

Lecture 12

Mobile Trusted Devices

Mobile Business I (WS 2022/23)

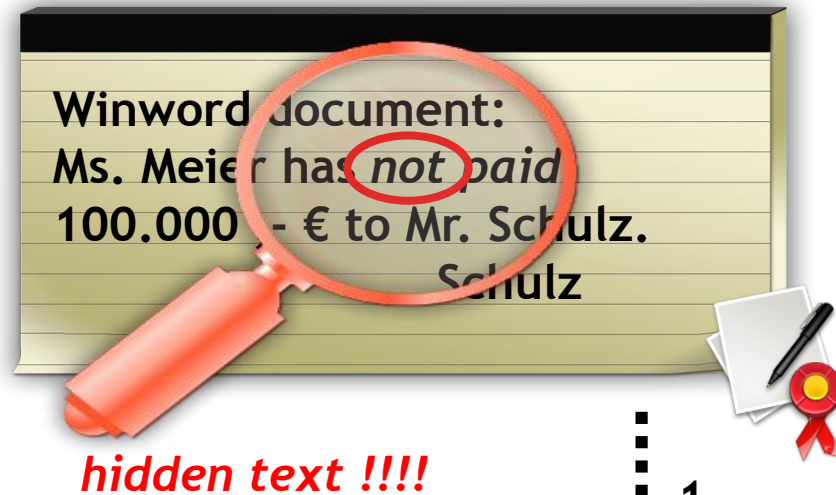
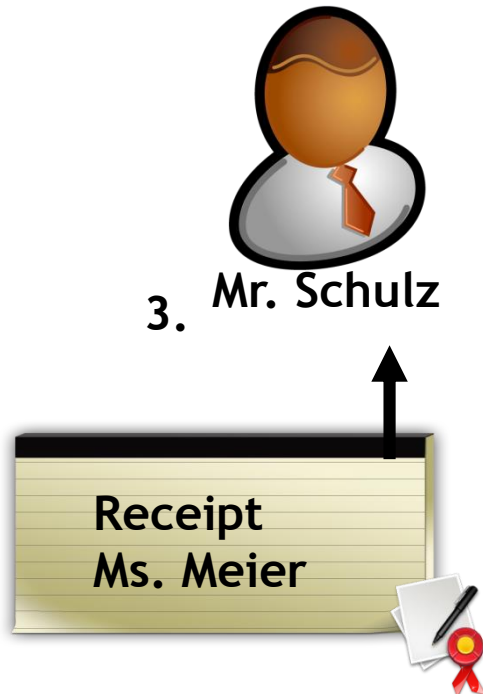
Prof. Dr. Kai Rannenber

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

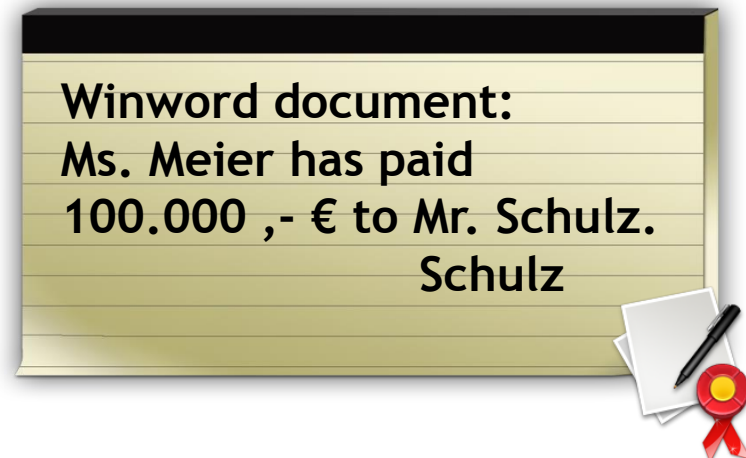


- Introduction and Motivation – Security Issues
- Security of Current Mobile Platforms
- Standardisation Activities for Trusted Mobile Platforms
- (Mobile) Equipment Identifier
- Mobile Market Players and their Interests
- Usage Scenarios for Trusted Mobile Platforms
- Matching Usage Scenarios and Players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

Presentation Problems



2.



Example: display of data (German
Signature Law - SigG § 17(2))

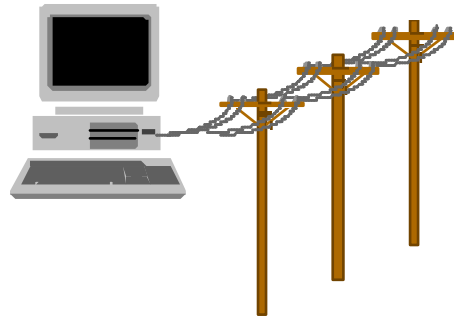
- Explicit indication before a signature is being created
- Perceptibility which data the signature refers to
- Accordance of displayed data and signed data (“What you see is what you sign.”)

[SigG 2001]

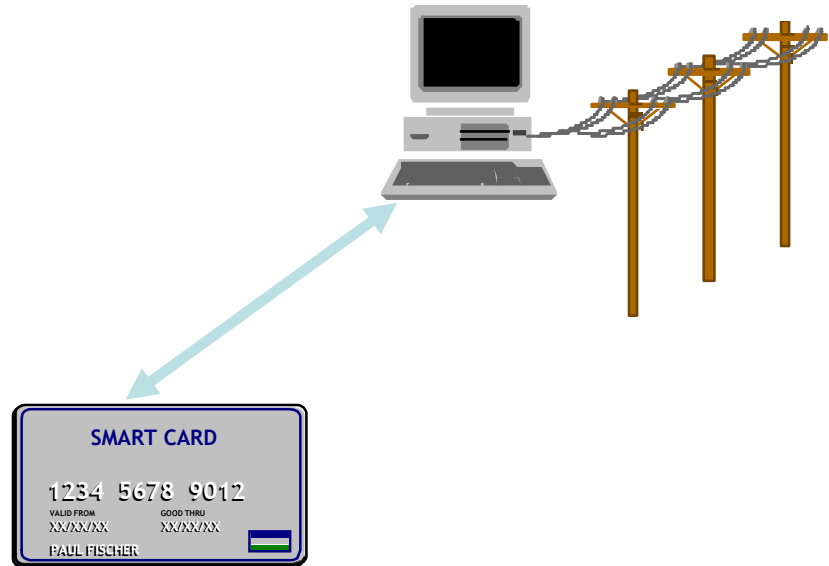
1. Qualified electronic signature creation devices shall ensure, by appropriate technical and procedural means, that at least:
 - a) the **confidentiality** of the electronic signature **creation data** used for electronic signature creation is **reasonably assured**;
 - b) the electronic signature creation data used for electronic signature creation can **practically occur only once**;
 - c) the **electronic signature creation data** used for electronic signature creation **cannot**, with **reasonable** assurance, be **derived** and the **electronic signature is reliably protected against forgery** using **currently available technology**;
 - d) the electronic signature creation data used for electronic signature creation can be reliably **protected by the legitimate signatory against use by others**.

2. Qualified electronic signature creation devices shall **not alter the data to be signed or prevent such data from being presented** to the signatory prior to signing.
3. **Generating or managing electronic signature creation data** on behalf of the signatory may only **be done by a qualified trust service provider**.
4. Without prejudice to point (d) of point 1, **qualified trust service providers** managing electronic signature creation data on behalf of the signatory may **duplicate** the electronic **signature creation data only for back-up purposes** provided the following requirements are met:
 - a) the security of the duplicated datasets must be at the same level as for the original datasets;
 - b) the number of duplicated datasets shall not exceed **the minimum needed to ensure continuity of the service**.

[eIDAS 2014]



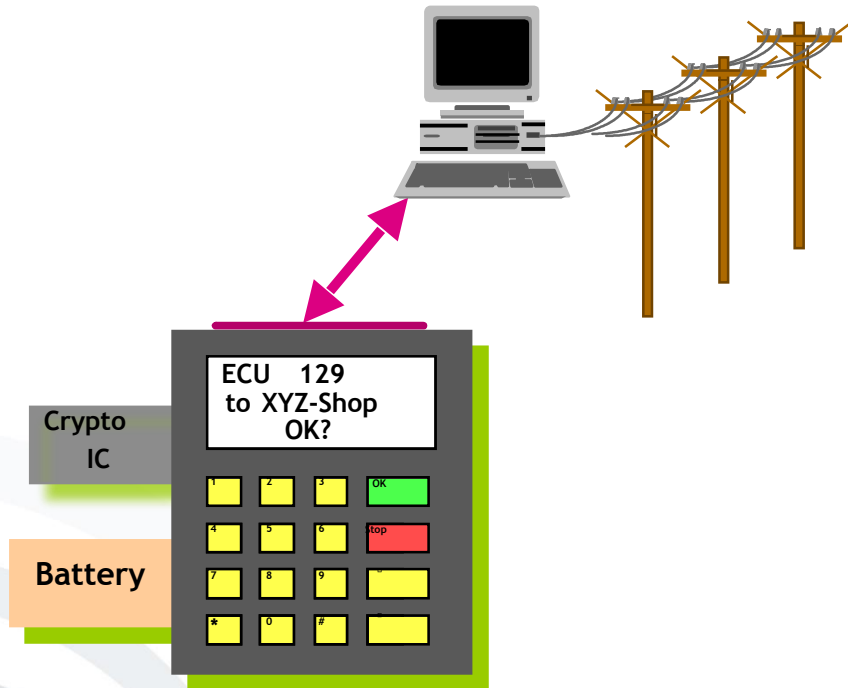
Private key
on HD, in memory



Private key and
signature function
in chip card

Secure Equipment

Avoiding Threats from Trojan Horses



**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

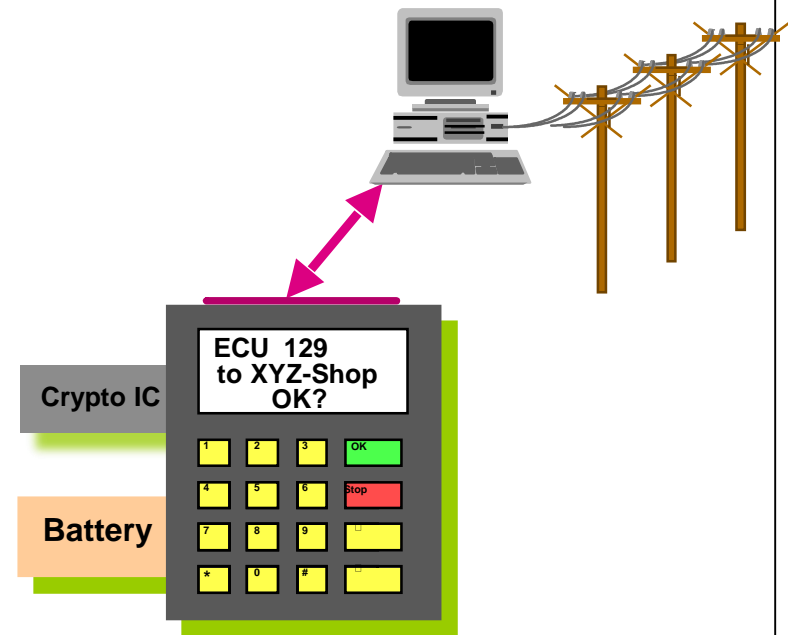


Order

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

- 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, LTE
 - Bluetooth, Infrared, WLAN, NFC
- Private and confidential data can and will be stored on the mobile device.
- Camera is (in many cases) included.



[Source: Sony]

- 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
- Powerful attackers with a clear business and operational case

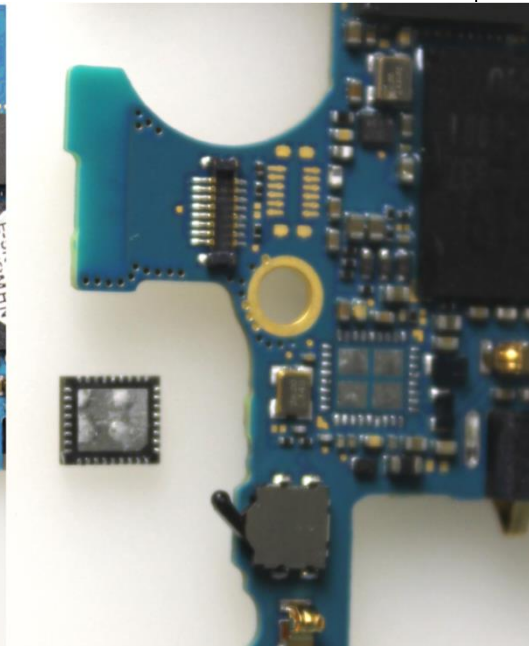
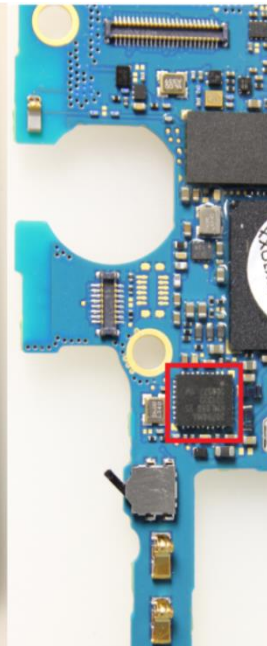


- A Secure Element (SE) is a hardware token that offers secure services, e.g. tamper-proof storage and cryptographic operations.
 - Smart card (contact or contactless)
 - SIM/UICC card
 - Smart/Secure microSD card
 - Embedded Secure Element (eSE)



Embedded Secure Element (eSE)

- Secure microcontroller
- Unremovable part of the mainboard of the device (usually a smartphone)
- Interchanging or extraction of the SE is not possible (unlike other SE form factors).
- eSEs use various types of interfaces:
 - Single Wire Protocol (SWP)
 - Dual Wire Protocol (DWP)
 - Inter-integrated circuit (I2C)
 - Universal Serial Bus (USB)
 - Proprietary interfaces



- 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
- 
- Three large, light blue curved lines in the bottom-left corner of the slide, resembling a stylized 'C' or a series of concentric arcs.

- 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

Standardisation Activities

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 (since 1995)	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 (2004 -2010) Application Security Project Trusted Environment Project	Mobile Operators, Equipment Manufacturers, Service Providers	<ul style="list-style-type: none"> • Open framework for mobile device manufacturers and associated software and hardware suppliers • Definition for hardware-based security functions 	Application Security Framework
Security Working Group of the Open Mobile Alliance (OMA) (since 2002)	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
GlobalPlatform (since 1999)	Mobile Operators, Payment Associations, Public Sector Organisations and Government Agencies	Creation and publishing of specifications for secure chip technology	GlobalPlatform Card Specification

Trusted Computing Group (TCG)



- Consortium of around 75 companies
- Initiative founded in 2003 as successor to the Trusted Computing Platform Alliance (TCPA)
- Led by AMD, Cisco, Dell, HP, Huawei, IBM, Infineon, Intel, Juniper, Lenovo, Microsoft, Google and Toyota
- Goal: implement trusted computing
- www.trustedcomputinggroup.org



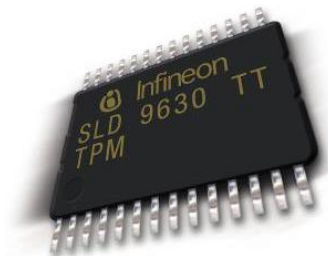
- About:

“The Trusted Computing Group (TCG) is a not-for-profit organization formed to develop, define and promote open, vendor-neutral, global industry standards, supportive of a hardware-based root of trust, for interoperable trusted computing platforms.”

[TCG2014]

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.
- Problems:
 - To secure the provability, the statement has to come from the TPM.
 - 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

Mobile Application Domains according to GSMA

DOMAINS	Certification Process	Description	Access Rights (Promptings at execution)
Untrusted	None	LOW Security → High Risk ✓ Helps Developers	- 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	- 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	- Access to all functionalities - No user promptings
Manufacturer	OEM	HIGH Security → Very low Risk through enhanced cert prog, contractual relationship with developer	- 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)
 - 40-character alphanumeric code
- Google Android ID
 - Can be changed by user with factory reset
- Trusted Platform Module (TPM)
 - (Public part of the) Endorsement Key (EKpub)

- 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

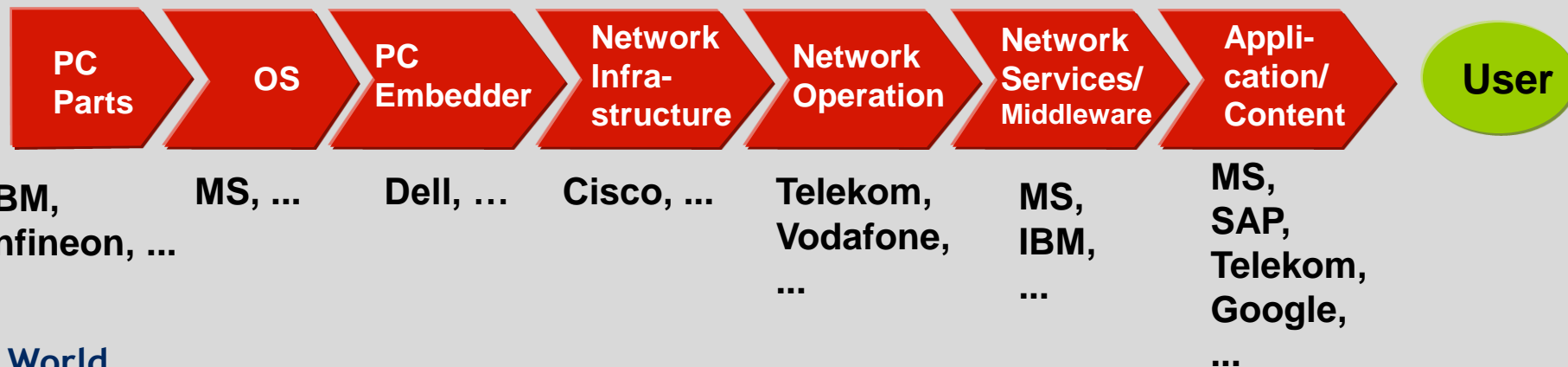
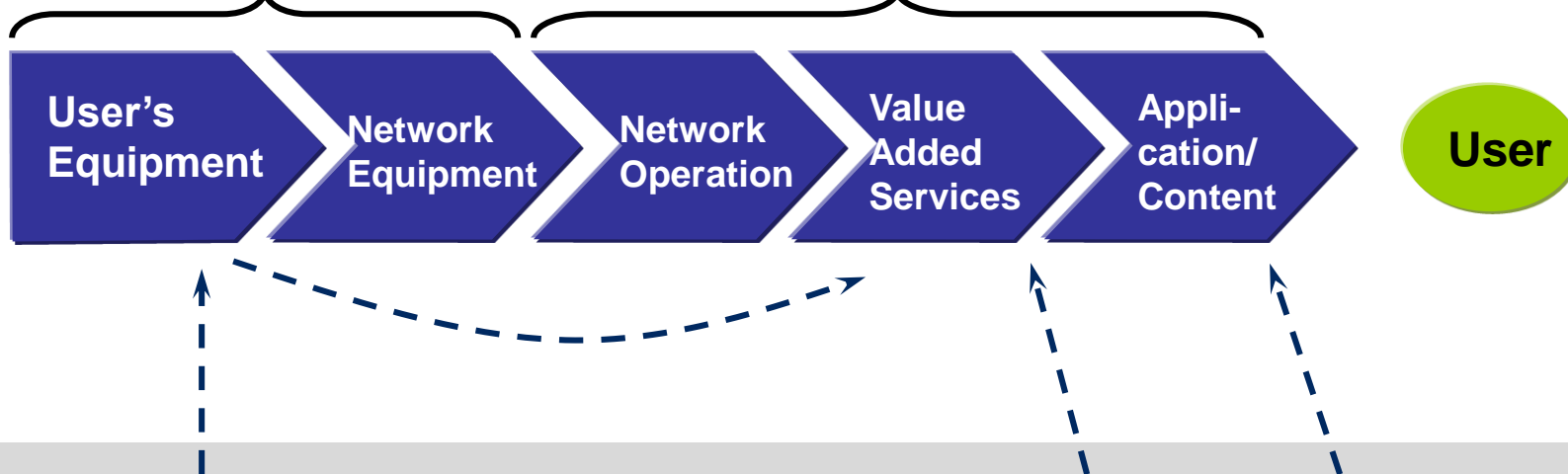
- Mobile equipment manufacturers
- (Mobile) Telecom Operators
- MVNOs
- Content providers
- Application service providers
- Private customers
- Corporate buyers
- Corporate users
- Intelligence agencies

- In the past, main manufacturers of mobile devices were mobile phone manufacturers (e.g. Nokia, Motorola), producing both hardware and the software.
- Meanwhile the value chain for mobile devices has become more complex: Significant elements may come from third parties, e.g.
 - hardware (designs) from ARM, Infineon, Texas Instruments,
 - software from Google, Microsoft.
- The more a manufacturer is perceived as the provider of the respective platform, the more risks of the mobile platform are affecting them.
- Today, mobile devices are sold particularly as part of a powerful ecosystem (Google, Apple, Microsoft).

GSM World

Equipment Manufacturers
(Apple, Samsung, Microsoft/Nokia,
Lenovo, Huawei, ...)

Telcos
(Telekom, Vodafone, Telefónica...)



IT World

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



The logo for Telefonica, featuring the word 'Telefonica' in a blue script font, underlined with a blue horizontal line.



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.



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



warner | music | group



VIACOM

NBCUniversal



THE WALL STREET JOURNAL.



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



iZettle



PayPal



finanzinformatik



- 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 device manufacturer/mobile OS provider/mobile network operator.



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

➡ Most security-conscious customers

➡ Benefit from Mobile Device Management solutions (cf. Section “Usage Scenarios for Trusted Mobile Platforms”)



[Zeit2013]

- Are using mobile infrastructures predominantly for business needs.
- Like private users, but with usage restrictions imposed by employers or (mobile) OS for security purposes
 - This includes corporate users who are allowed to bring and use personally owned mobile devices (*Bring your own device - BYOD*)



- Eavesdrop (and manipulate?) globally exchanged information to gather intelligence, regardless of whether a suspicion exists or not.



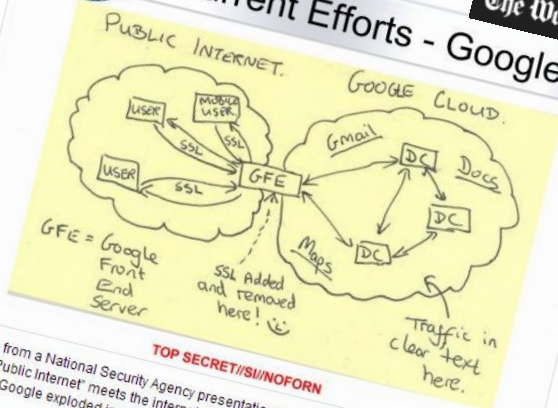
NSA tracking cellphone locations worldwide, Snowden documents show

The Washington Post

NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say

The Washington Post

Current Efforts - Google



In this slide from a National Security Agency presentation on "Google Cloud Exploitation," a sketch shows where the "Public Internet" meets the internal "Google Cloud" where user data resides. Two engineers with close ties to Google exploded in profanity when they saw the drawing.

By Barton Gellman and Ashkan Soltani, Published: October 30 E-mail the writer

The National Security Agency has secretly broken into the main communications links that connect Yahoo and Google data centers around the world, according to documents obtained from former NSA contractor Edward Snowden and interviews with knowledgeable officials.

By tapping those links, the agency has positioned itself to intercept millions of user accounts, many of which contain everything it collects from them.

Video: The National Security Agency gathers location data from around the world by tapping into the cables that connect mobile networks globally and that serve U.S. cellphones as well as foreign ones.

By Barton Gellman and Ashkan Soltani, Published: December 4 E-mail the writer

The National Security Agency is gathering nearly 5 billion records a day on the whereabouts of cellphones around the world, according to top-secret documents and interviews with U.S. intelligence officials, enabling the agency to track the movements of individuals — and map their relationships — in ways that would have been previously unimaginable.

The records feed a vast database that stores information about the locations of at least hundreds of millions of devices, according to the officials and the documents, which were provided by former NSA contractor Edward Snowden. New projects created to analyze that data have provided the intelligence community with what amounts to a mass surveillance tool.

- 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

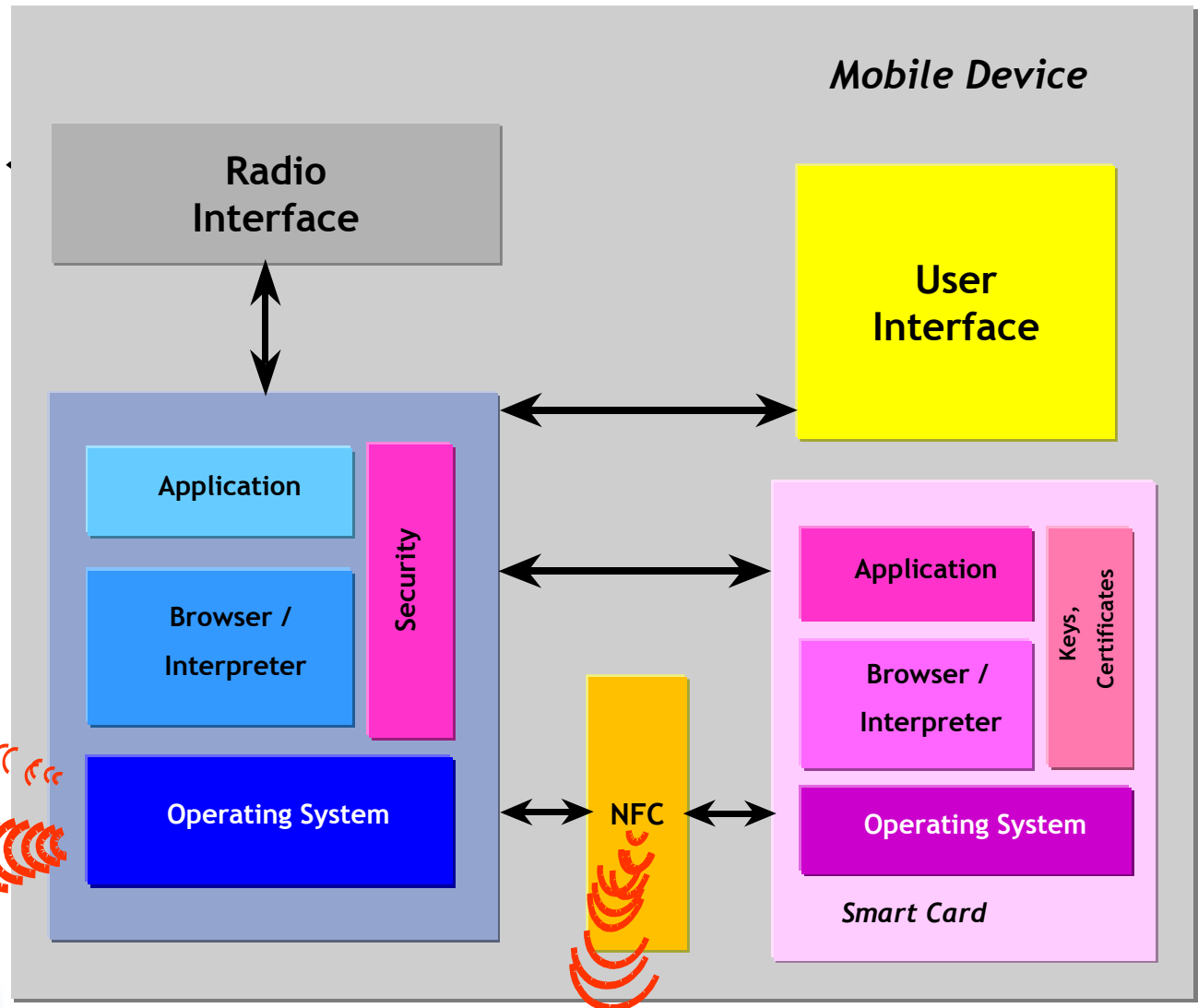
- Secure OS
- Mobile Device Management (MDM)
- Secure corporate network interaction
- Digital Rights Management (DRM)
- Device misuse prevention
- Storage of additional credentials on the mobile device
- Mobile Wallets

- 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, Mobile Device Management)


OS – Functional Architecture



Radio
Link



- Software to secure, monitor, manage and support mobile devices
- Over-the-air distribution of
 - Applications
 - Data
 - Configuration settings
- ➔ Higher security level, lower cost and fewer downtimes

- 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.
- 
- A series of light blue concentric curved lines in the bottom-left corner of the slide, resembling a stylized signal or wave.

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

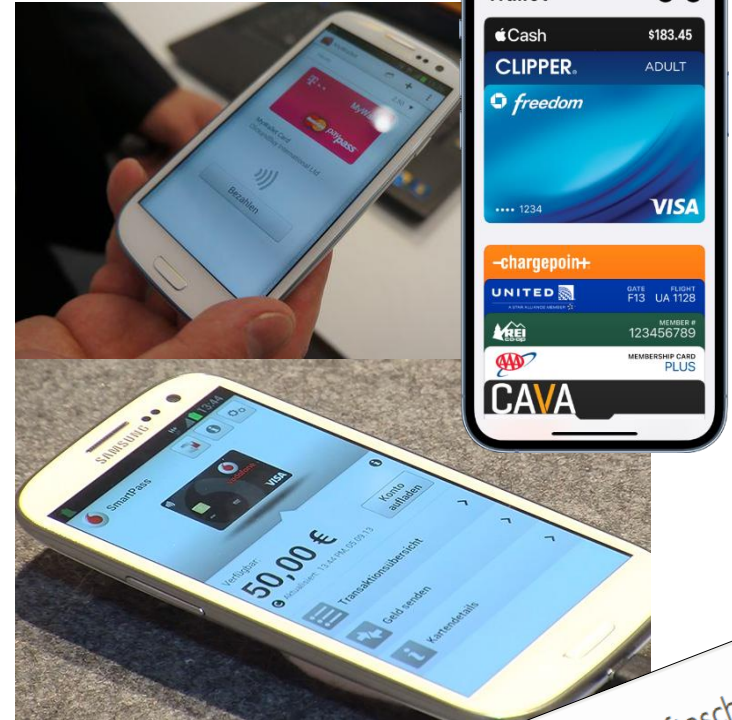
- Most mobile devices provide device access protection via PIN or password input.
- Many mobile users don't use this functionality (inconvenience).
- Mobile device could provide protection mechanisms such as
 - strong user authentication,
 - strong user authorisation,
 - data access management,
 - data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



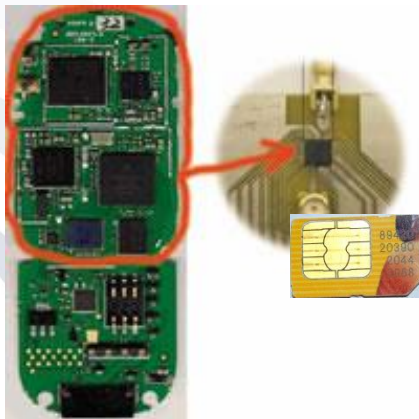
- SIM card is used as secure storage for mobile operator credentials.
- Idea: Storing credentials on the device, if mobile devices can offer secure storage based on trusted computing.
- A trusted platform needs to provide
 - cryptographic functions,
 - key management support,
 - dependable user authorisation,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



- (NFC) Mobile Wallets
 - contain virtual payment cards and other cards, e.g. customer loyalty cards
 - use the UICC/SIM-based Secure Element (SE)
 - Licensed by Deutsche Telekom, Vodafone, Telefónica and E-Plus independently in 2014.
- Mobile Wallet application “runs” in non-secure memory of the mobile device whereas a UICC payment application runs within the SE.



<https://support.apple.com/de-de/guide/iphone/iphone05b5539/ios>



Telefónica O2 to begin beta testing NFC payments in Germany

By Sarah Clark | January 21st, 2013

"Soon, children will only know from history books what a wallet and hard cash are," says René Schuster, CEO of Telefónica Germany, as the carrier prepares to make payments available to customers from...

E-Plus Mobile Wallet – das Smartphone als Brieftasche

Die Mobile Wallet ermöglicht mehr als Zahlungen

4. November 2013 Unternehmen

Manuela Mirzadeh
Kommentar schreiben

Mit der „Mobile Wallet“-App macht die E-Plus Gruppe das Smartphone zur digitalen Brieftasche. Die Lösung wird ab Frühjahr 2014 bei den Marken und Partnern des Unternehmens an den Start gehen. Im Bus das Ticket vorzeigen, Rabattaktionen im Kaufhaus nutzen, in das Studio einchecken, beim Einkauf im Drogeriemarkt zahlen und gleichzeitig Bonuspunkte sammeln – zukünftig ist das buchstäblich alles aus einer Hand möglich. Mit der App können Kunden- und Bank-Karten, die das Portmonee sprengen, in der digitalen Brieftasche verwahrt werden.

Two (draft) regulations
“Water-proofing” and “drilling holes”
at the same time ?

Digital wallet regulation (eIDAS 2.0)

- Establishing the concept of a secure digital wallet, e.g. based on personal computers like smartphones
- “The user shall be in full control of the European Digital Identity Wallet” (Art. 1 (7) inserting Art. 6a (7) into eIDAS 1.0)
- Only full control by users can create the necessary trust by users.
- [EC 2021, EP 2022]


“Chat Control” regulation

- Declared goal: to prevent and combat child sexual abuse.
- Measures to listen into possibly dangerous communication, e.g. by
 - **Restrictions on encryption:** Can severely limit the trustworthy protection of the identity information between e.g. cloud and device
 - **“Client side scanning” (and reporting) on user devices:** Impacts the integrity of the scanned client devices (typically smartphones)
- [EC 2022]

- 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
 - malware protection

 - Mobile platform security also relevant for application providers (services dealing with sensitive or financial information)
- 
- A series of three concentric, curved lines in a light blue color, located in the bottom-left corner of the slide.

Players and security features they are especially interested in

Usage Scenarios/ Players	Mobile Equipment manufacturers	Mobile operators	MVNOs	Content providers	Appl. Service providers	Private customers	Corp. buyers	Corp. users	Intelligence Agencies
Secure OS	++	++	++		+	+	++	+	
Digital Rights Management	+	+	+	++					
Device misuse prevention						+	++	+	
Storage of additional credentials	+				+	+	+		
Secure corporate network interaction		+			+		++	+	
Mobile Wallet	++	++				+			

Key Players' Interests

Mobile Equipment Manufacturers

Secure operating systems
DRM
Mobile Wallet
Storage of additional credentials

Content Providers

DRM

Device Owners

Malware and device misuse prevention (Corporate Buyers notably *Mobile Device Management*)
Free choice of applications and full device control

Device Users

Usability
Malware and device misuse prevention



MVNO's

Secure operating system
DRM

Mobile Operators

Secure operating systems
DRM
Mobile Wallet
Secure corporate network interaction

Application Service Providers

Secure operating systems
Storage of additional credentials
Secure corporate network interaction

- 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 had good chances to migrate into trusted platforms.
- All mobile market players are interested in device security enhancements.
- Major players are actively engaged in the standardisation and development process.
- Based on trustworthy platforms, mobile devices could facilitate the development of security-critical mobile commerce and mobile business applications 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
- Challenges:
 - Usable privacy and security configurations for users, e.g. Privacy-by-design;
 - Competing legislation trying to enable external access to devices that would need to be secure.

- [EC 2021] European Commission: Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity, COM/2021/281 final; 2021-06-03; <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0281>
- [EC 2022] European Commission: Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down rules to prevent and combat child sexual abuse, COM/2022/209 final; 2022-05-12; <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52022PC0209>
- [eIDAS 2014] EU eIDAS regulation (2014), REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC; https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG
- [EP 2022] European Parliament: Legislative Train Schedule: Revision of the eIDAS Regulation - European Digital Identity (EUid); <https://www.europarl.europa.eu/legislative-train/spotlight-JD22/file-eid>
- [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; https://www.m-chair.de/images/documents/publications/Rannenber/DuD_Mobile_Trusted_Computing_20050814.pdf.
- [Posegga2001] Posegga (2001), WiTness.
- [Riscure2014] Marc Witteman (Riscure): Are Embedded Secure Elements more secure than traditional smart cards?, www.cartes-america.com/files/are_embedded_secure_elements_more_secure_than_traditional_smart_cards___tilburg_witteman.pdf, accessed 2014-11-04.

- [SigG 2001] Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz - SigG)* 16. Mai 2001 (BGBl. I S. 876), geändert durch Artikel 2 des Gesetzes über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften vom 16. Mai 2001 (BGBl. I S. 876)
- [TCG2014] Trusted Computing Group (2013), www.trustedcomputinggroup.org, accessed 2014-10-09.
- [WaPo2013a] NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say, http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html, accessed 2013-12-09.
- [WaPo2013b] NSA tracking cellphone locations worldwide, Snowden documents show, http://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html, accessed 2013-12-09.
- [Zeit2013] Bundesbehörden sehen Risiken beim Einsatz von Windows 8, www.zeit.de/digital/datenschutz/2013-08/trusted-computing-microsoft-windows-8-nsa, accessed 2013-12-05.