mobile business

Lecture 6

GOETHE UNIVERSITÄT FRANKFURT AM MAIN

Information & Communication Security (SS 16)

Electronic Signatures

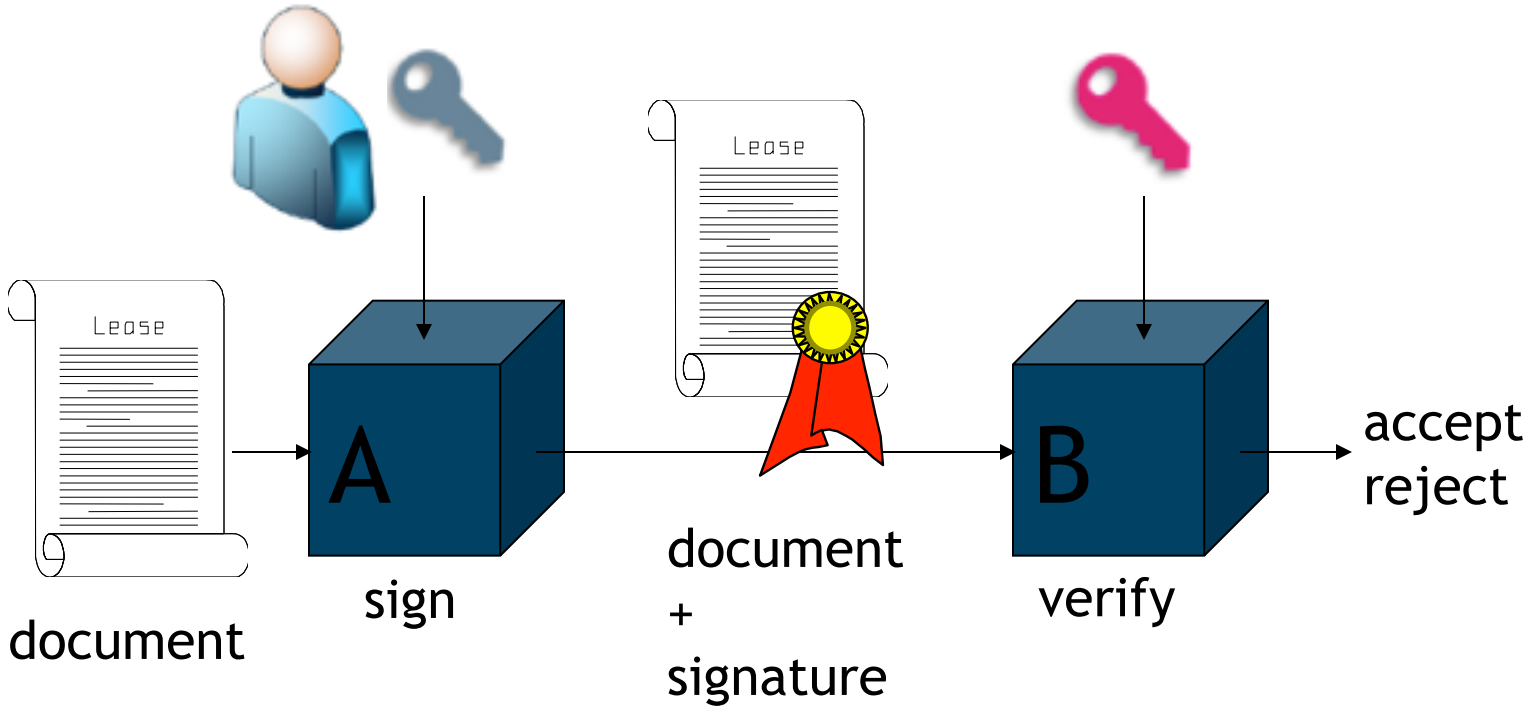
Prof. Dr. Kai Rannenberg

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

Agenda

- General Concept
- Algorithms
- Legal Framework
- Mobile Signatures
- Secure Display Components
- Personal Security Assistants

Digital Signatures



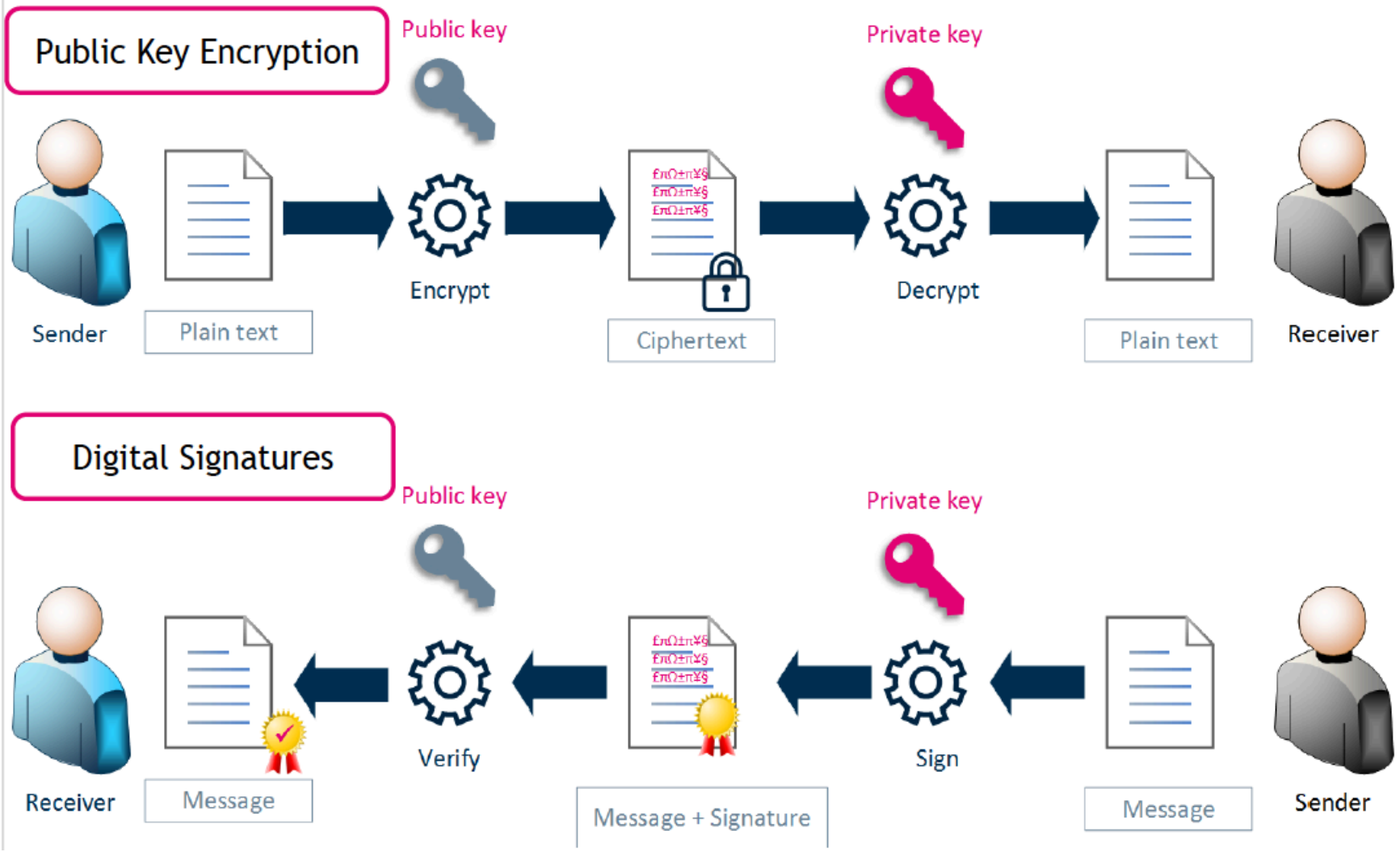
- Protect the authenticity and integrity of documents signed by A
- B has to get an authentic copy of A's public key.

Digital Signatures

Definition: A digital signature is a construct that authenticates both origin and contents of a message in a manner that is provable to a third party.

[Bishop2005]

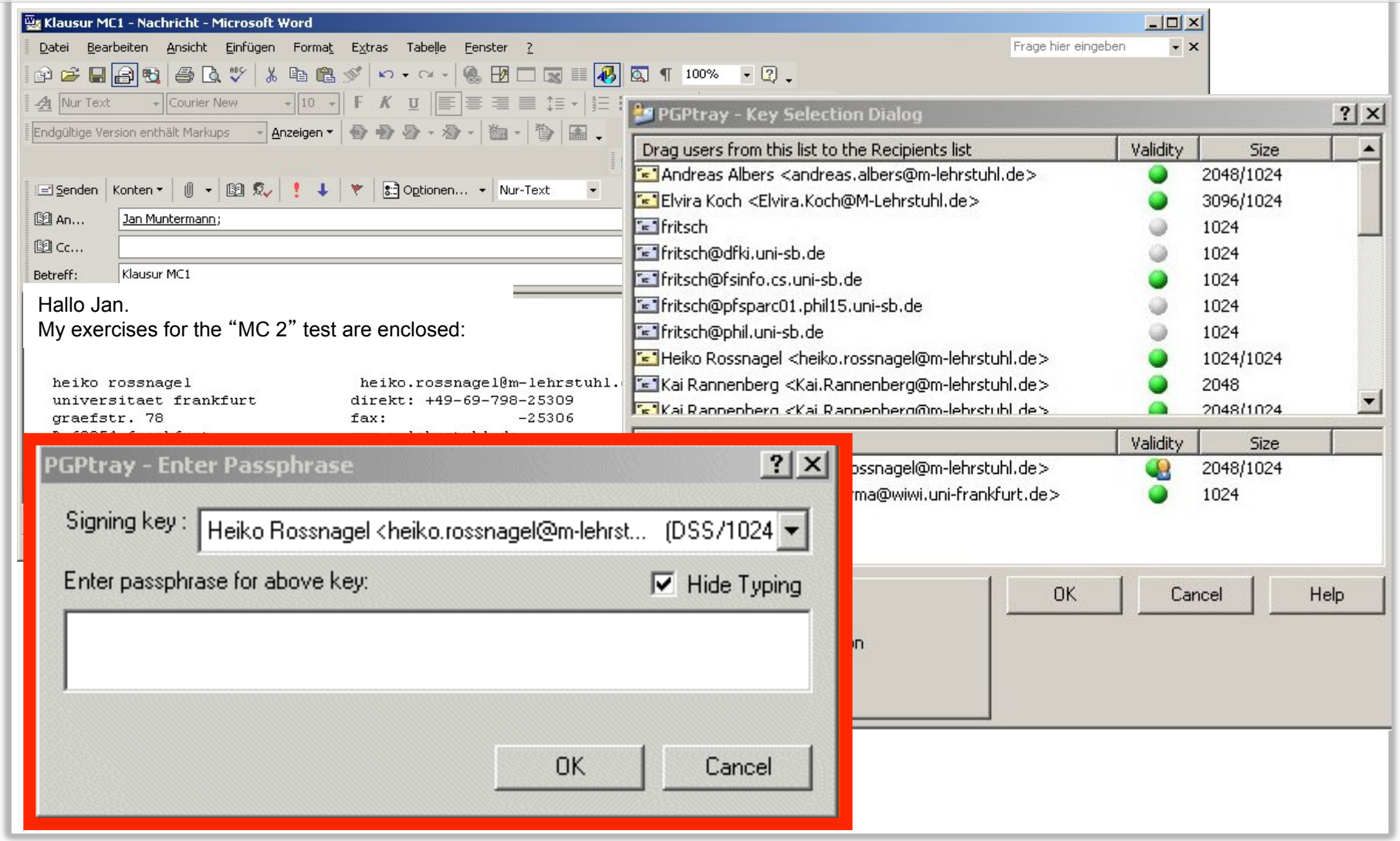
Asymmetric Signature System



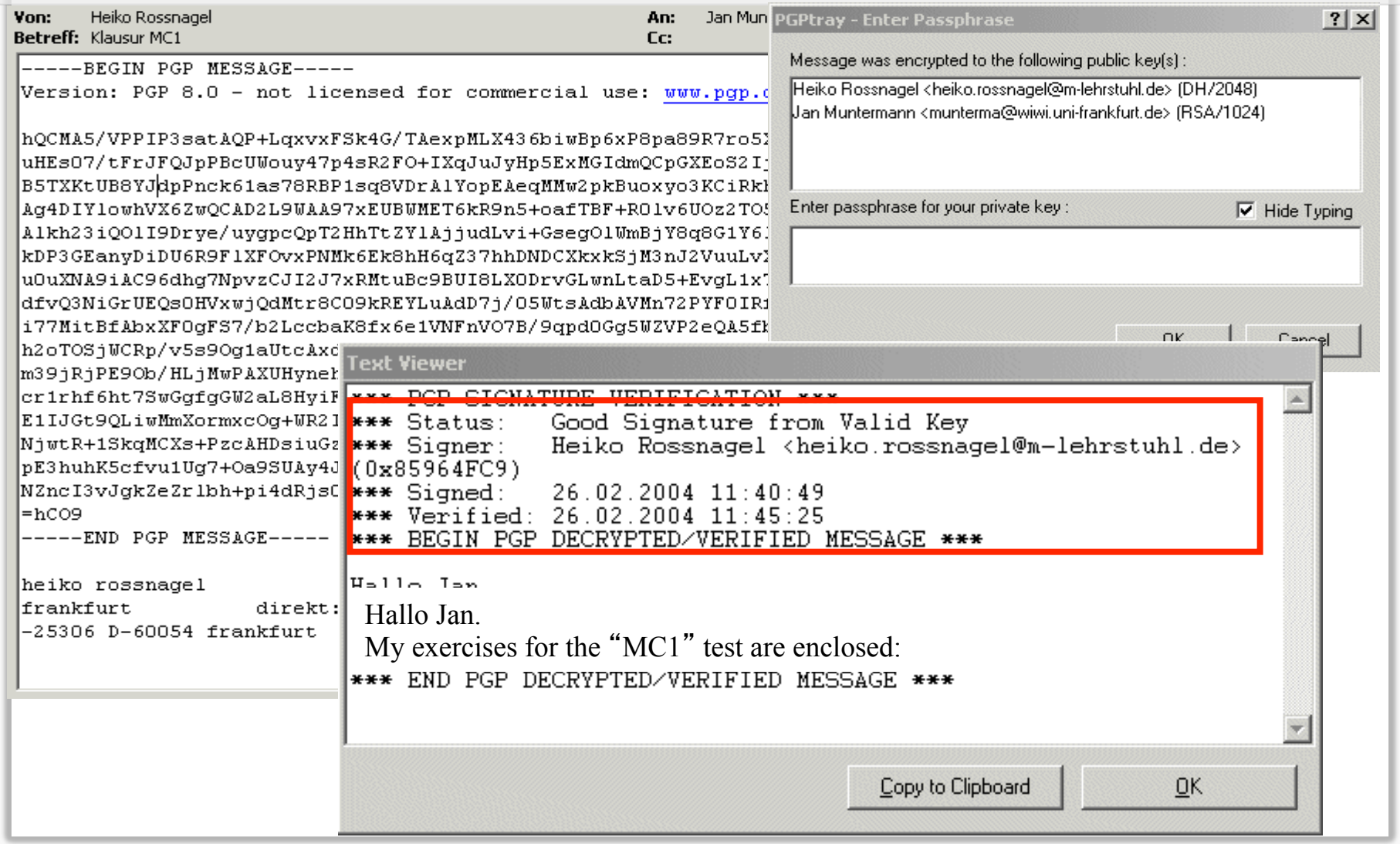
Asymmetric Signature system

Digital signatures	Public Key Encryption
The holder of the private key (sender) signs the message.	“Any one” can encrypt a message.
“Any one” can verify that a signature is valid.	Only the holder of the private key (receiver) can decrypt the message.

Example PGP: Encrypt and Sign a Message



Example PGP: Decrypt and Check a Message



mobile business

Agenda

- General Concept
- Algorithms
- Legal Framework
- Mobile Signatures
- Secure Display Components
- Personal Security Assistants

Asymmetric Signature Systems: Examples

- RSA: **R**ivest, **S**hamir, **A**dleman
  - Asymmetric encryption system which also can be used as a signature system via “inverted use”,
  - Message encrypted with the private key (= signing key) gives the signature,
  - Decoding with the public key (=testing key) has to produce the message.

[Rivest et al. 1978]

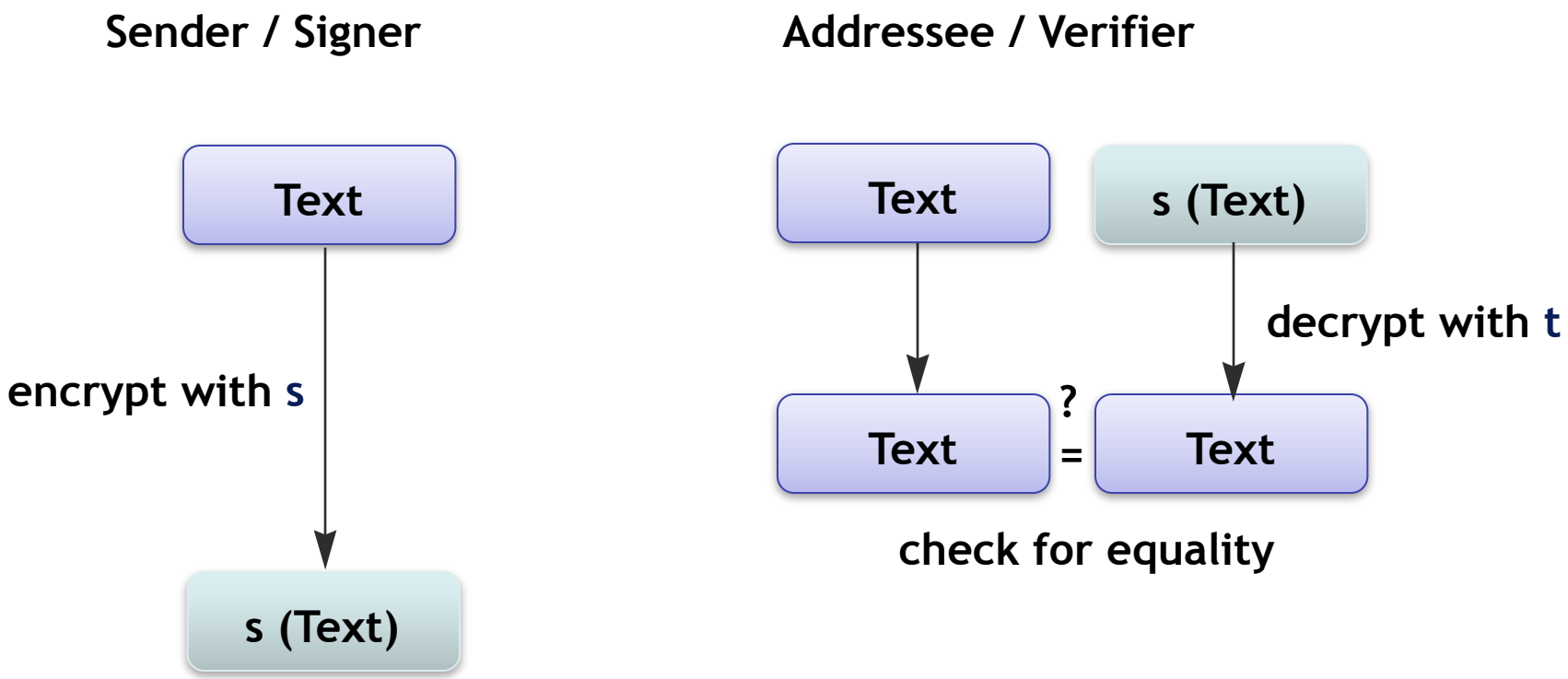
- DSA: Digital Signature Algorithm
  - Determined in the Digital Signature Standard of the NIST (USA),
  - Based on discrete logarithms (Schnorr, ElGamal),
  - Key length is set to 1024 bit.

mobile business

Public Key Algorithms

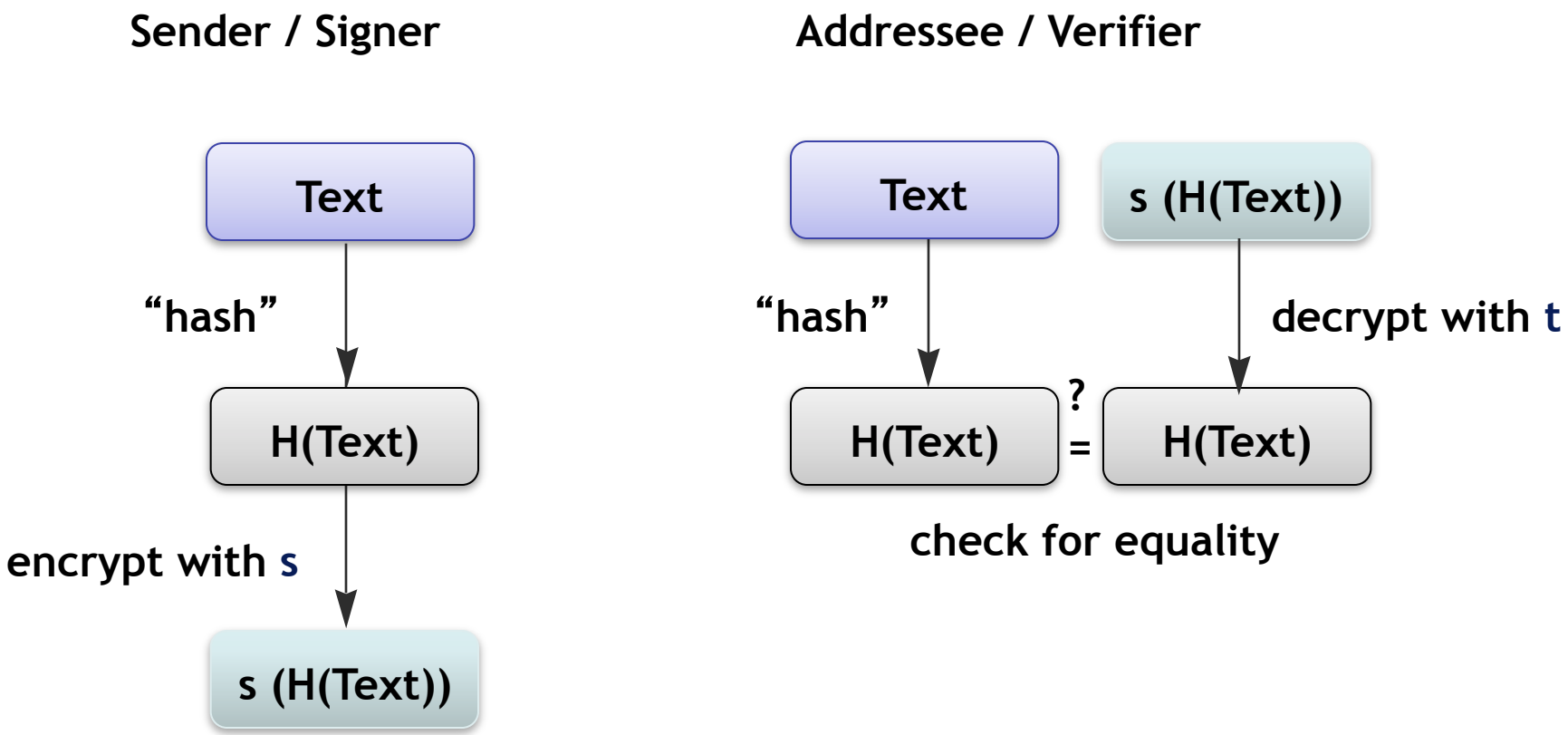
Algorithm	Algorithm family
RSA	Integer factorization
Digital Signature Algorithm (DSA)	Discrete logarithm
Elliptic Curve Digital Signature Algorithm (ECDSA)	Elliptic curves

Asymmetric Signature System (Simplified Example RSA)



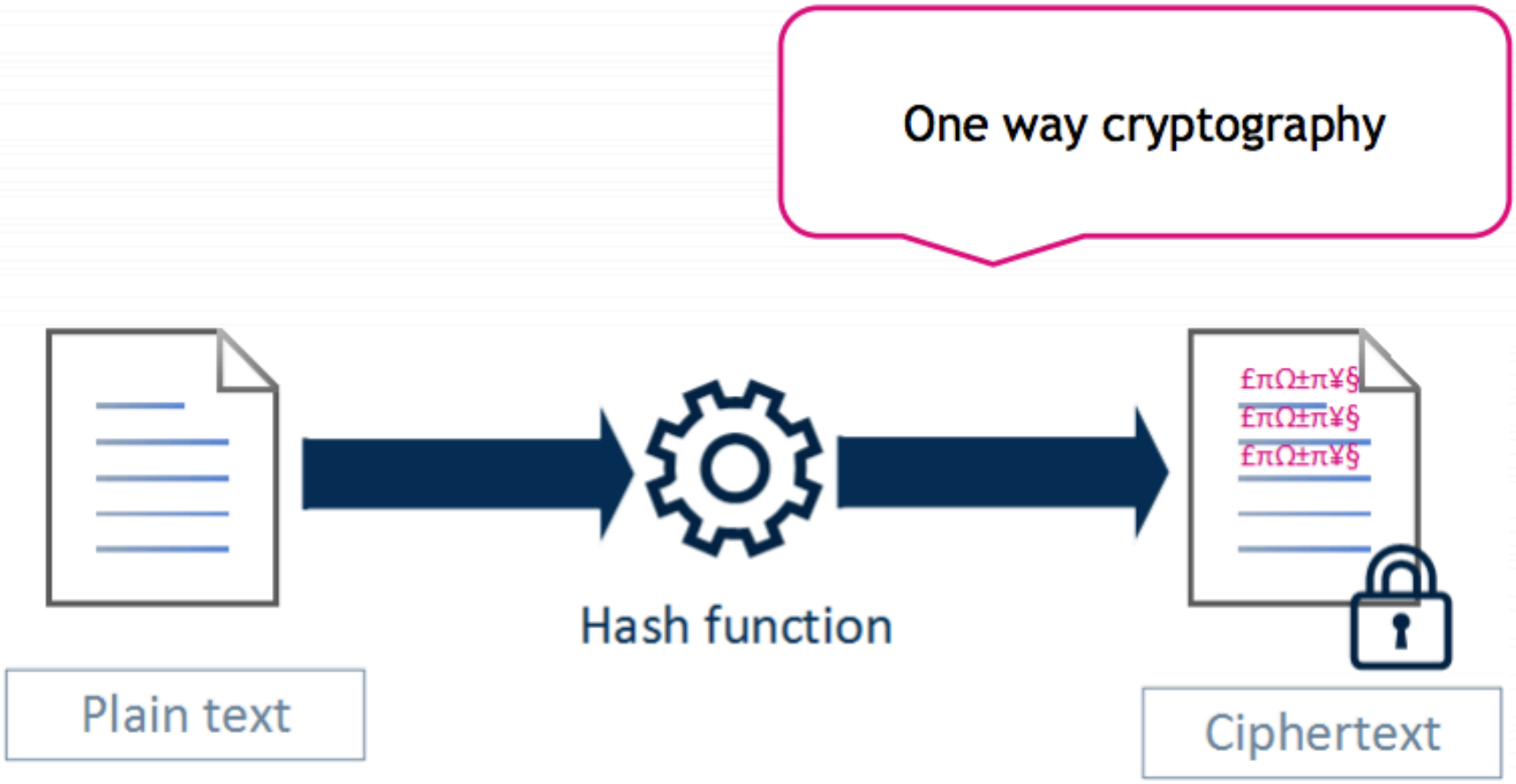
- Signing key s only with the sender, test key t public
- Example is often mistakenly generalized.

Asymmetric Signature System (Example RSA)

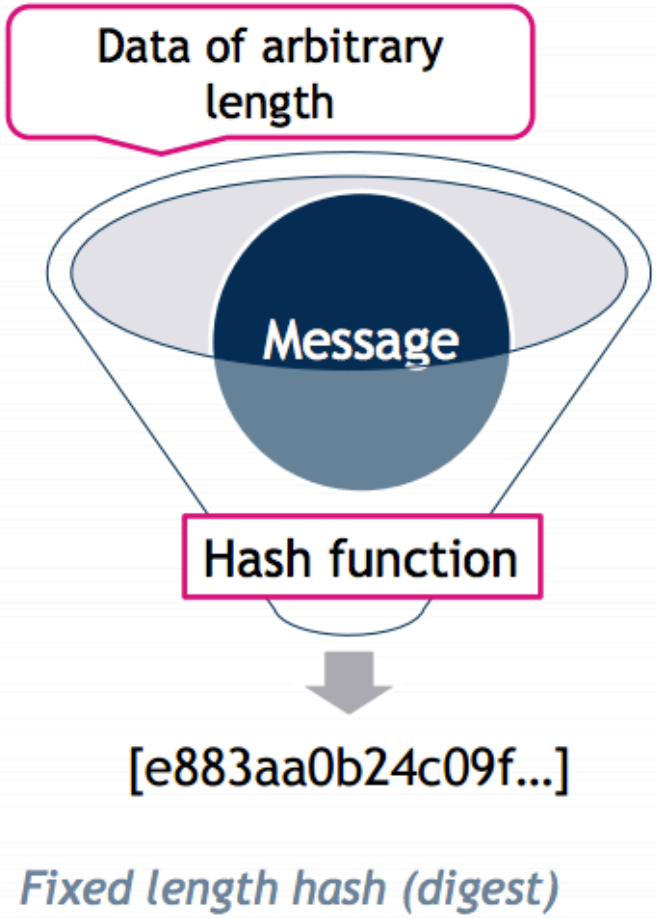


- Signing key s only with the sender, test key t public
- Example is often mistakenly generalized.

Hash Functions – I



Hash Functions – II

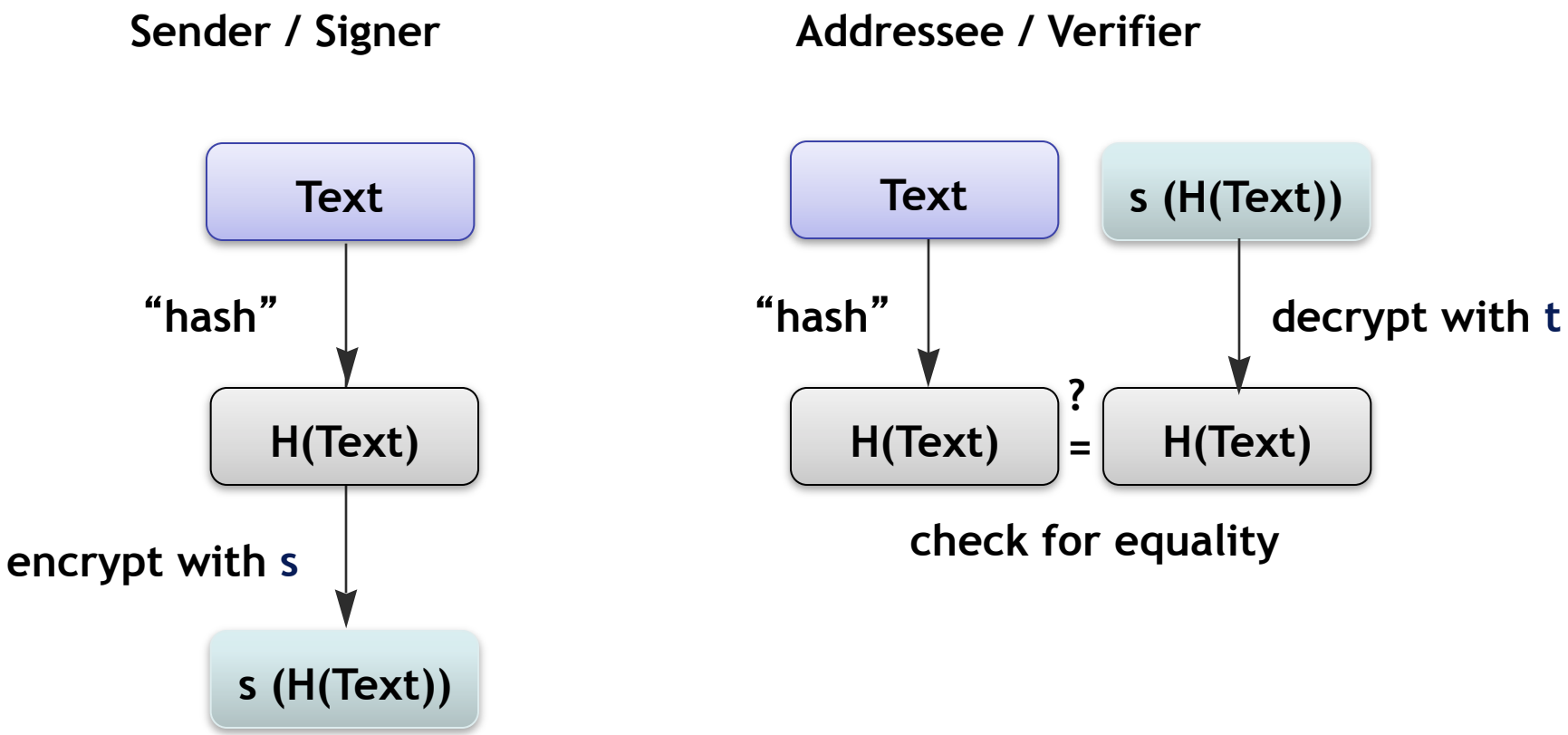


General hash functions *(H(s))*

Transformation of an input string *s* into an output string *h* **of fixed length** which is called hash value.

Example: mod 10 in the decimal system

Asymmetric Signature System (Example RSA)



- Signing key s only with the sender, test key t public
- Example is often mistakenly generalized.

Agenda

- General Concept
- Algorithms
- Legal Framework
- Mobile Signatures
- Secure Display Components
- Personal Security Assistants

EU eIDAS regulation 2014

- The EU REGULATION (EU) No 910/2014 on electronic signatures refers to the concept of an **electronic signature** as:

> "data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign"

[EU eIDAS Regulation 2014]

The advanced electronic signature requirements

Directive 1999/93/EC

- Uniquely linked to the signatory;
- Capable of identifying the signatory;
- Created using means that the signatory can maintain under their sole control;
- Linked to the data to which it relates in such a manner that any subsequent change in the data is detectable.

[EC Directive 1999]

REGULATION (EU) No 910/2014 repealing directive 1999/93/EC

- Uniquely linked to the signatory;
- Capable of identifying the signatory;
- Created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control;
- Linked to the data signed therewith in such a way that any subsequent change in the data is detectable.

[EU eIDAS Regulation 2014]

German Signature Law (SigG)

- **Objective and Area of Application**

(1) The purpose of this law is to create general conditions for digital signatures under which they may be deemed secure and forgeries of digital signatures or falsifications of signed data may be reliably ascertained.

SigG Requirements as to Technical Components

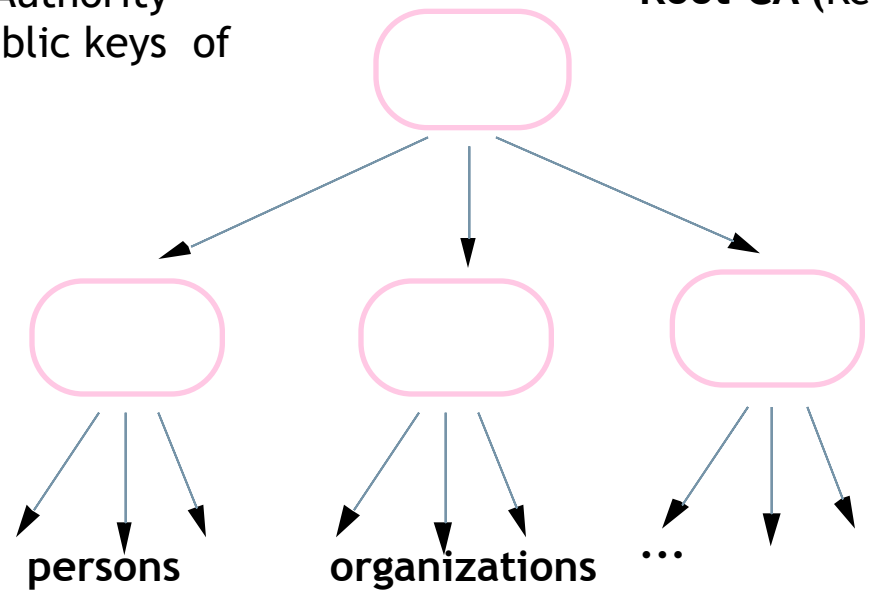
Example: display of data (§ 17(2)) [SigG01]

The signature component must:

- Clearly notify the signer that a signature is to be created *before* the signature is created
- Make clearly perceptible which data the signature refers to
- Secure the accordance of displayed data and signed data (“What you see is what you sign.”)

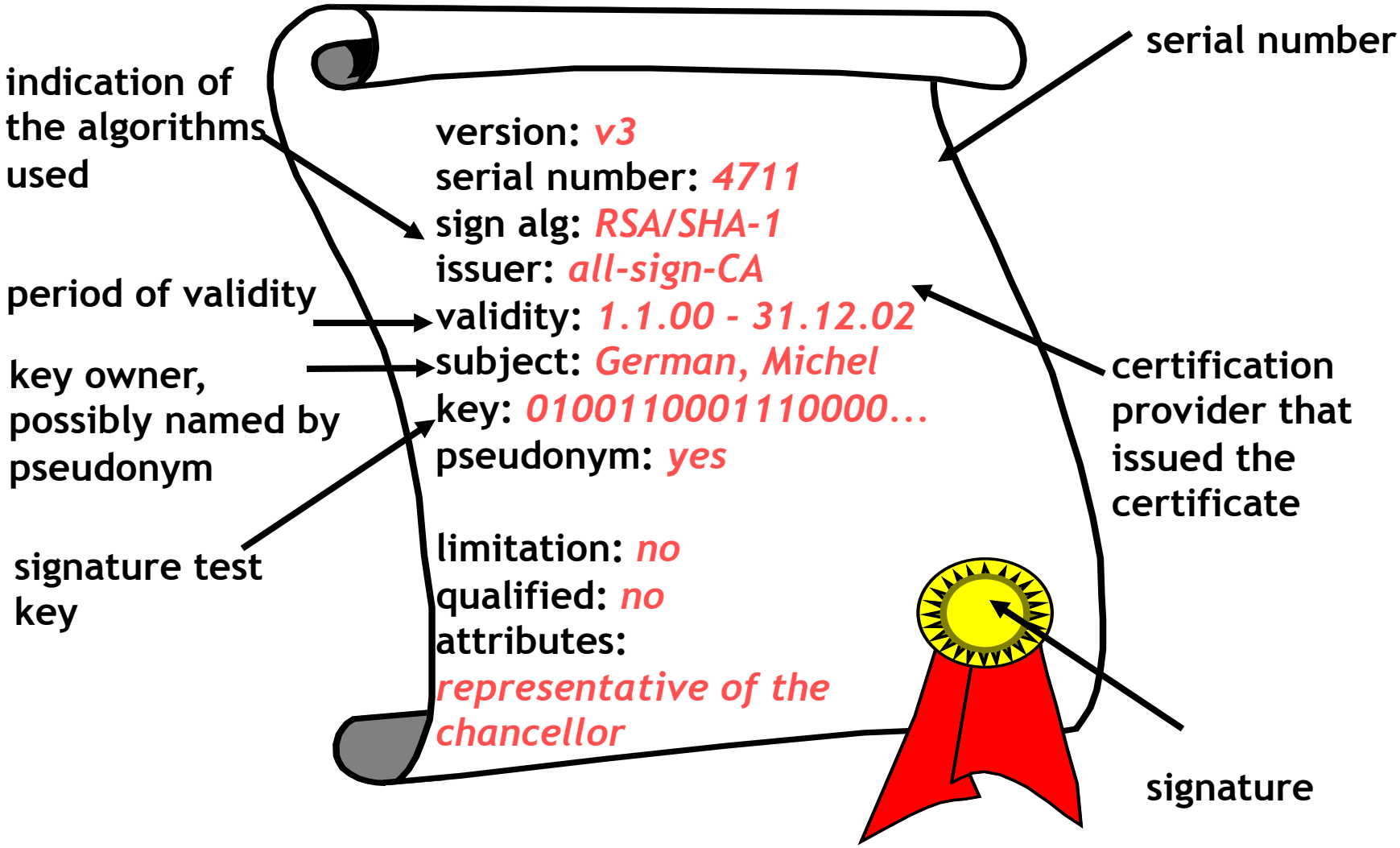
Hierarchical Certification of Public Keys
(Example: German Signature Law)

Regulatory Authority confirms public keys of the CAs



- The actual checking of the identity of the key owner takes place at so called Registration Authorities (e.g. notaries, bank branches, T-Points, ...)
- Security of the infrastructure depends on the reliability of the CAs.

Content of a Key Certificate
(according to German Signature Law and Regulation)



Tasks of a Certification Authority
(according to German Signature Law and Regulation)

- Reliable identification of persons who apply for a certificate
- Information on necessary methods for fraud resistant creation of a signature
- Provision for secure storage of the private key
  - At least Smartcard (protected with PIN)
- Publication of the certificate (if wanted)
- Barring of certificates (managing revocation lists)
- If necessary emission of time stamps
  - For a fraud resistant proof that an electronic document has been at hand at a specific time

Requirements to an Accredited CA
(according to German Signature Law and related Regulation)

- Checking of the following items by certain confirmation centers (BSI, TÜVIT, ...)
  - Concept of operational security
  - Reliability of the executives and of the employees as well as of their know-how
  - Financial strength for sustained operation
  - Exclusive usage of licensed technical components according to SigG and SigV
  - Security requirements as to operating premises and their access controls
- Possibly license of the Regulatory Authority

mobile business

Agenda

- General Concept
- Algorithms
- Legal Framework
- Mobile Signatures
- Secure Display Components
- Personal Security Assistants

Qualified Electronic Signatures

- Advanced electronic signatures:
  - Uniquely linked to the signatory;
  - Capable of identifying the signatory;
  - created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and
  - linked to the data signed therewith in such a way that any subsequent change in the data is detectable.
- Qualified certificates:
  - ‘qualified certificate for electronic signature’ means a certificate for electronic signatures, that is issued by a qualified trust service provider and meets the requirements laid down in Annex I.

[EU eIDAS regulation 2014]

Mobile Signatures

- Mobile signatures are signatures, which are created using a mobile device and which rely on signature or certification services in a location independent telecommunication environment.
- Usage: signatory mobility beyond fixed, secure desktop workstation with trusted, personal signing equipment.

[Roßnagel 2004]

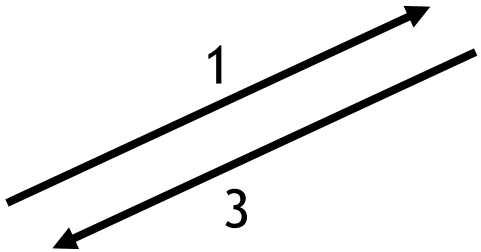
Server vs. Client Signatures

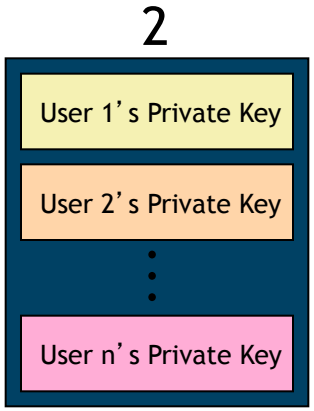
- Server based electronic signatures are signatures, that are created by a service provider for a user.
- Client signatures are electronic signatures created only by means of the mobile device.

[Roßnagel 2004]

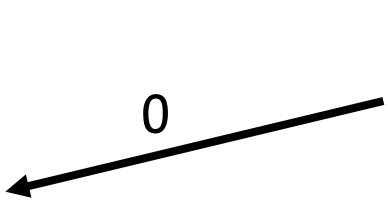
Server Signatures Infrastructure

Mobile device

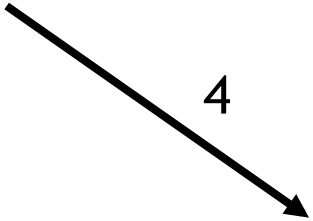




Signature Server



CSP



Relying party

0: Certificate Service Provider (CSP) creates certificate.
1: Mobile user authorizes signature on server.
2: Server creates signature for mobile user.
3: Signature sent to mobile user
4: Signature sent to relying party

[Roßnagel 2004]

Analysis of Server Signatures

Directive 1999/93/EC

- This violates article 2,2 (c) of EC directive for advanced signatures:
  "…by means the signatory can maintain under his sole control."

[EC Directive 1999]

REGULATION (EU) No 910/2014 repealing directive 1999/93/EC

- article 26 (c) of REGULATION (EU) No 910/2014 for advanced signatures:
  "…by means the signatory, with high level of confidence, can maintain under his sole control."

[EU eIDAS Regulation 2014]

- Infrastructure to enforce secure authorization of server signatures has high complexity.

Client Signatures: Multiple Cards

Use of separate smart cards for telephony and signature:

- Dual Card
  Exchange of SIM against Secure Signature Creation Device (SSCD)
- Dual Slot
  Mobile device carries two card readers for SIM and SSCD

[Roßnagel 2004]

Client Signatures: SIM based

- One smart card with both functions
  - Can be equivalent to established SSCDs
  - Can be certified according to security evaluation criteria
  - Under control of the user
- Needs two different PIN codes!

[Roßnagel 2004]

Challenges of SIM Signatures | 1

- Who owns the smart card?
  - SIM issued by Mobile Operator (MO)
  - SSCD issued by CSP
  - SIM stores keys that belong to MO & user.
  - What happens to signature when user changes Mobile Operator?
- Challenge:
  Provide a shipment model for SIM cards within the MO distribution scheme that gives users a choice of their CSP.

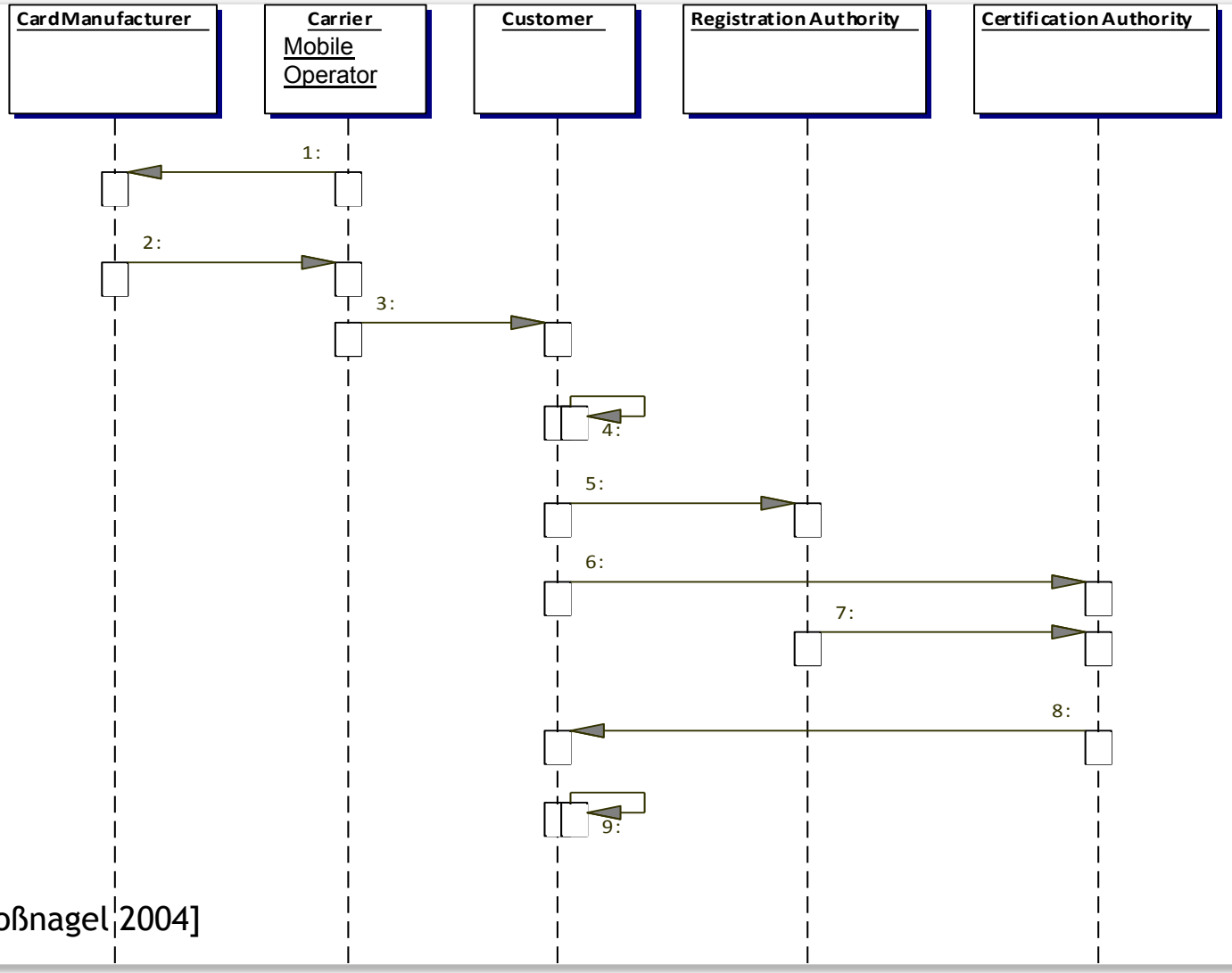
[Roßnagel 2004]

Challenges of SIM Signatures |2

- Customer wants to use SIM right away, but certification for signature takes time.
- Solution:
  - Handing out the signature capable SIM Card and
  - adding signing functionality later on request.
- Is this still an advanced signature based on a qualified certificate?

[Roßnagel 2004]

Certification on Demand



[Roßnagel 2004]

Certification on Demand

1. The MO gives IMSI/Ki pairs to a card manufacturer (or lets them be generated there based on information from the MO).
2. The card manufacturer returns (or provides) a SIM card containing an IMSI/Ki pair, a key generator for the signature application and the public key of the RootCA to the Mobile Operator.
3. The SIM card is sold to the customer and the Mobile Operator provides a nullpin, that is used to activate the signing functionality.
4. The customer activates the signing functionality by entering the nullpin.
5. The customer registers at a Registration Authority of his choice, providing identification information and his public key.
6. The customer sends his identification information signed with his private key over the air to the Certification Authority.
7. The Registration Authority sends the public key and the identification information to the Certification Authority.
8. If the information provided by the customer and the Registration Authority match the Certification Authority issues a certificate for the customer and sends it over the air to his mobile phone.
9. The user can verify the validity of his certificate by checking the certificate issued by the RootCA for the Certification Service Provider

[Roßnagel 2004]

Certification on Demand

- Distribution scheme of Mobile Operator stays intact.
- Signature capable SIM will be more expensive but MO can create revenue with:
  - Increase in traffic
  - Selling signature capable SIM cards at a higher price
- CSP gains large potential customer base.

[Roßnagel 2004]

Mobility and Signing

- Restrictions in mobile devices
  - Expensive, low-band data transfer, e.g. over GSM/ GPRS
  - Visualization of complex “Document To Be Signed” (DTBS) on mobile device’s small display is tricky.
  - Online-verification of certification paths with low-band data rates is not always feasible.
  - Limited memory may hinder the proper processing of revocation lists.
- Platform security
  - Mobile phones are becoming open platforms
  - A trusted device is necessary (➲ TCG/Perseus)

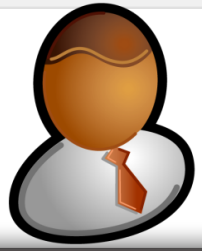
[Roßnagel 2004]

mobile business

Agenda

- General Concept
- Algorithms
- Legal Framework
- Mobile Signatures
- Secure Display Components
- Personal Security Assistants

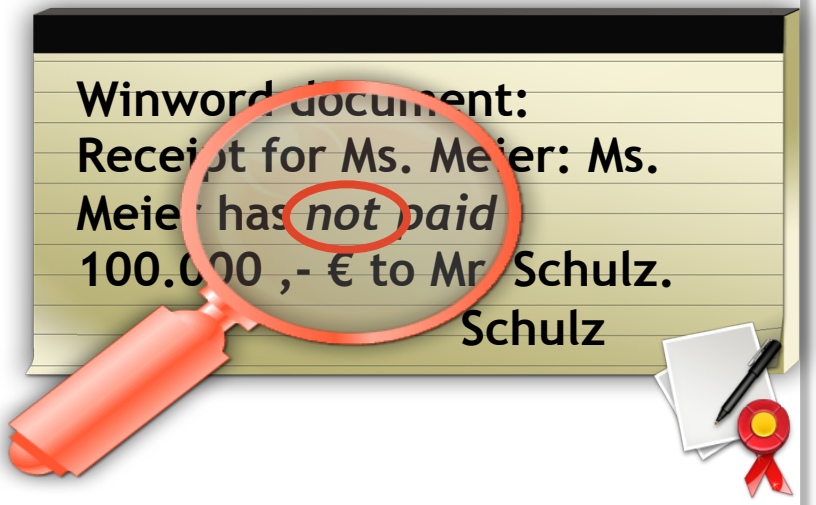
Presentation Problems



Mr. Schulz

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

Ms. Meier



But check for hidden text !!!!

[Based on IsRo]

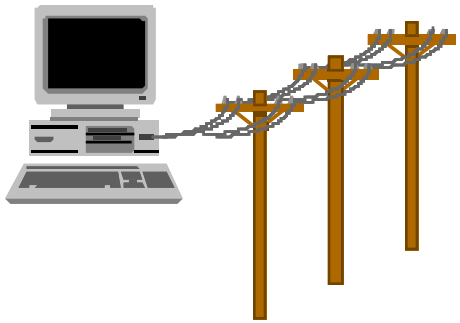
SigG Requirements as to Technical Components

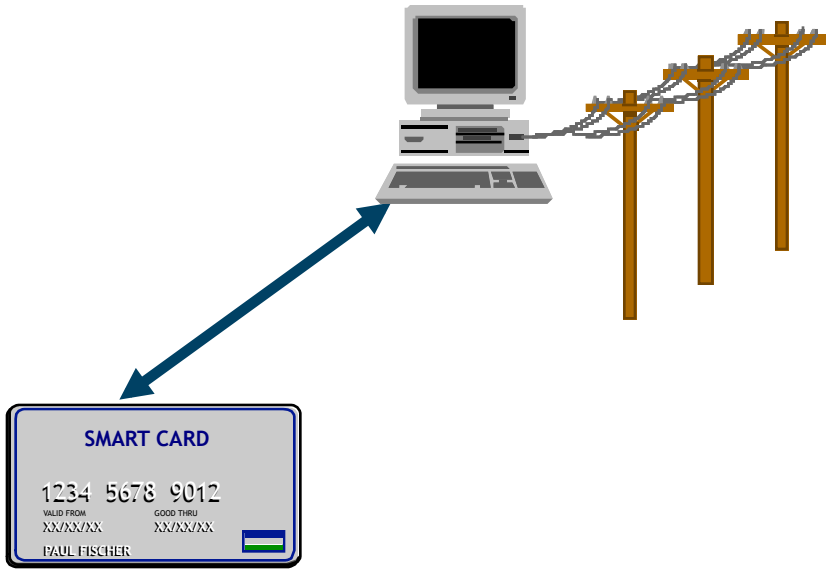
Example: display of data (§ 17(2)) [SigG01]

The signature component must:

- Clearly notify the signer that a signature is created *before* the signature is created
- Make clearly perceptible which data the signature refers to
- Secure the accordance of displayed data and signed data (“What you see is what you sign.”)

Secure Equipment: Threats from Trojan Horses

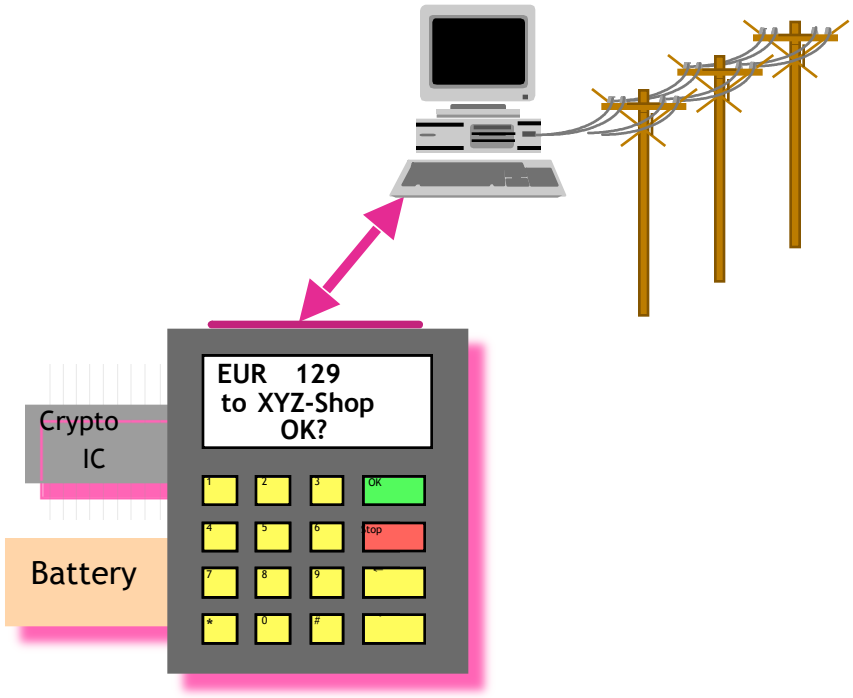




Private key
on HD, in memory

Private key and
signature function in chip card

Secure Equipment: Avoiding Threats from Trojan Horses



Wallet with private key and signature function

Secure Equipment: How to view a document

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

mobile business

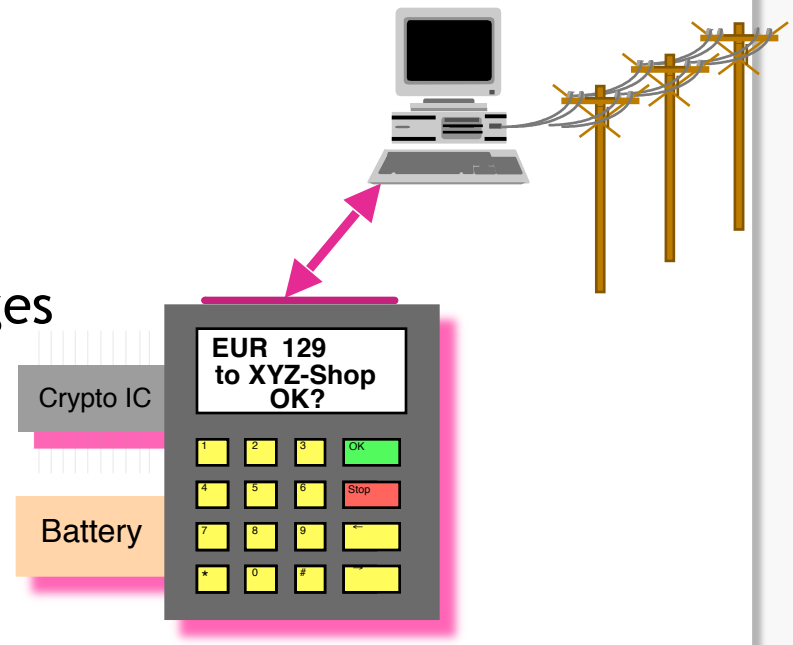
Agenda

- General Concept
- Algorithms
- Legal Framework
- Mobile Signatures
- Secure Display Components
- Personal Security Assistants

Personal Terminals

A popular vision: Security Assistants

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



Challenges of Personal Terminals

- 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 what it shall do?
  - How (much) can I trust it?

Personal Security Assistants Platforms?

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

Literature

- Bishop, Matt (2005): Introduction to Computer Security. Boston: Addison Wesley, 2005.
- EC Directive 1999/93/EC (1999)
  Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures.
- 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.
- Federrath, H. and Pfitzmann, A. (1997)
  Bausteine zur Realisierung mehrseitiger Sicherheit, in: G. Müller and A. Pfitzmann (Eds.): *Mehrseitige Sicherheit in der Kommunikationstechnik*, Boston, Addison Wesley, pp. 83-104.
- Isselhorst/Rohde, BSI.
- Rivest, R. L.; Shamir, A. and Adleman, L. (1978)
  A Method for Obtaining Digital Signatures and Public Key Cryptosystems, *Communications of the ACM* (21:2), pp. 120-126.
- Roßnagel, H. (2004)
  Mobile Signatures and Certification on Demand, in: S. K. Katsikas; S. Gritzalis and J. Lopez (Eds.): *Public Key Infrastructures*, Berlin Heidelberg, Springer, pp. 274-286.31

Annex I
EU eIDAS regulation 2014, requirements for qualified certificate

- an indication that the certificate has been issued as a qualified certificate …
- Data about the qualified trust service provider issuing the qualified certificates …
- … name of the creator of the seal and, where applicable, registration number as stated in the official records;
- … validation data and details of the beginning and end of the certificate's period of validity;
- the certificate identity code
- the advanced electronic signature or advanced electronic seal of the issuing qualified trust service provider;
- the location where the certificate supporting the advanced electronic signature or advanced electronic seal is available;
- the location of the services that can be used to enquire as to the validity status of the qualified certificate;
- An indication where the electronic seal creation data related to the electronic seal validation data is located in a qualified electronic seal creation device…

[EU eIDAS Regulation 2014]