Lecture 10

Application Domains III: (Mobile) Electronic Signatures

Mobile Business II (SS 2020)

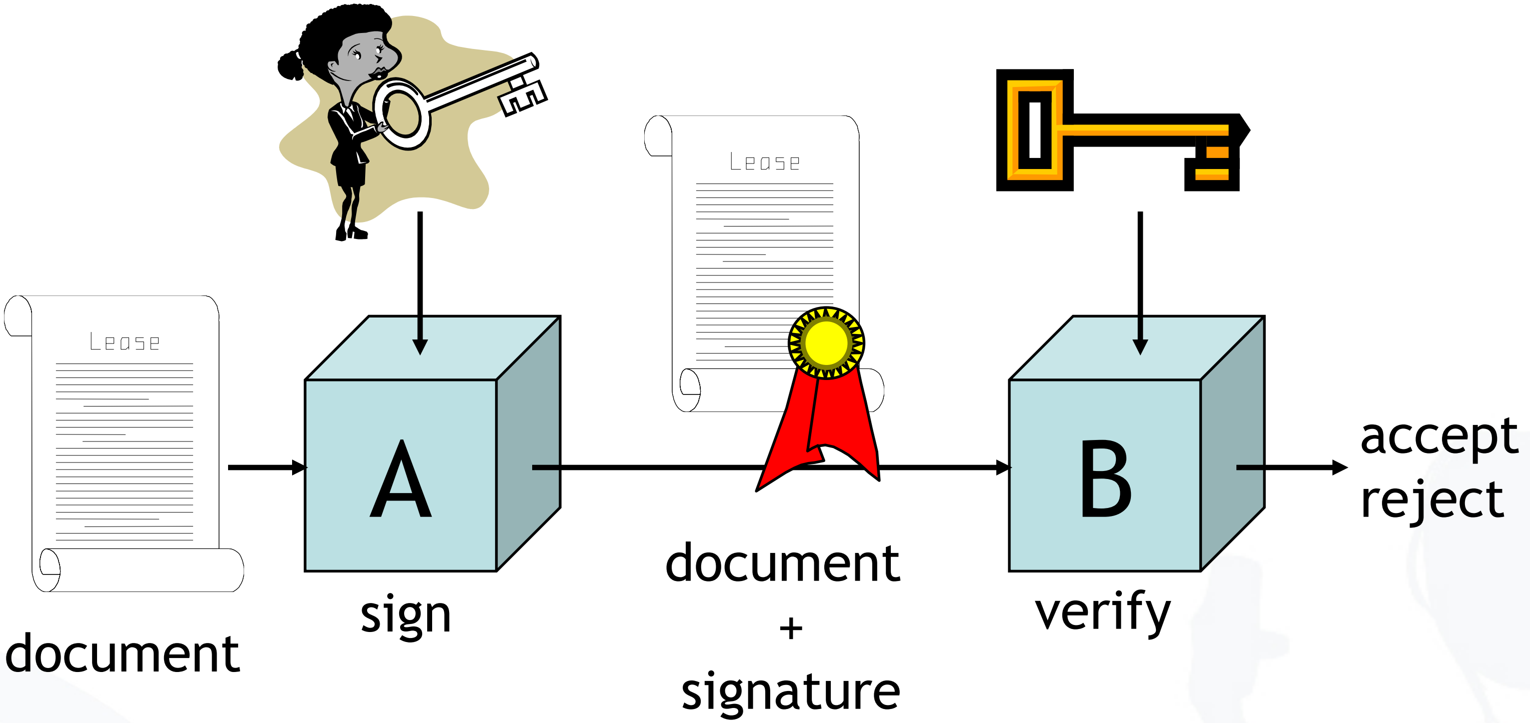
Prof. Dr. Kai Rannenberg

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

Agenda

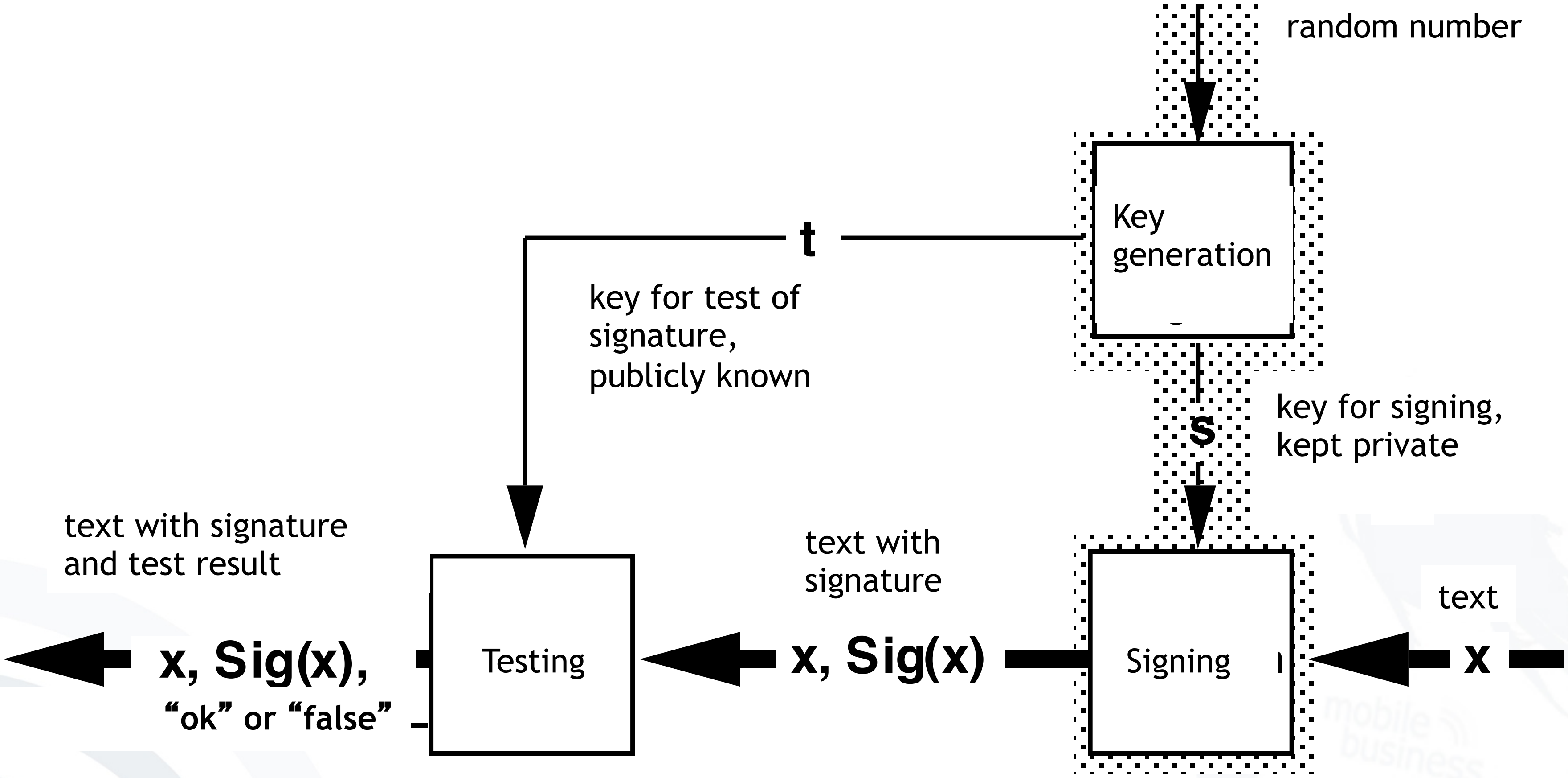
- General Concept
- Algorithms
- Legal Framework
- German Signature Market
- Mobile Signatures
- Secure Display Components and Personal Security Assistants

Digital Signatures



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

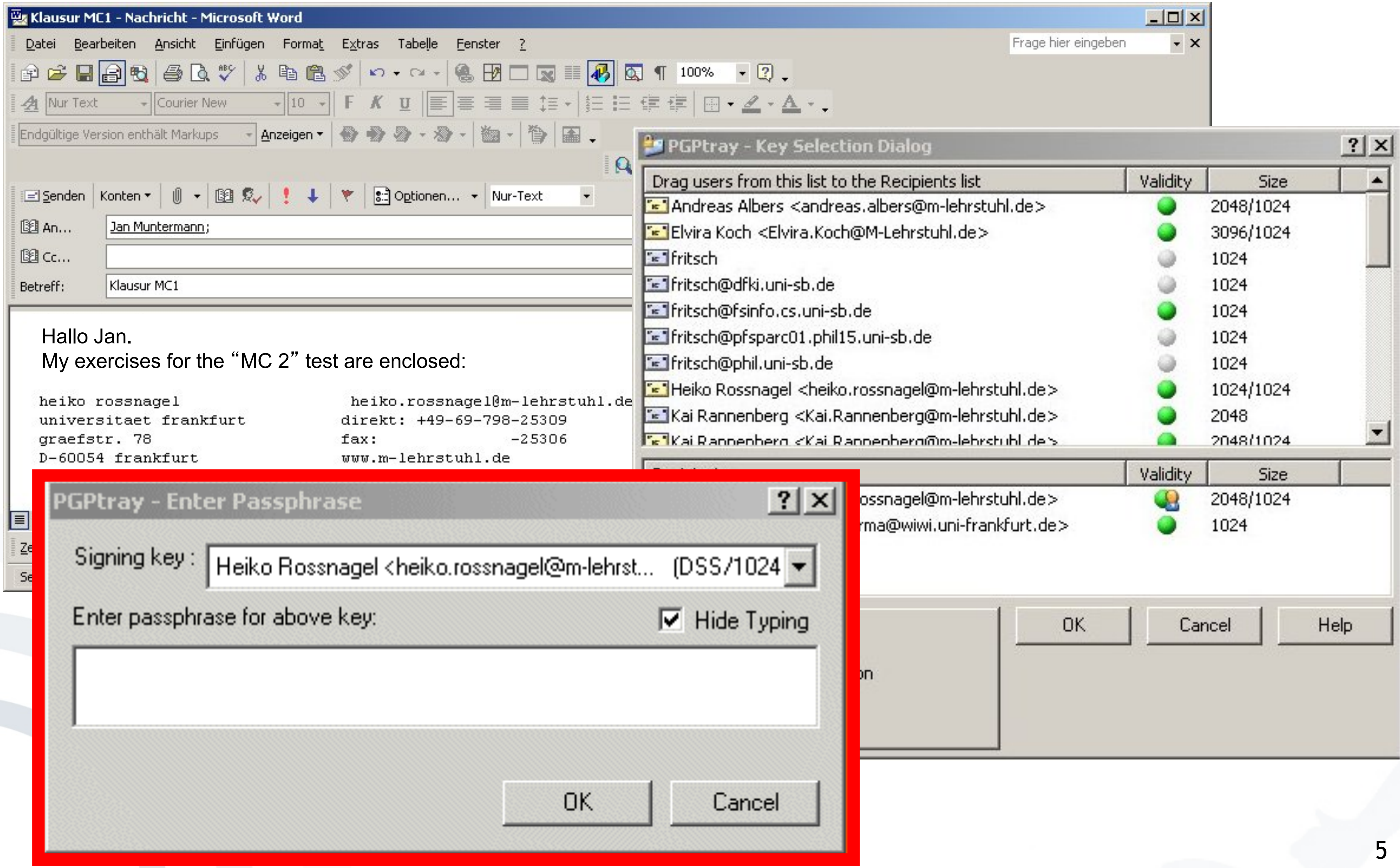
Asymmetric Signature System


random number
Key generation
t
key for test of signature, publicly known
s
key for signing, kept private
text with signature and test result
x, Sig(x), "ok" or "false"
Testing
text with signature
x, Sig(x)
Signing
text
x

➲ locked glass show-case; just one key to put something in

[Federrath and Pfitzmann 1997]

Example PGP: Encrypt and Sign a Message



Klausur MC1 - Nachricht - Microsoft Word
Datei Bearbeiten Ansicht Einfügen Format Extras Tabelle Fenster ?
Frage hier eingeben
100%
Nur Text
Courier New
10
Endgültige Version enthält Markups
Anzeigen
Senden
Konten
Optionen...
Nur-Text
PGPtray - Key Selection Dialog
OK
Cancel
Help
PGPtray - Enter Passphrase
OK
Cancel

An...: Jan Muntermann;

Cc...:

Betreff: Klausur MC1

Hallo Jan.
My exercises for the “MC 2” test are enclosed:

```
heiko rossnagel                  heiko.rossnagel@m-lehrstuhl.de
universitaet frankfurt          direkt: +49-69-798-25309
graefstr. 78                    fax:             -25306
D-60054 frankfurt               www.m-lehrstuhl.de
```

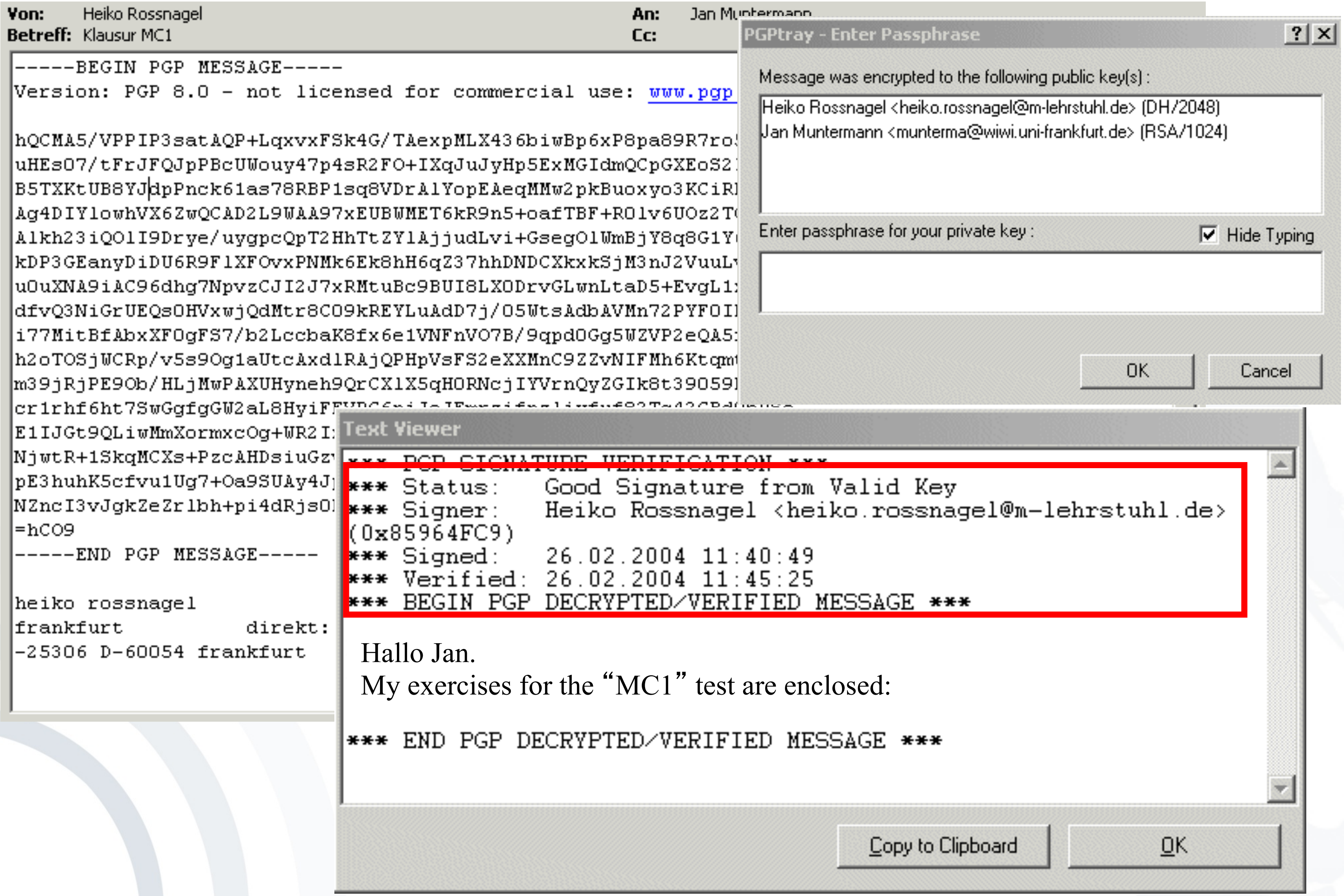
Drag users from this list to the Recipients list	Validity	Size
Andreas Albers <andreas.albers@m-lehrstuhl.de>	●	2048/1024
Elvira Koch <Elvira.Koch@M-Lehrstuhl.de>	●	3096/1024
fritsch	○	1024
fritsch@dfki.uni-sb.de	○	1024
fritsch@fsinfo.cs.uni-sb.de	●	1024
fritsch@pfsparc01.phil15.uni-sb.de	○	1024
fritsch@phil.uni-sb.de	○	1024
Heiko Rossnagel <heiko.rossnagel@m-lehrstuhl.de>	●	1024/1024
Kai Rannenberg <Kai.Rannenberg@m-lehrstuhl.de>	●	2048
Kai Rannenberg <Kai.Rannenberg@m-lehrstuhl.de>	●	2048/1024

	Validity	Size
ossnagel@m-lehrstuhl.de>	●	2048/1024
rma@wiwi.uni-frankfurt.de>	●	1024

Signing key : Heiko Rossnagel <heiko.rossnagel@m-lehrst... (DSS/1024

Enter passphrase for above key: ☑ Hide Typing

Example PGP: Decrypt and Check a Message



Von: Heiko Rossnagel
Betreff: Klausur MC1
An: Jan Muntermann
Cc:

```
-----BEGIN PGP MESSAGE-----
Version: PGP 8.0 - not licensed for commercial use: www.pgp

hQCMA5/VPPIP3satAQP+LqxvxFSk4G/TAexpMLX436biwBp6xP8pa89R7ro
uHEs07/tFrJFQJpPBcUWouy47p4sR2FO+IXqJuJyHp5ExMGIdmQCpGXEoS2
B5TXKtUB8YJdpPnck61as78RBP1sq8VDrA1YopEAeqMMw2pkBuoxyo3KCiR
Ag4DIYlowhVX6ZwQCAD2L9WAA97xEUBWMET6kR9n5+oafTBF+R01v6UOz2T
Alkh23iQO1I9Drye/uygpcQpT2HhTtZYlAjjudLvi+GsegO1WmBjY8q8G1Y
kDP3GEanyDiDU6R9F1XFOvxPNMk6Ek8hH6qZ37hhDNDCXkxkSjM3nJ2VuuL
u0uXNA9iAC96dhg7NpvzCJI2J7xRMtuBc9BUI8LX0DrvGLwnLtaD5+EvgL1
dfvQ3NiGrUEQsOHVxwjQdMtr8C09kREYLuAdD7j/05WtsAdbAVMn72PYFOI
i77MitBfAbxXFOgFS7/b2LccbaK8fx6e1VNFnVO7B/9qpd0Gg5WZVP2eQA5
h2oTOSjWCRp/v5s9Og1aUtcAxd1RAjQPHpVsFS2eXXMnC9ZZvNIFMh6Ktqm
m39jRjPE9Ob/HLjMwPAXUHyneh9QrCX1X5qHORNcjIYVrnQyZGIk8t39059
cr1rhf6ht7SwGgfgGW2aL8HyiF
E1IJGt9QLiwMmXormxcOg+WR2I
NjwtR+1SkqMCXs+PzcAHDsiuGz
pE3huhK5cfvu1Ug7+Oa9SUAy4J
NZncI3vJgkZeZr1bh+pi4dRjs0
=hCO9
-----END PGP MESSAGE-----


heiko rossnagel
frankfurt              direkt:
-25306 D-60054 frankfurt
```

Message was encrypted to the following public key(s) :

Heiko Rossnagel <heiko.rossnagel@m-lehrstuhl.de> (DH/2048)
Jan Muntermann <munterma@wiwi.uni-frankfurt.de> (RSA/1024)

Enter passphrase for your private key :

☑ Hide Typing

```
*** PGP SIGNATURE VERIFICATION ***
*** Status:   Good Signature from Valid Key
*** Signer:   Heiko Rossnagel <heiko.rossnagel@m-lehrstuhl.de>
(0x85964FC9)
*** Signed:   26.02.2004 11:40:49
*** Verified: 26.02.2004 11:45:25
*** BEGIN PGP DECRYPTED/VERIFIED MESSAGE ***
```

Hallo Jan.
My exercises for the “MC1” test are enclosed:

```
*** END PGP DECRYPTED/VERIFIED MESSAGE ***
```

Agenda

- General Concept
- Algorithms
- Legal Framework
- German Signature Market
- Mobile Signatures
- Secure Display Components and Personal Security Assistants

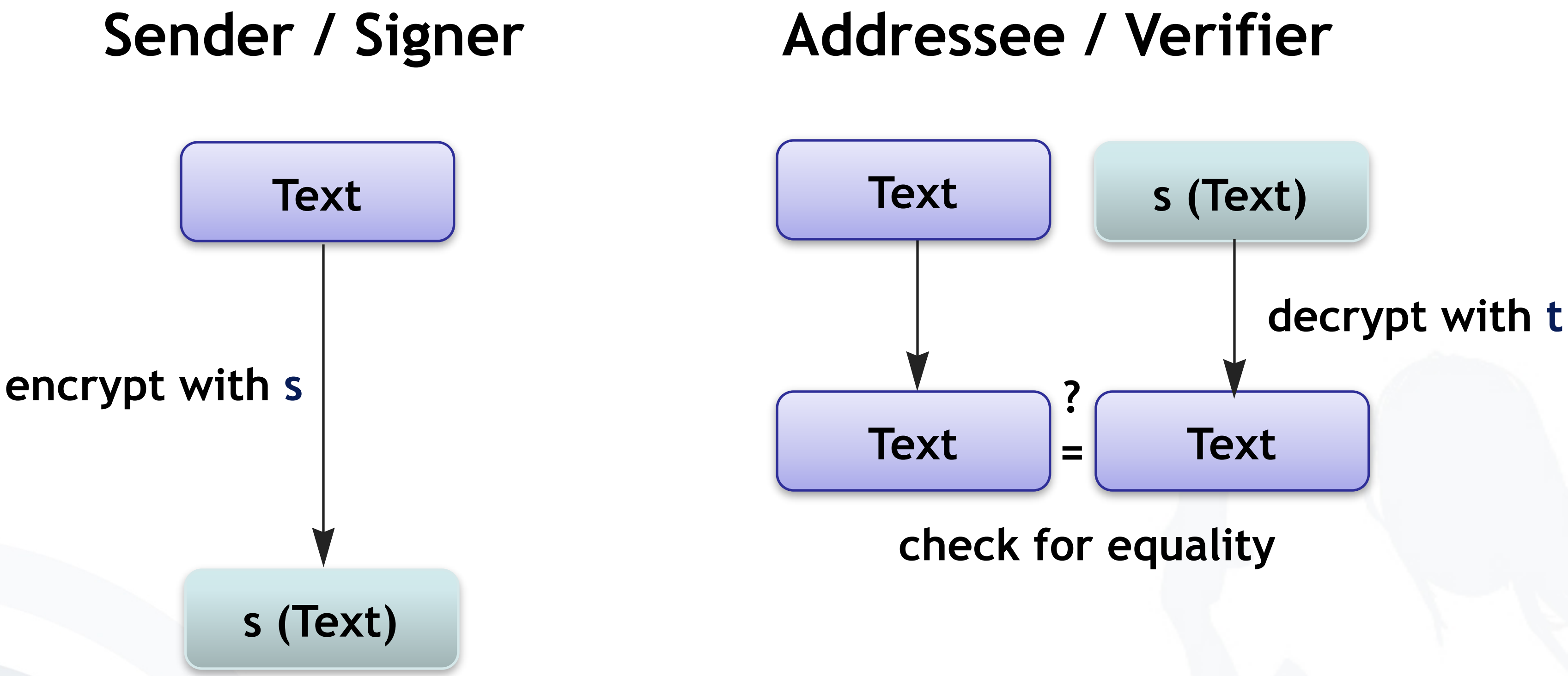
Asymmetric Signature Systems: Examples

- 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]

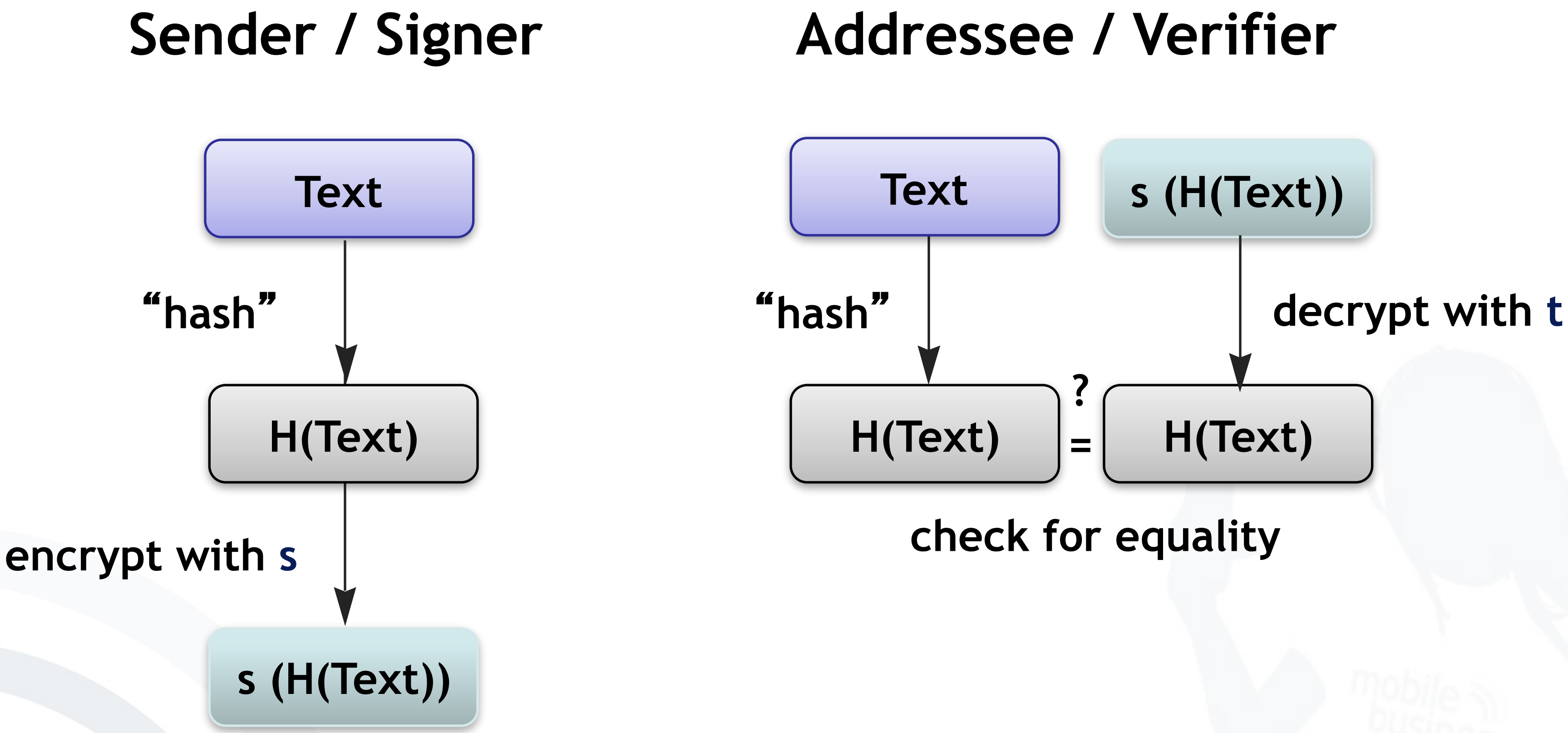
- DSA: Digital Signature Algorithm
  - Determined in the Digital Signature Standard of the NIST (USA),
  - Based on discrete logarithms (Schnorr, ElGamal),
  - Key length is set to 1024 bit.

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

- **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
- **Cryptographic** hash functions
  - Generally require further characteristics
    - *H*(*s*) is easily to compute for each *s*.
    - *H*(*s*) must be difficult to invert: In terms of figures it is difficult to compute *s* from *h*.
    - Virtual collision freedom: In terms of figures it is difficult to create collisions H(s1) = H(s2).
  - Examples: SHA-1, MD5, MD4

Agenda

- General Concept
- Algorithms
- Legal Framework
- German Signature Market
- Mobile Signatures
- Secure Display Components and 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.

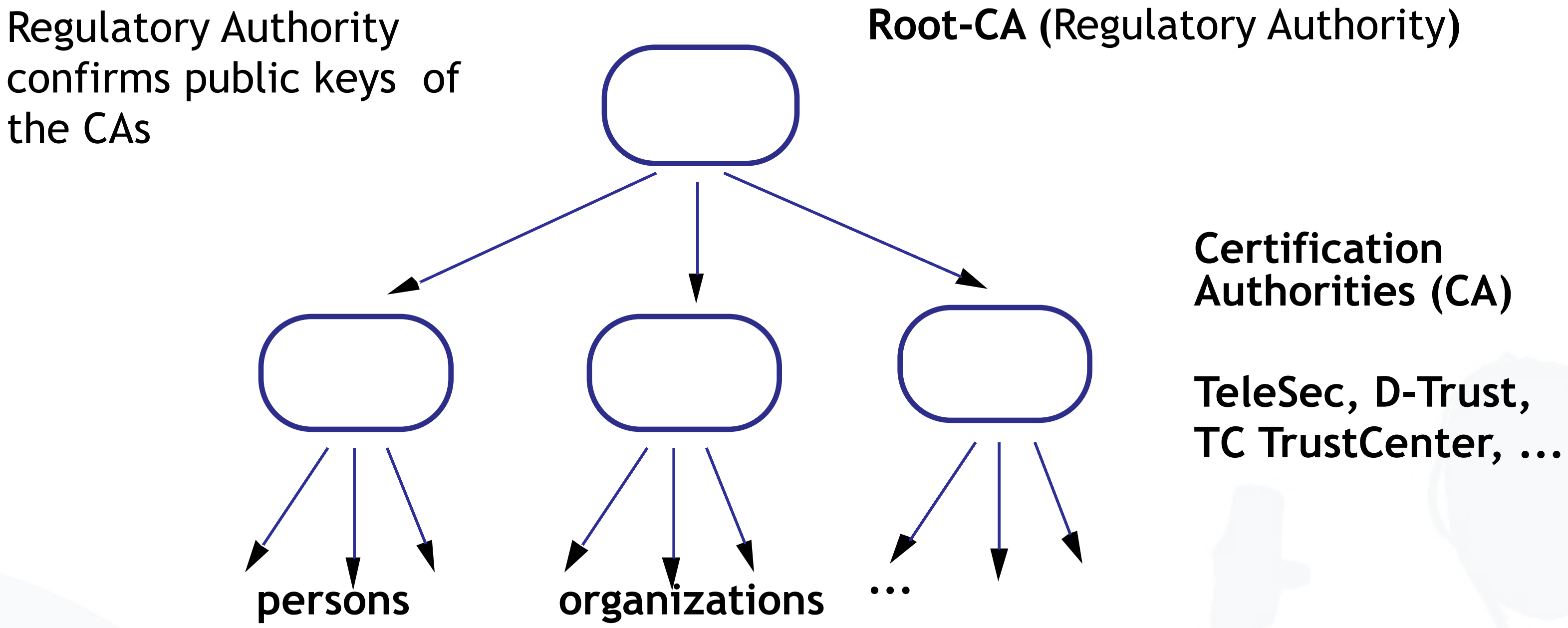
SigG Requirements as to Technical Components

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.”)

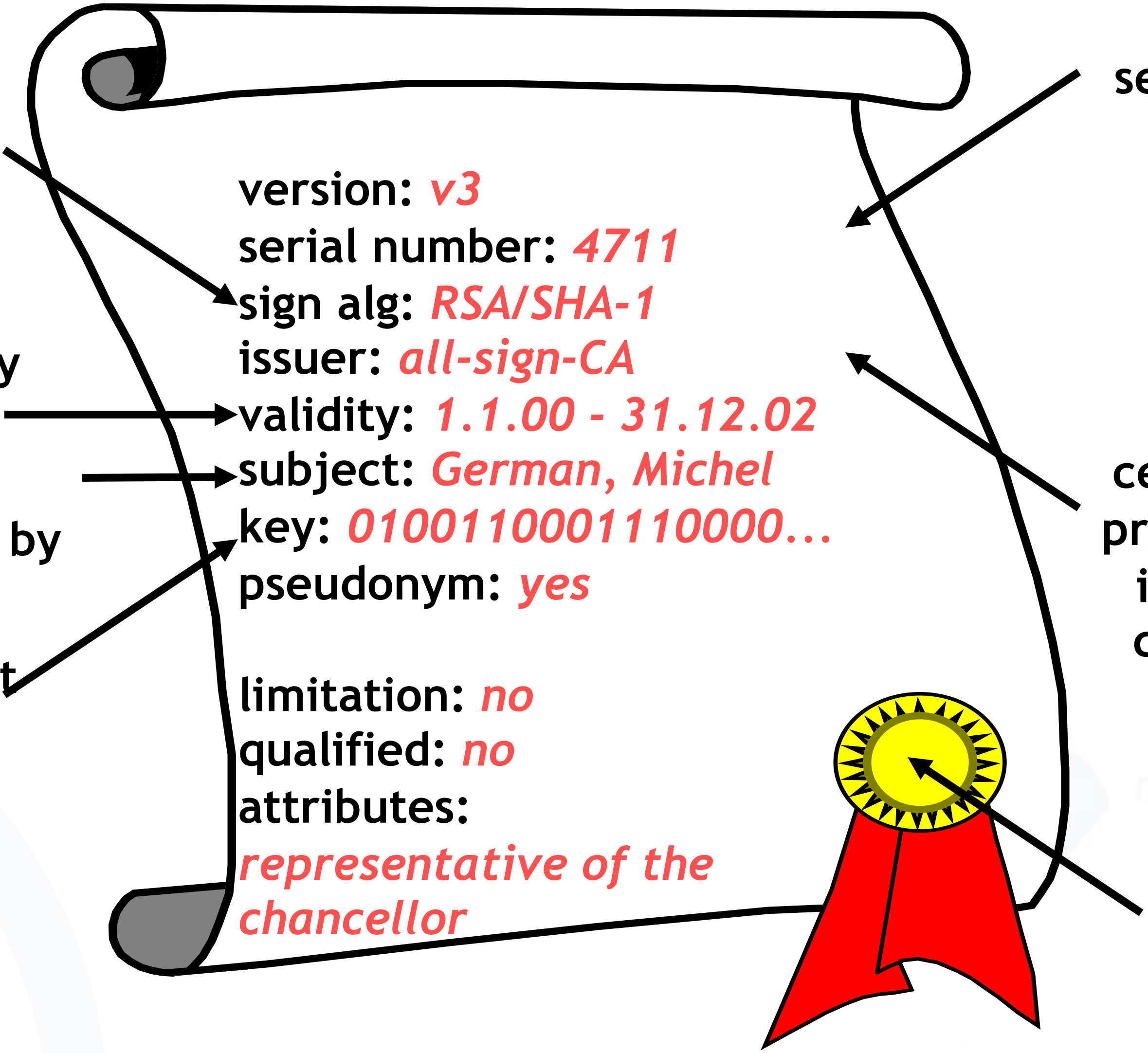
Hierarchical Certification of Public Keys
(Example: German Signature Law)


Regulatory Authority confirms public keys of the CAs
Root-CA (Regulatory Authority)
Certification Authorities (CA)
TeleSec, D-Trust, TC TrustCenter, ...
persons
organizations
...

- 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)



indication of the algorithms used

period of validity

key owner, possibly named by pseudonym

signature test key

version: *v3*
serial number: *4711*
sign alg: *RSA/SHA-1*
issuer: *all-sign-CA*
validity: *1.1.00 - 31.12.02*
subject: *German, Michel*
key: *0100110001110000...*
pseudonym: *yes*

limitation: *no*
qualified: *no*
attributes:
representative of the chancellor

serial number

certification provider that issued the certificate

signature

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
- 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 power for continuous 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 regulation authority

Agenda

- General Concept
- Algorithms
- Legal Framework
- German Signature Market
- Mobile Signatures
- Secure Display Components and Personal Security Assistants

Signature Market

- Legal and technical framework exists for years.
- So far qualified electronic signatures are not successful in the market.
- Circa 0.4 million qualified certificates in total have been issued in Germany from 2001 to 2010 [Sommer 2011].

➲ Expectations have not been fulfilled.

Fees in 2005 (in €)

Certificate Service Providers (CSP)	Fee for Issuing of a certificate	Basic fee per year of use	Total fee for 2-year usage
D-Trust GmbH	41	29	99
Deutsche Post Signtrust	0	39	78
TC Trust Center	8	62	132
T-TeleSec	23,57	42,95	109,47

[Lippmann and Roßnagel 2005]

Discontinued Certificate Service Providers

Certificate Service Providers (CSP)	Fee for issuing a certificate	Basic fee per year of use	Total fee for 2-year usage	Service discontinued
Deutsche Post Signtrust	0	39	78	June 2015
TC Trust Center	8	62	132	June 2006

[BNetzA 2015]

Fees in 2016 (in €)

Prices incl. 19% VAT

Certificate Service Providers (CSP)	Total costs Certificate validity of				
	1 year	2 years	3 years	4 years	5 years
D-Trust GmbH (100% subsidiary of Bundesdruckerei GmbH) d-trust.de	n/a	129,71	n/a	213,01	n/a
Medisign GmbH (for health care professionals) medisign.de	82,80	n/a	n/a	n/a	n/a
TeleSec - Trust Center der Deutschen Telekom AG telesec.de	n/a	99,00	129,00	n/a	199,00
Bundesnotarkammer zertifizierungsstelle.bnotk.de/	n/a	49,90	n/a	n/a	n/a

[CSP websites, BNetzA 2015]

Costs and Benefits

	Private Customers		Companies		Public Administration	
	Costs	Benefits	Costs	Benefits	Costs	Benefits
Electronic bid invitations			■	■		■
Electronic tax declaration	■		■			■
Access to public archives	■		■	■		■
Electronic elections	■					■
Application for public documents	■					■
Notifying change of residence	■					■
Electronic dunning procedures			■	■		■
Electronic marketplaces	■	■	■	■	■	■
Automated orderings			■	■	■	■
Online-Banking	■		■	■	■	
Alteration of contracts online	■			■		
Electronic billing			■	■		
Archiving			■	■	■	■
Total	8	1	9	9	4	10

[Lippmann and Roßnagel 2005]

Agenda

- General Concept
- Algorithms
- Legal Framework
- German Signature Market
- Mobile Signatures
- Secure Display Components and Personal Security Assistants

How it was: Qualified Electronic Signatures

- Advanced electronic signatures:
  - Uniquely linked to the signatory
  - Capable of identifying the signatory
  - Created using means that the signatory maintains under his sole control
  - Linked to the data to which it relates in such a manner that any subsequent change of the data is detectable
- Qualified certificates:
  - Can be issued for advanced signatures by CSPs if they meet the requirements of Annex I of the EC Directive

[EC-Directive 1999]

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.

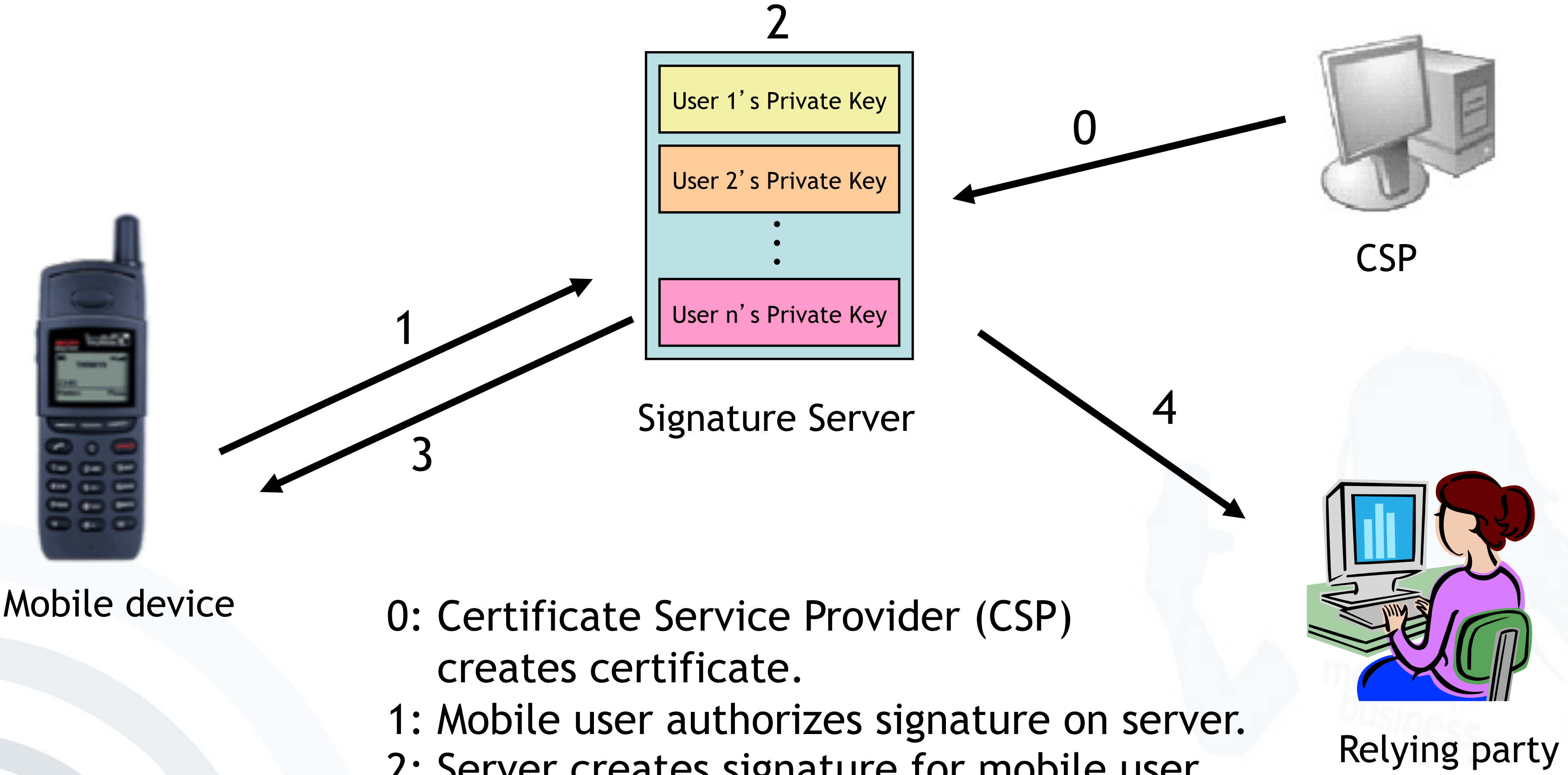
[Roßnagel 2004]

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



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]

Server Signatures Legal Context

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]

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.

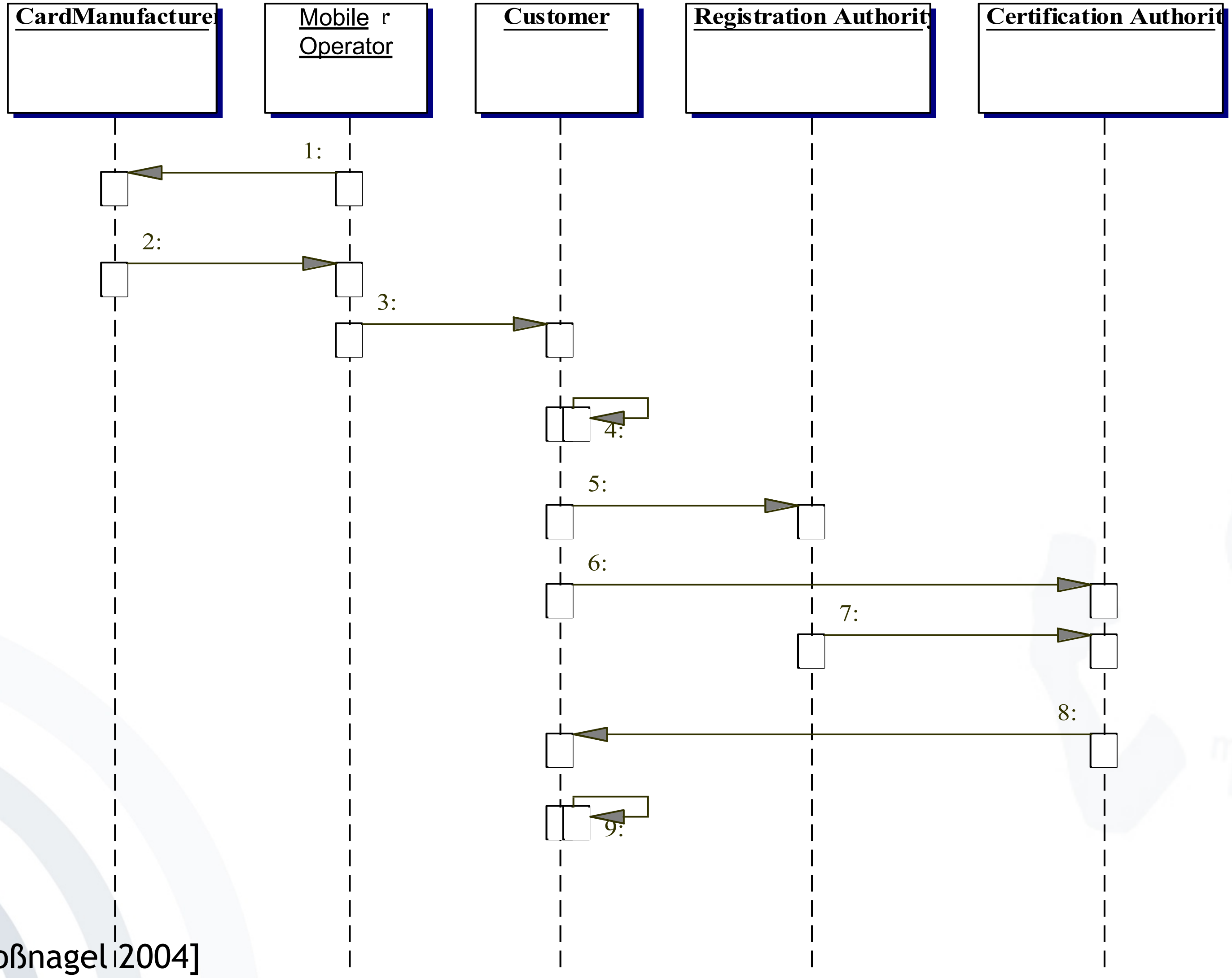
[Roßnagel 2004]

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
  - 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.

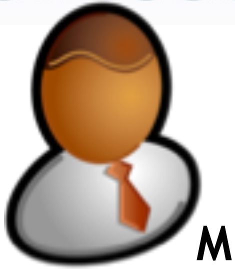
- Platform security
  - Mobile phones are becoming open platforms
  - A trusted device is necessary (➲ TCG/Perseus)

[Roßnagel 2004]

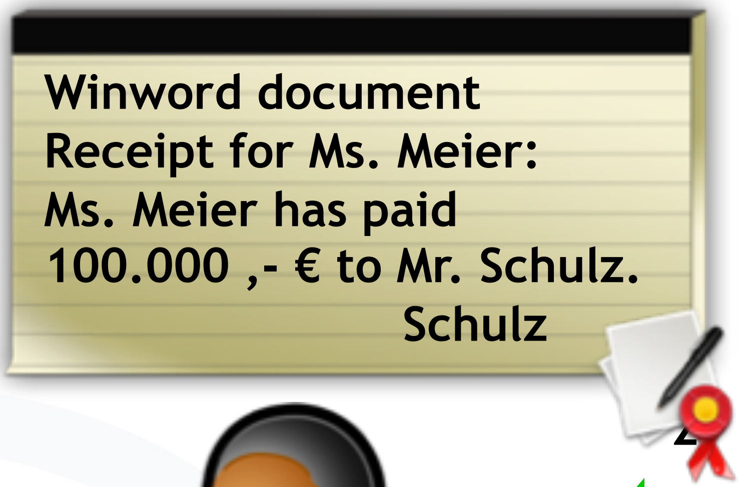
Agenda

- General Concept
- Algorithms
- Legal Framework
- German Signature Market
- Mobile Signatures
- Secure Display Components and Personal Security Assistants

Presentation Problems

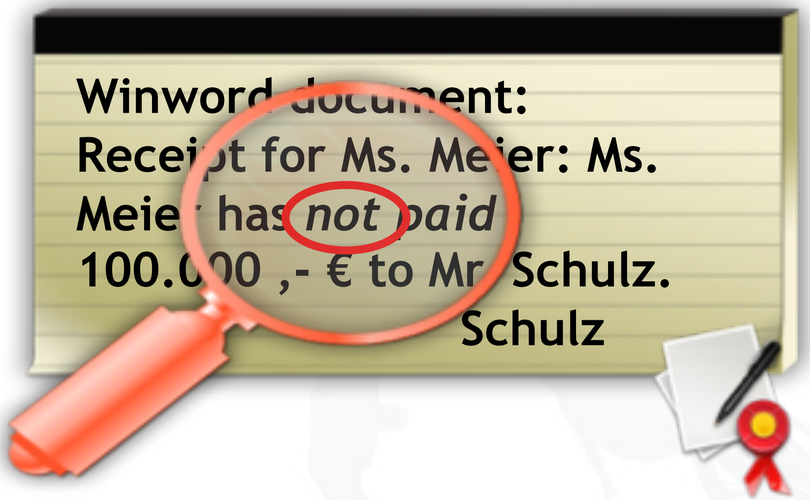


Mr. Schulz



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

Ms. Meier



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

But check for hidden text !!!!

[Based on IsRo]

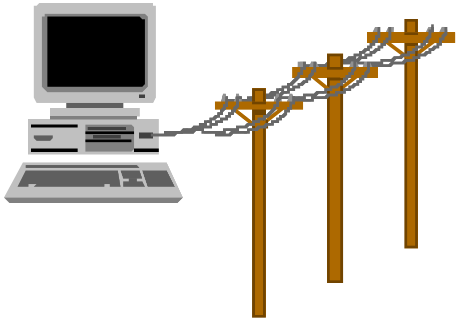
SigG Requirements as to Technical Components

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

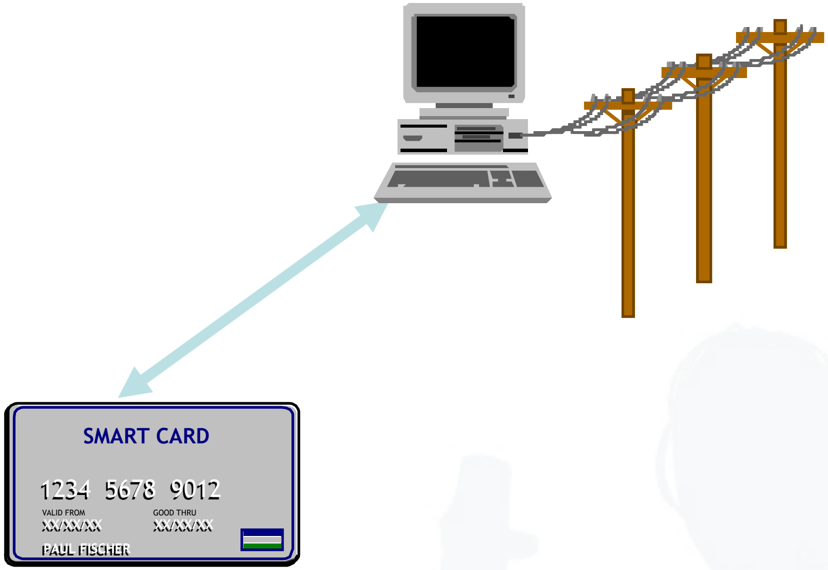
The signature component must:

- 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

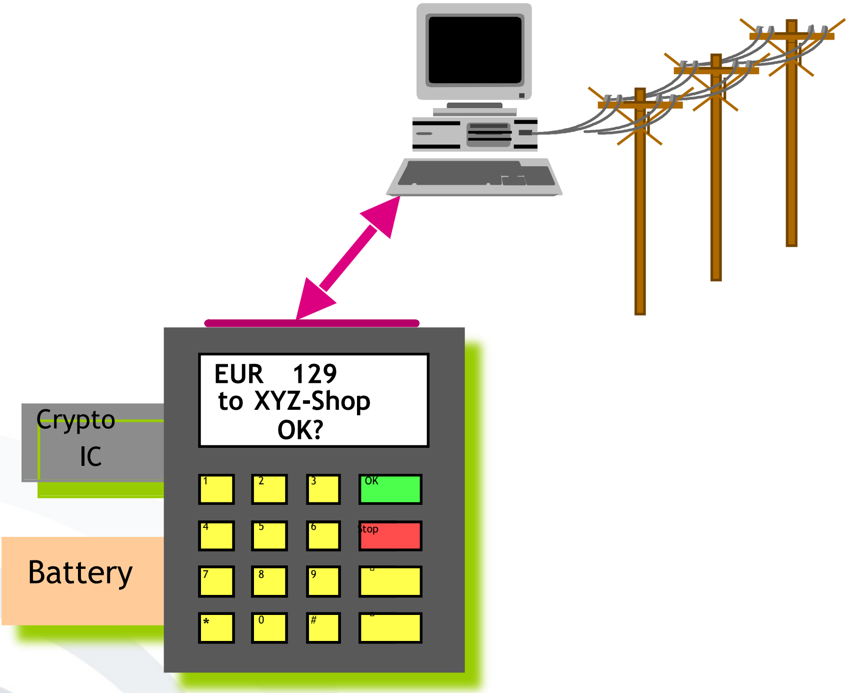


Private key
on HD, in memory



Private key and
signature function in chip card

Secure Equipment: Avoiding Threats from Trojan Horses



Wallet with private key and signature function mobile business

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

↓

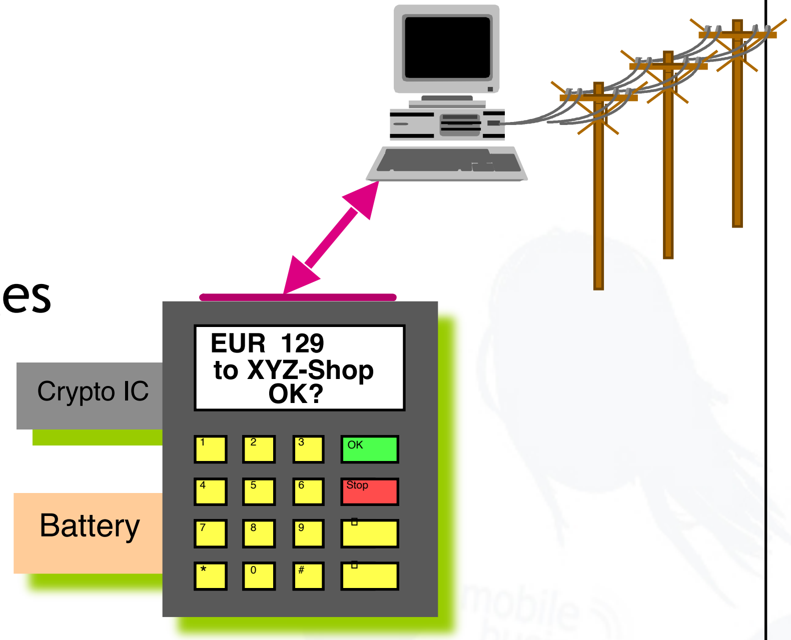
Order

Buyer
Certificate
Date
Description
Total
Currency
Signature

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 (1)

- BNetzA (2015)
  Auflistung beaufsichtiger Zertifizierungsdiensteanbieter und Informationen für Anbieter, www.bundesnetzagentur.de/cln_1421/DE/Service-Funktionen/QualifizierteelektronischeSignatur/WelcheAufgabenhatdieBundesnetzagentur/AufsichtundAkkreditierungvonAnbietern/ZertifizierungsDiensteAnbietr_node.html, accessed 2015-04-13.
- 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.
- EUeIDASregulation(2014),REGULATION(EU)No910/2014 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.
- Fritsch, L. and Roßnagel, H. (2005)
  Die Krise des Signaturmarktes,: Lösungsansätze aus betriebswirtschaftlicher Sicht, in: H. Ferderrath (Eds.): *Sicherheit 2005,* Bonn, Köllen Druck+Verlag GmbH, pp. 315-327.
- Isselhorst/Rohde, BSI.
- Lippmann, S. and Roßnagel, H. (2005)
  Geschäftsmodelle für signaturgesetzkonforme Trust Center, in: O. K. Ferstl; E. J. Sinz; S. Eckert and T. Isselhorst (Eds.): *Wirtschaftsinformatik 2005,* Heidelberg, Physica-Verlag, pp. 1167-1187.

Literature (2)

- 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.
- Roßnagel, H. (2007)
  Mobile Qualifizierte Elektronische Signaturen – Analyse der Hemmnisfaktoren und Gestaltungsvorschläge zur Einführung der qualifizierten elektronischen Signatur.
- Antonius, S CEO TUViT GmbH (2011)
  The recent trend of the personal authentcation environment and “eID” in Germany, Personal Athentication Environment Seminar