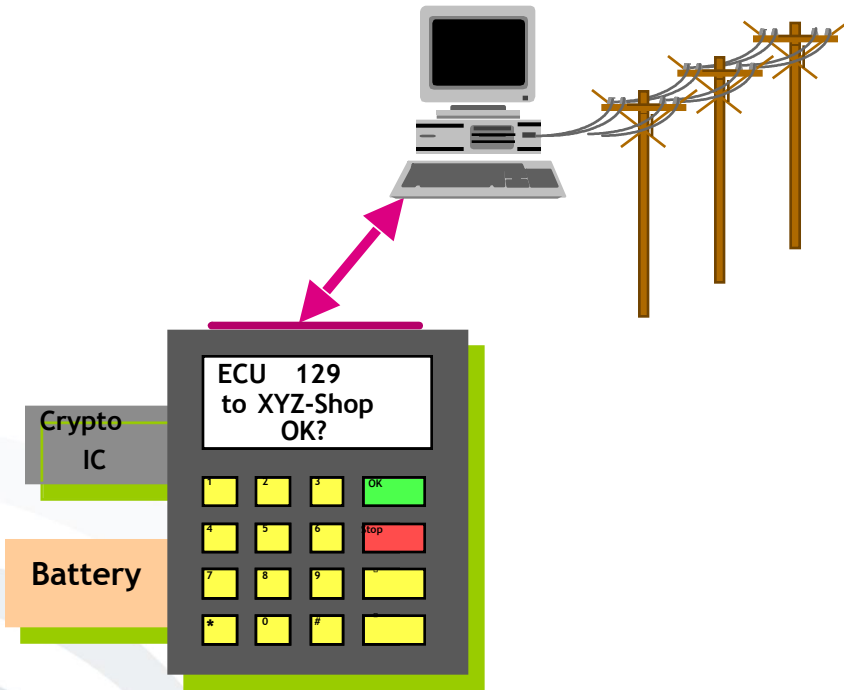
Example: display of data (§ 17(2))

- Explicit indication before a signature is being created
- Perceptibility which data the signature refers to
- Accordance of displayed data and signed data (“What you see is what you sign.”)



Private key
on HD, in memory

Private key and
signature function
in chip card



Wallet with
private key and
signature function

Order

Buyer's organization, address, country
Tel./fax/email/URL
Company registration no.
VAT-No.
Buyer's name
Certificate
Seller's organization, address, country
Seller's name
Date
Buyer's reference number
Content description
Seller's article number
Buyer's article number
Number of items
Unit of item
Item price
Tax
Freight and delivery
Total
Currency
Shipping address
Comments
Appended files
Applicable Law
Agreed means of payment
Payment agreed by
Buyer's signature

Split User Interface

← All fields on normal screen

Essential fields on secure hardware

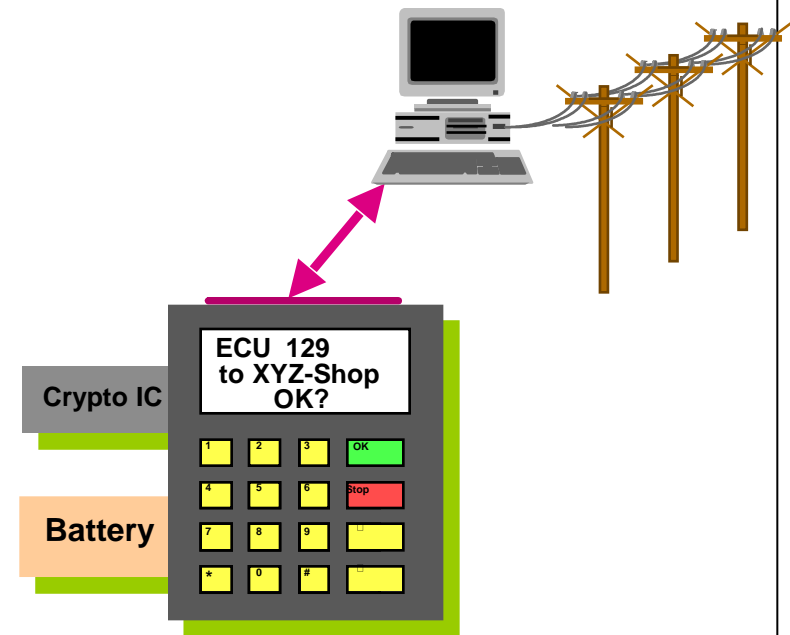


Order

Buyer
Certificate
Date
Description
Total
Currency
Signature

A popular vision: Security Assistants

- Storing personal data
 - Addresses, calendars
 - Money, keys
 - Preferences ...
- Performs sensitive processes
 - Decoding of confidential messages
 - Signature creation
- Assists negotiations
 - Documents which are accepted by other parties
 - Methods of payment
 - Reachability



- Usability
 - Portability
 - Good visibility of important information (“new network“)
 - Adequate representation of the functionality
- Protection from
 - Unauthorized access to stored data
 - Manipulation of the functionality (e.g. “Trojan Horses”)
 - Denial-of-Service attacks
- Trust (of non-experts)
 - Does the equipment do what it shall do?
 - How (much) can I trust it?

- Personal digital assistants
- Mobile phones
- Watches
- Pens
- Chip cards
- ...



- Introduction and Motivation – Security Issues
- Security of Current Mobile Platforms
- Standardisation Activities for Trusted Mobile Platforms
- (Mobile) Equipment Identifier
- Mobile Market Players and their Interests
- Usage Scenarios for Trusted Mobile Platforms
- Matching Usage Scenarios and Players
- Conclusion and Outlook

Once upon a time ...

- Closed platforms
- No additional software could be installed.
- Limited functionality



- Open platforms
- Lots of software can be installed:
 - For different purposes
 - From different vendors
- Communication with different protocols possible:
 - GSM/GPRS, UMTS
 - Bluetooth, Infrared, WLAN
- Private and confidential data can and will be stored on the mobile device.
- Camera is (in many cases) included.



[Source: HTC]

- Risks of Malware
 - Viruses, Worms, Dialler, Trojan Horses, etc.
- Passwords can (and will most likely) be deactivated.
- External storage media enables potential attackers to steal private information.
- Different communication protocols can be used to attack device or steal data.
- Camera also introduces new risks.
 - Stealing paper based confidential information
 - Invasion of personal privacy



- Trend from open platforms to open and trusted platforms
- Risks coming with the openness
- Trusted Computing for mobile platforms promises open and secure systems.
- Considered important in industry
- Many initiatives, approaches and players in the mobile communication industry

- Introduction and Motivation – Security Issues
- Security of Current Mobile Platforms
- Standardisation Activities for Trusted Mobile Platforms
- (Mobile) Equipment Identifier
- Mobile Market Players and their Interests
- Usage Scenarios for Trusted Mobile Platforms
- Matching Usage Scenarios and Players
- Conclusion and Outlook

Organization/ Project	Participants	Goals	Results
Mobile Phone Work Group of the TCG (since 2005)	Nokia and a “large number of wireless vendors, component manufacturers and mobile service or content providers”	Adaptation of TCG specifications to mobile device requirements	Reference Architecture and trusted Module Specification
Trusted Mobile Platform project (2003/2004)	Intel, IBM, NTT DoCoMo	Architecture definition of a trusted execution environment at different trust levels	Hardware and Software Architecture Description, Protocol Specification
GSM Association / Mobile Application Security	Mobile Operators (Vodafone, Orange, T-Mobile, France Telecom)	Definition and promotion of a Mobile Application Security Framework for open operation system platforms	Application Security Terminal Requirements based on domain model and terminal security policies, Application Certification Program
OMTP Group (till 2010) Application Security Project Trusted Environment Project	Mobile Operators, Equipment Manufacturers, Service Providers	Recommendation for open mobile platforms establishing an open framework for mobile device manufacturers and associated software and hardware suppliers Development of the Mobile Application Security Framework Requirement definition for hardware-based security functions	Application Security Framework
Security Working Group of the Open Mobile Alliance (OMA)	Mobile Operators, Equipment Manufacturers, Service Providers	Specification of the operation of security mechanisms, features and services for mobile clients, servers and related entities	Specifications of Wireless Transport Layer Security, Wireless Identity Module, Wireless Public Key Infrastructure, Smartcard Web Server, and other requirements for application layer and transport layer security



- Consortium of (in 2010 approximately 100) companies
- Initiative founded in 2003 as successor to the Trusted Computing Platform Alliance (TCPA)
- Led by AMD, Fujitsu, HP, IBM, Infineon, Intel, Lenovo, Microsoft and Wave
- Goal: implement trusted computing
- www.trustedcomputinggroup.org

- About:

“The Trusted Computing Group (TCG) is a not-for-profit organization formed to develop, define, and promote open standards for hardware-enabled trusted computing and security technologies, including hardware building blocks and software interfaces, across multiple platforms, peripherals, and devices.

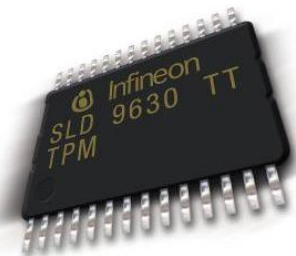
TCG specifications will enable more secure computing environments without compromising functional integrity, privacy, or individual rights.

The primary goal is to help users protect their information assets (data, passwords, keys, etc.) from compromise due to external software attack and physical theft.”

[TCG2006]

Trusted Platform Module (TPM)

- The TPM is a chip to make computers more secure as a part of the TCG specification.
- It is like a hard coded smartcard with the big difference that it is not bound to a concrete user, but to a system (e.g. a PC).
- ***Other usages:*** PDAs, mobile devices, and consumer electronics.
- Passive chip, can neither influence the booting process nor the operation directly
- Has a unique identifier and so serves for the identification of the system.



- Feature: User shall be able to make provable statements.
- Problem: to secure the provability, the statement has to come from the TPM. Furthermore the TPM has to prove that it is a real TPM:
 1. It has to be possible that corrupt TPMs may be barred from the process.
 2. For privacy reasons a TPM should not have a recognisable identity.
- Solution via:
 - Trusted third parties
 - Zero-knowledge proof

DOMAINS	Certification Process	Description	Access Rights (Promptings at execution)
Untrusted	None	LOW Security → High Risk ✓ Helps Developers	<ul style="list-style-type: none"> - No access to very sensitive functionalities - Regular user promptings for all other sensitive functional groups
Trusted	3rd party certification e.g. UTI/Java Verified	MEDIUM Security → Limited Risk through certification programmes	<ul style="list-style-type: none"> - Access to most sensitive functionalities - User prompting with options to switch off
Operator/ High Trust	e.g. operator managed certification programme	HIGH Security → Very low Risk through enhanced cert prog, contractual relationship with developer	<ul style="list-style-type: none"> - Access to all functionalities - No user promptings
Manufacturer	OEM	HIGH Security → Very low Risk through enhanced cert prog, contractual relationship with developer	<ul style="list-style-type: none"> - Access to all functionalities - No user promptings

- Introduction and Motivation – Security Issues
- Security of Current Mobile Platforms
- Standardisation Activities for Trusted Mobile Platforms
- (Mobile) Equipment Identifier
- Mobile Market Players and their Interests
- Usage Scenarios for Trusted Mobile Platforms
- Matching Usage Scenarios and Players
- Conclusion and Outlook

- IMEI (“international mobile equipment identity“)
- IMSI („international mobile subscriber identity“)
- Apple Unique Device Identifier (UDID)
 - Combination of 40 numbers and letters
- Google Android ID
 - Can be changed by user with factory reset
- Trusted Platform Module (TPM)

(Mobile) Equipment Identifier

- IMEI, IMSI, UDID, Android ID, TPM:
Who knows the user's identity and
interprets the user's behaviour?

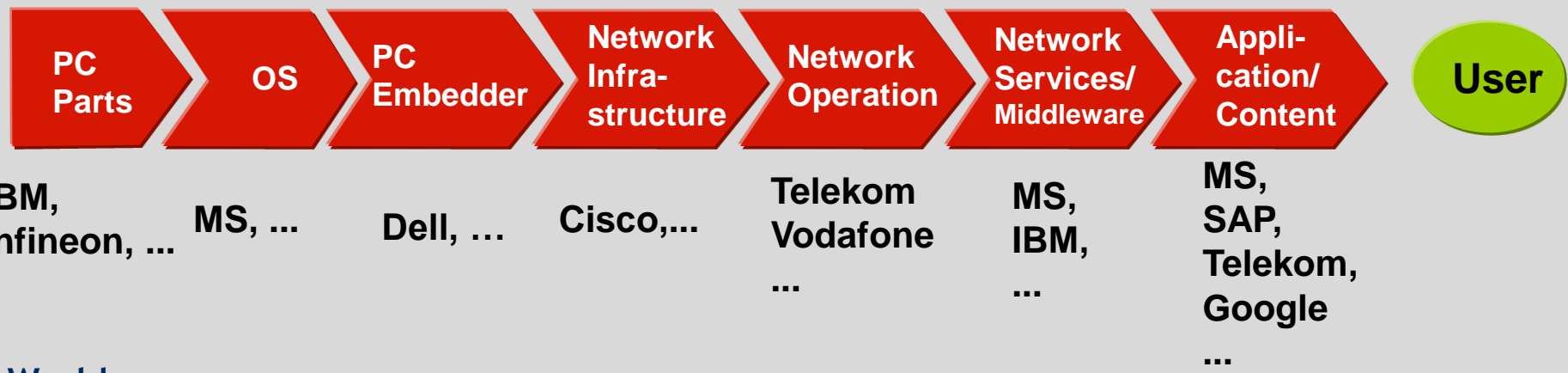
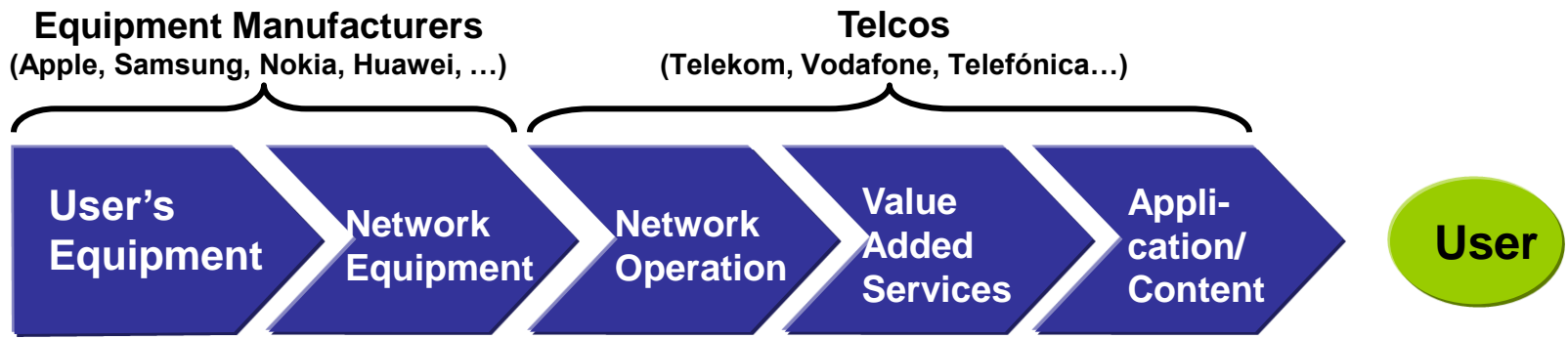


- Introduction and Motivation – Security Issues
- Security of Current Mobile Platforms
- Standardisation Activities for Trusted Mobile Platforms
- (Mobile) Equipment Identifier
- Mobile Market Players and their Interests
- Usage Scenarios for Trusted Mobile Platforms
- Matching Usage Scenarios and Players
- Conclusion and Outlook

- Mobile equipment manufacturers
- (Mobile) Telecom Operators
- MVNO's
- Content providers
- Application service providers
- Private customers
- Corporate buyers
- Corporate users

- In the past main manufacturers of mobile equipment were mobile phone manufacturers (e.g. Nokia, Motorola), producing both hardware and the software.
- Meanwhile the value chain for mobile equipment is more complex: Parts may come from third parties, **mobile equipment manufacturers:**
 - E.g. hardware from Infineon, HTC, Samsung.
 - E.g. software from Microsoft, Google.
- The more they are perceived as the providers of the respective product, the more risks of mobile platforms are affecting the equipment manufacturers.

GSM World



IT World (Based on: SAP)

- Functions of mobile operators that relate to trusted computing:
 - operate networks,
 - provide services,
 - maintain direct customer relationships,
 - provide mobile devices to customers (often by subsidising their costs).
- Most powerful players in the mobile market



Telefonica



中国移动通信
CHINA MOBILE

Definition:

A **mobile virtual network operator (MVNO)** is a company that does not own a licensed frequency spectrum and wireless infrastructure, but resells wireless services under their own brand name, using the network of another mobile network operator.

Explanation:

- An MVNO's roles and relationship to the mobile phone operator vary by market.
- In general, an MVNO is an entity or company that works independently of the operator and can set its own tariff structures.



Based on [Wikipedia2010]



JETA
digital

- Are producing and/or distributing digital content (e.g. games, ring tones, music, movies, TV (DVB-H))
- Interest in:
Securing their property rights on the provided content ➔ Digital Rights Management (DRM)

The logo for BMG, featuring the letters "BMG" in a bold, black, sans-serif font with a red triangle above the letter "M".

BMG



- Providing mobile application services (e.g. LBS, mobile banking, mobile payment services, news services)
- Interest in:
Ensuring that the devices used by customers for authenticating transactions are not compromised.



clever-tanken.de



- Usually not concerned about security of their mobile device.
 - Interest in:
Functionality, usability and design properties of their mobile device
- ➔ Security failures are perceived as a mistake made by the manufacturer/
mobile operator



- IT managers, technical staff and system administrators
- Interest in:
Concerned about mobile devices and mobile access causing security holes in their enterprise system.



➔ Most security-conscious customers



- Are using mobile infrastructures predominantly for business needs.
- Interest in:
Like private users, but with usage restrictions imposed by employers for security purposes

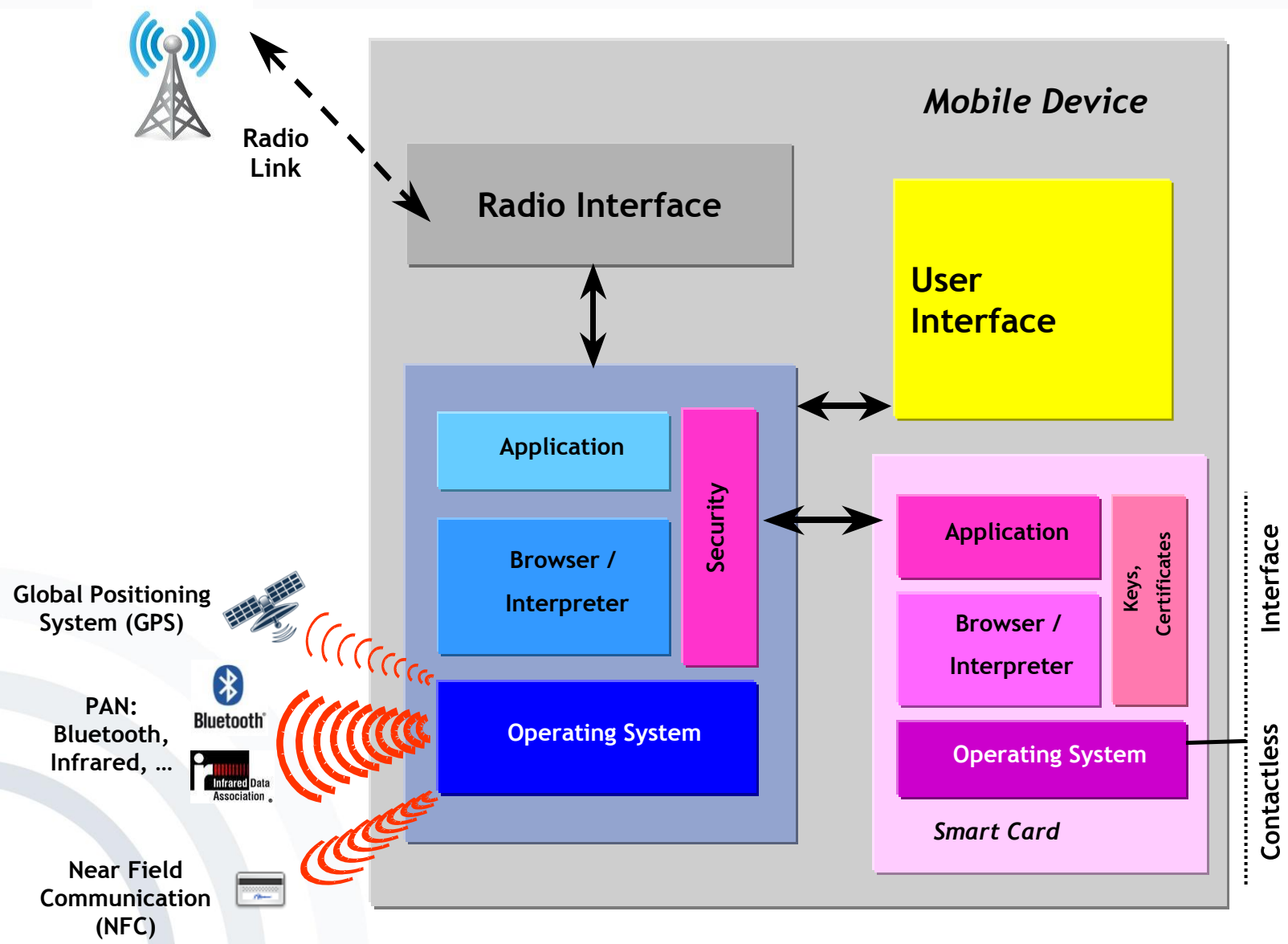
- Introduction and Motivation – Security Issues
- Security of Current Mobile Platforms
- Standardisation Activities for Trusted Mobile Platforms
- (Mobile) Equipment Identifier
- Mobile Market Players and their Interests
- Usage Scenarios for Trusted Mobile Platforms
- Matching Usage Scenarios and Players
- Conclusion and Outlook

- Secure OS
- Digital Rights Management (DRM)
- Device misuse prevention
- Storage of additional credentials on the mobile device
- Secure corporate network interaction

- Trusted mobile platforms can help to protect the operating system (system software and applications) from manipulations.
- Integrity of the system can be observed by user or remote party (e.g. features like secure booting)

OS - Functional Architecture

[Based on Posegga2001]



- Mobile device could provide a facility that can be integrated within a DRM infrastructure, e.g.
 - device authentication,
 - cryptographic functions,
 - certificate management support.



- Most mobile devices provide device access protection via PIN or password input.
- Many mobile users don't use this functionality (inconvenience).
- Mobile device could provide protection mechanisms such as
 - strong user authorisation,
 - data access management,
 - data encryption.



mobile business Storage of additional Credentials on the Mobile Device

- SIM card is used as secure storage for mobile operator credentials.
- Idea: Moving credentials on the device, if mobile devices can offer secure storage based on trusted computing (additionally storing of sensitive data on device).
- A trusted platform needs to provide
 - cryptographic functions,
 - key management support,
 - dependable user authorisation,
 - secure data access.



- Staff members can easily copy confidential information to the mobile device and carry it out of the secured perimeter.
- Trusted mobile device could facilitate secure device identification in the corporate network and provide reliable mechanisms for secure data exchange.

- Introduction and Motivation – Security Issues
- Security of Current Mobile Platforms
- Standardisation Activities for Trusted Mobile Platforms
- (Mobile) Equipment Identifier
- Mobile Market Players and their Interests
- Usage Scenarios for Trusted Mobile Platforms
- Matching Usage Scenarios and Players
- Conclusion and Outlook

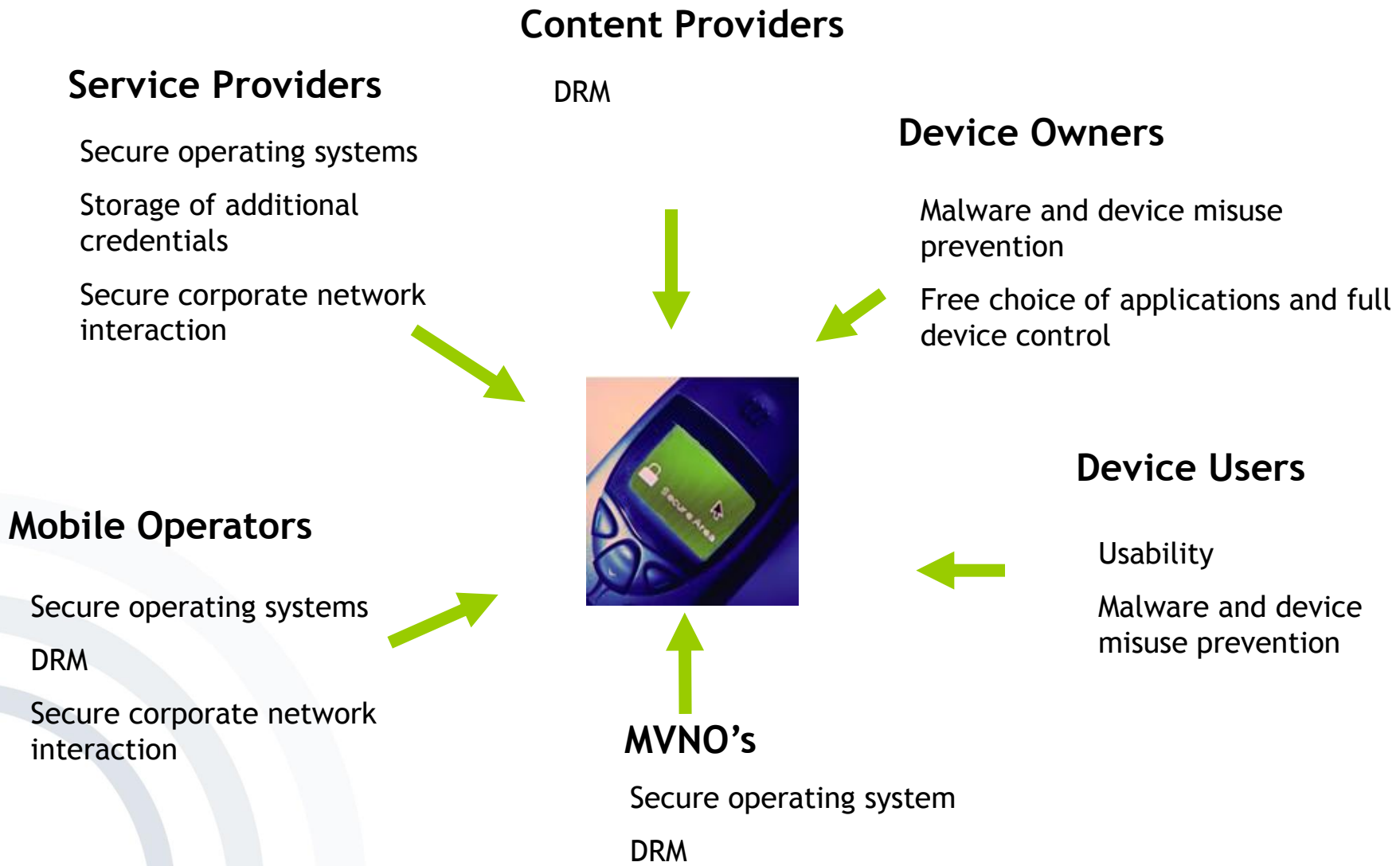
- Security options enabled by trusted platform features and the respective usage scenarios correspond to different interests of the different players within the mobile market:
 - The security of mobile platforms is valued as especially important by **equipment manufacturers, mobile operators, MVNO's and corporate buyers** (loss of money or reputation can pose significant problem for them). As most security conscious group, they have a high interest in the security of the operating system.

- For **corporate** and **private customers** high importance of reliable and trustworthy devices and malware protection.
- Mobile platform security also relevant for application providers (services dealing with sensitive or financial information)

Players and security features they are especially interested in

Usage Scenarios/ Players	Equipm. manu- facturers	Mobile opera- tors	MVNOs	Content provid- ers	Appl. service provid. ers	Private custom- ers	Corp. buyers	Corp. users
Secure operating system	++	++	++		+	+	++	+
Digital Right Management	++	+	+	++				
Device misuse prevention						+	++	++
Storage of additional credentials	+				+	+	+	
Secure corporate network interaction		+			+		++	+

[PiskRannRoss2005]



- Introduction and Motivation – Security Issues
- Security of Current Mobile Platforms
- Standardisation Activities for Trusted Mobile Platforms
- (Mobile) Equipment Identifier
- Mobile Market Players and their Interests
- Usage Scenarios for Trusted Mobile Platforms
- Matching Usage Scenarios and Players
- Conclusion and Outlook

- Mobile platforms have good chances to migrate into trusted platforms.
- Mobile market players are interested in device security enhancements.
- Big players are actively engaged in the standardisation and development process.
- Based on trustworthy platforms new mobile devices can facilitate the development of security-critical mobile commerce and mobile business application and services (e.g. mobile payment, mobile signatures).

- Missing at the moment:
 - An architecture combining the features the different parties are interested in
 - An entity to drive this architecture, e.g. the one consortium comprising all the players and interests
 - The availability of all standardisation results for public review

- [GSM2005] GSM Association (2005), Mobile Application Security, www.gsmworld.com/using/security/gsma_mas_final_summary_v1.pdf, accessed 2006-11-03.
- [MurmanRossna2005] Murmann, Tobias; Rossnagel, Heiko (2005): Sicherheitsanalyse von Betriebssystemen für Mobile Endgeräte; In: Federrath, Hannes (ed): SICHERHEIT 2005, Sicherheit - Schutz und Zuverlässigkeit: Beiträge der 2. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e.V. (GI), Lecture Notes on Informatics (LNI), S.129 - 139.
- [PiskRannRoss2005] Pisko, Evgenia; Rannenber, Kai; Rossnagel, Heiko (2005): Trusted Computing in Mobile Platforms – Players, Usage Scenarios, and Interests; In: Datenschutz und Datensicherheit (DuD) (29:9), pp. 526-530.
- [Posegga2001] Posegga (2001), WiTness.
- [TCG2006] Trusted Computing Group (2006), www.trustedcomputinggroup.org, accessed 2006-11-03.
- [Wikipedia2011] en.wikipedia.org/wiki/Mobile_virtual_network_operator, accessed 2011-09-15