

Lecture 8

Application Domains II: (Mobile) Electronic Signatures

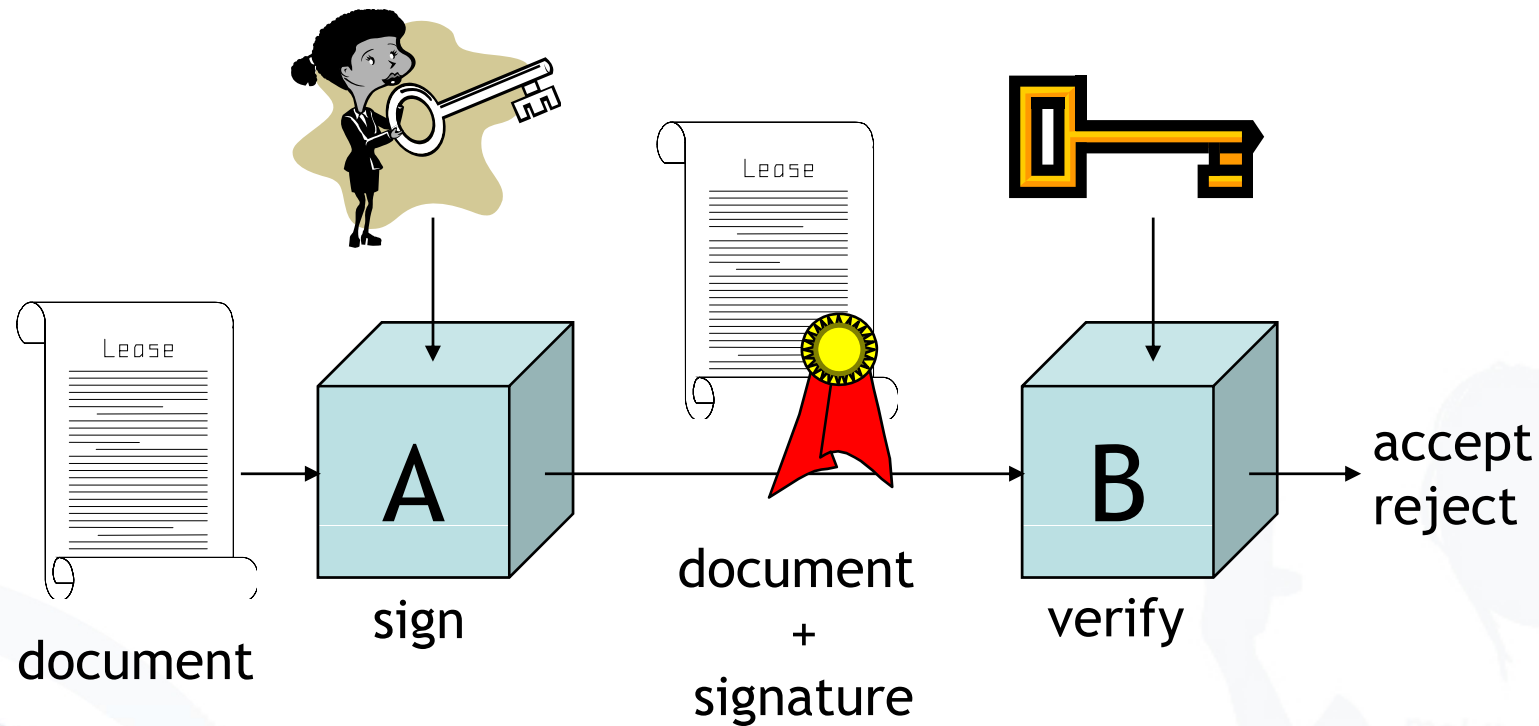


Mobile Business II (SS 2008)

Prof. Dr. Kai Rannenberg

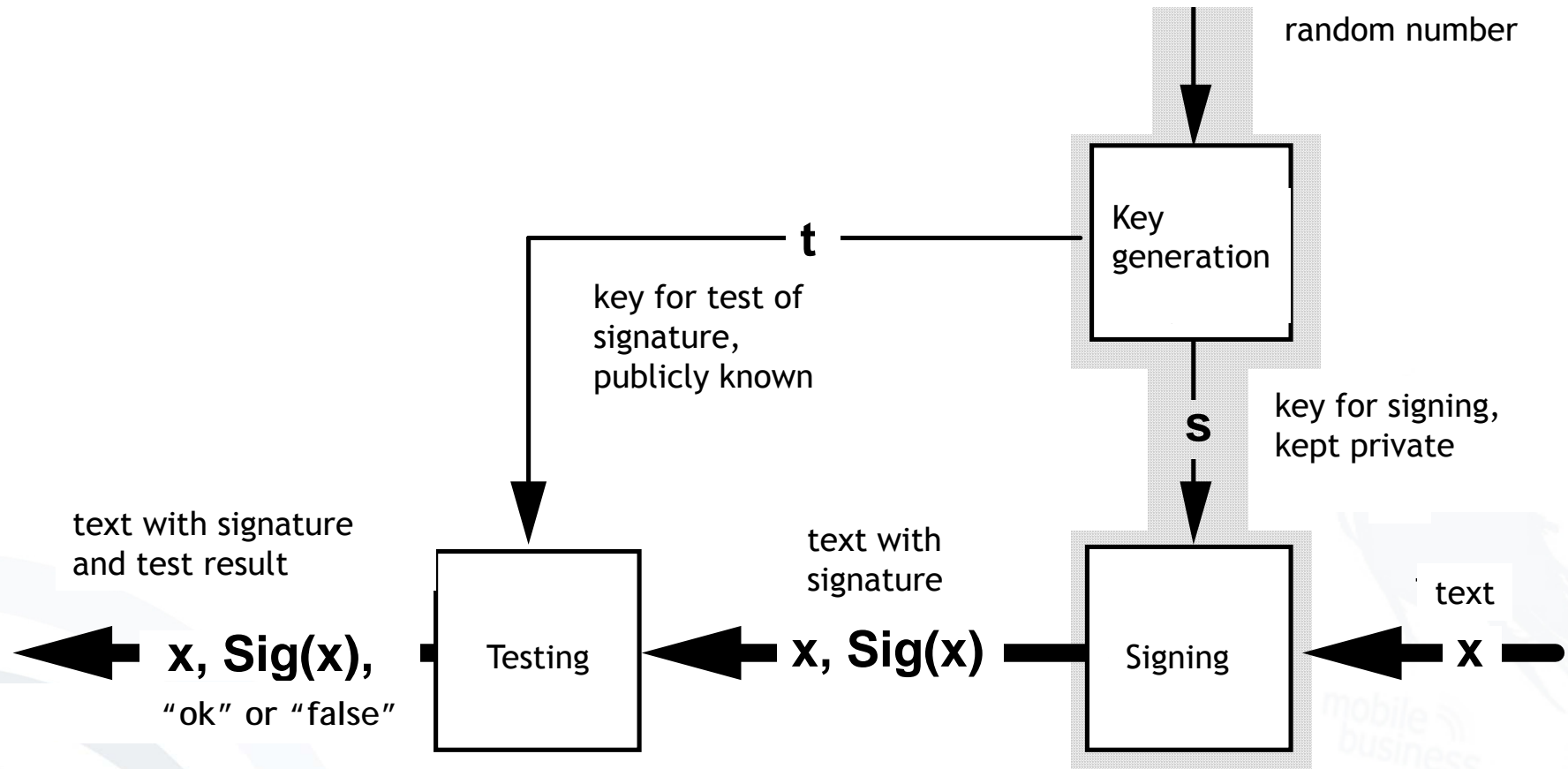
Chair of Mobile Business and Multilateral Security
Johann Wolfgang Goethe-Universität Frankfurt a. M.

- General Concept
- Algorithms
- Legal Framework
- German Signature Market
- Recent Initiatives in Europe
- Mobile Signatures
- New Price Model for electronic signatures
- Secure Display Components and Personal Security Assistants



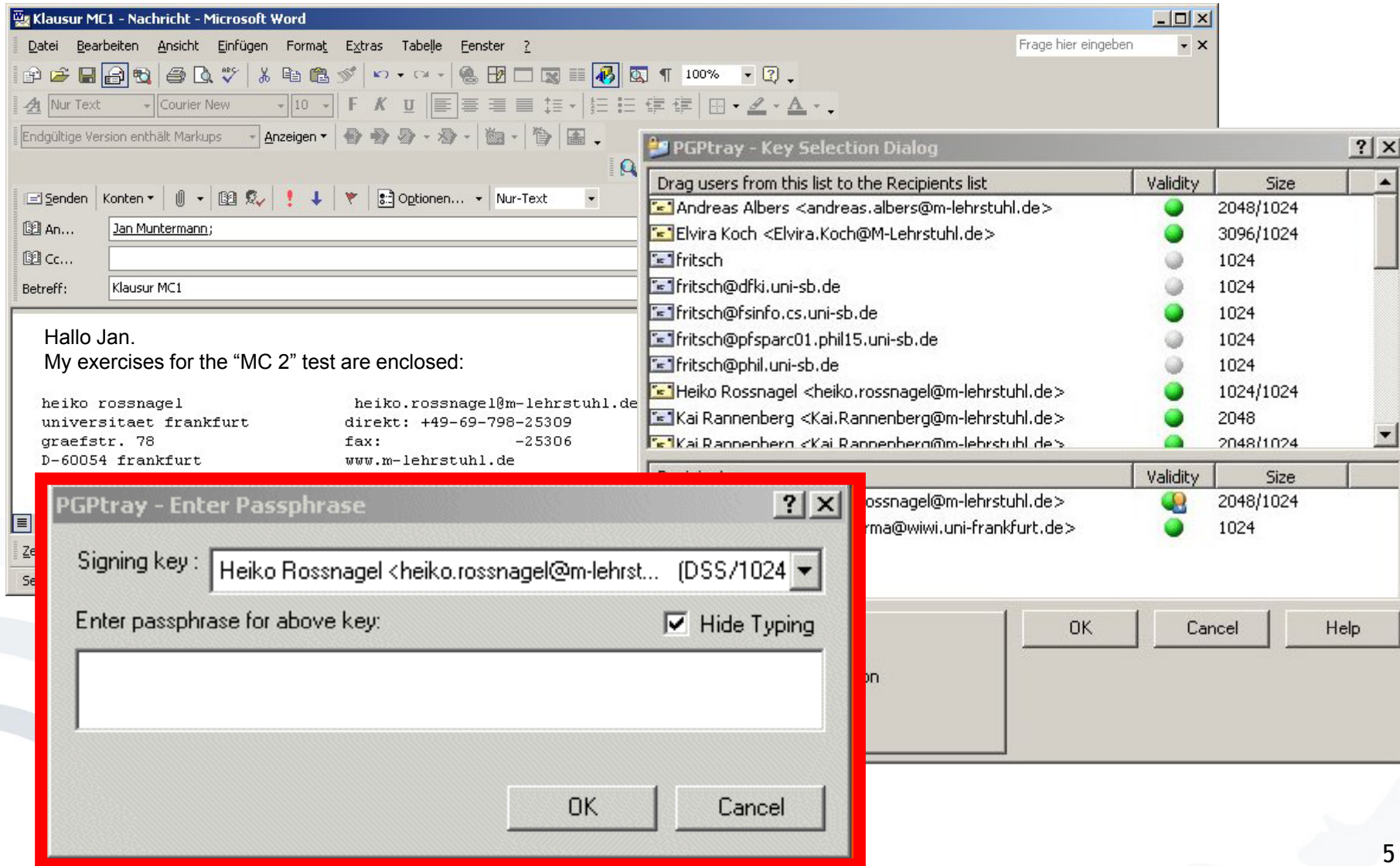
- ➔ Protect the authenticity of documents signed by **A**
- ➔ **B** has to get an authentic copy of **A**'s public key.

Asymmetric Signature System



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

Example PGP: Encrypt and Sign a Message



The screenshot shows a Microsoft Word window titled "Klausur MC1 - Nachricht - Microsoft Word" with a menu bar (Datei, Bearbeiten, Ansicht, Einfügen, Format, Extras, Tabelle, Fenster, ?) and a toolbar. The main text area contains an email composition window with the following details:

- An...:** Jan Muntermann;
- Betreff:** Klausur MC1
- Message Body:**

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
                    
```

Two PGP dialog boxes are overlaid on the email window:

- PGPTray - Key Selection Dialog:** A table with columns "Validity" and "Size". It lists several users for selection.

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 Rannenber <Kai.Rannenber@m-lehrstuhl.de>	●	2048
Kai Rannenber <Kai.Rannenber@m-lehrstuhl.de>	●	2048/1024
- PGPTray - Enter Passphrase:** A dialog box with a red border. It shows "Signing key:" set to "Heiko Rossnagel <heiko.rossnagel@m-lehrst... (DSS/1024)". Below it is a text field for the passphrase and a checked "Hide Typing" checkbox.

Von: Heiko Rossnagel
Betreff: Klausur MC1

An: Jan Muntermann
Cc:

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

hQCMA5/VPPIP3satAQP+LqxvxFSk4G/TAexpMLX436biwBp6xP8pa89R7ro...
uHEs07/tFrJFQJpPbcUWouy47p4sR2FO+IXqJuJyHp5ExMGIdmQCpGXEs2...
B5TXKtUB8YJdpPnck61as78RBP1sq8VDrAlYopEAeqMMw2pkBuoxyo3KCiR...
Ag4DIYlowhVX6ZwQCAD2L9WAA97xEUBWMET6kR9n5+oafTBF+RO1v6UOz2T...
Alkh23iQOI9Drye/uygpcQpT2HhTtZY1AjjudLvi+GsegOlWmBjY8q8G1Y...
kDP3GEanyDiDU6R9F1XF0vxPNMk6Ek8hH6qZ37hhDNDcXkxkSjM3nJ2VuuL...
uOuXNA9iAc96dhg7NpvzCJI2J7xRMtuBc9BUI8LXODrvGLwnLtaD5+EvgL1...
dfvQ3NiGrUEQsOHVxwjQdMtr8C09kREYLuAdD7j/05WtsAdbAVMn72PYFOI...
i77MitBfAbxXF0gFS7/b2LccbaK8fx6e1VNFnVO7B/9qpdOGg5WZVP2eQA5...
h2oTOSjWCRp/v5s9Og1aUtcAxd1RAjQPhVsFS2eXXMn9ZzvNIFMh6Ktqpm...
m39jRjPE9Ob/HLjMwPAXUHyneh9QrCX1X5qHORNcjIYVrnQyZGIk8t39059I...
cr1rhf6ht7SwGgfgGW2aL8HyiFFUQC6niLzIFmzif6uLzif692Tz43CPd...
E1IJGt9QLiwMmXormxcOg+WR2I...
NjwR+1SkqMCXs+PzcAHDsiuGz...
pE3huhK5cfvu1Ug7+Oa9SUay4J...
NZncI3vJgkZeZr1bh+pi4dRjs0...
=hCO9

-----END PGP MESSAGE-----

heiko rossnagel
frankfurt direkt:
-25306 D-60054 frankfurt

PGP Message Content:

```
*** 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 ***
```

PGP Tray Dialog:

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

OK Cancel

Text Viewer Dialog:

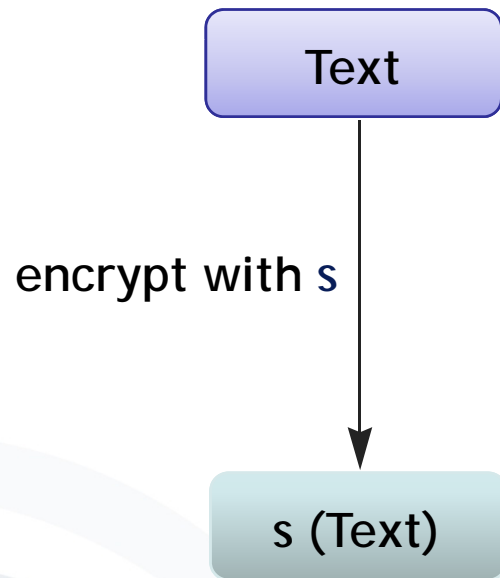
Copy to Clipboard OK

- General Concept
- Algorithms
- Legal Framework
- German Signature Market
- Recent Initiatives in Europe
- Mobile Signatures
- New Price Model for electronic signatures
- Secure Display Components and Personal Security Assistants

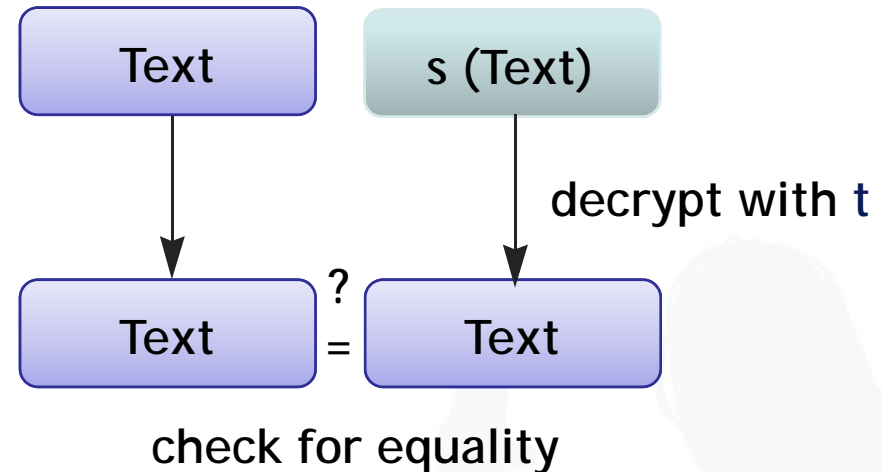
- **RSA: Rivest, Shamir, Adleman**
 - Asymmetric encryption system which also can be used as a signature system via “inverted use”,
 - Message encrypted with the private key (= signing key) gives the signature,
 - Decoding with the public key (=testing key) has to produce the message.

[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.

Sender / Signer

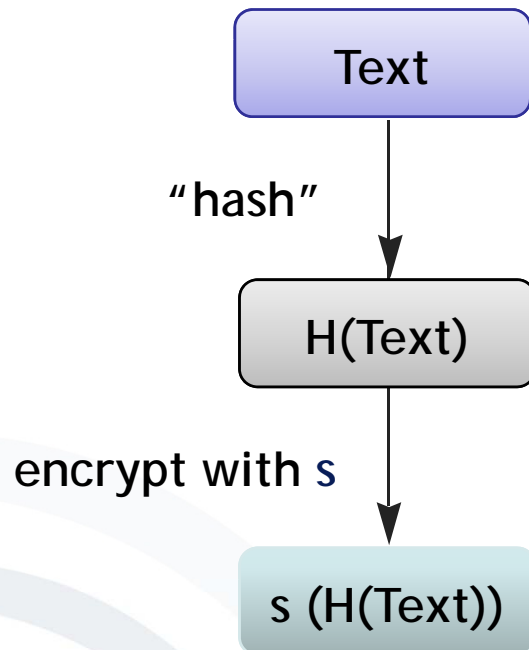


Addressee / Verifier

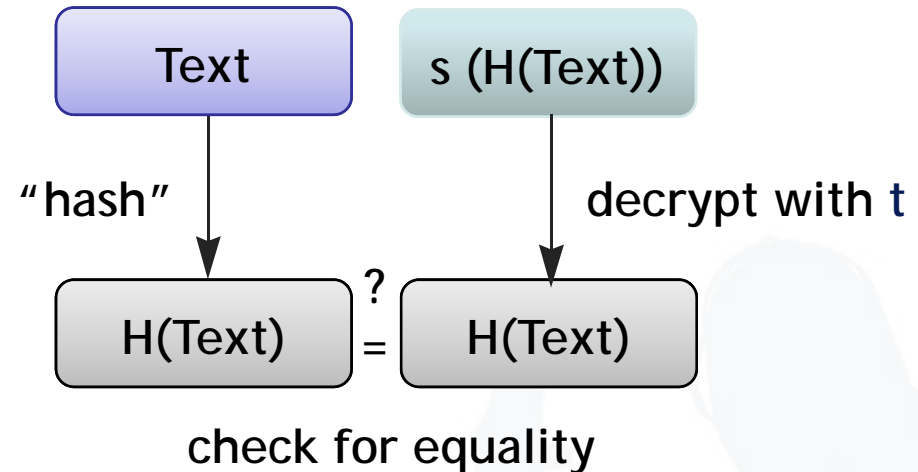


- ➔ Signing key s only with the sender, test key t public
- ➔ Example is often mistakenly generalized.

Sender / Signer



Addressee / Verifier



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

- 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 $H(s_1) = H(s_2)$.
 - Examples: SHA-1, MD5, MD4

- General Concept
- Algorithms
- Legal Framework
- German Signature Market
- Recent Initiatives in Europe
- Mobile Signatures
- New Price Model for electronic signatures
- Secure Display Components and Personal Security Assistants

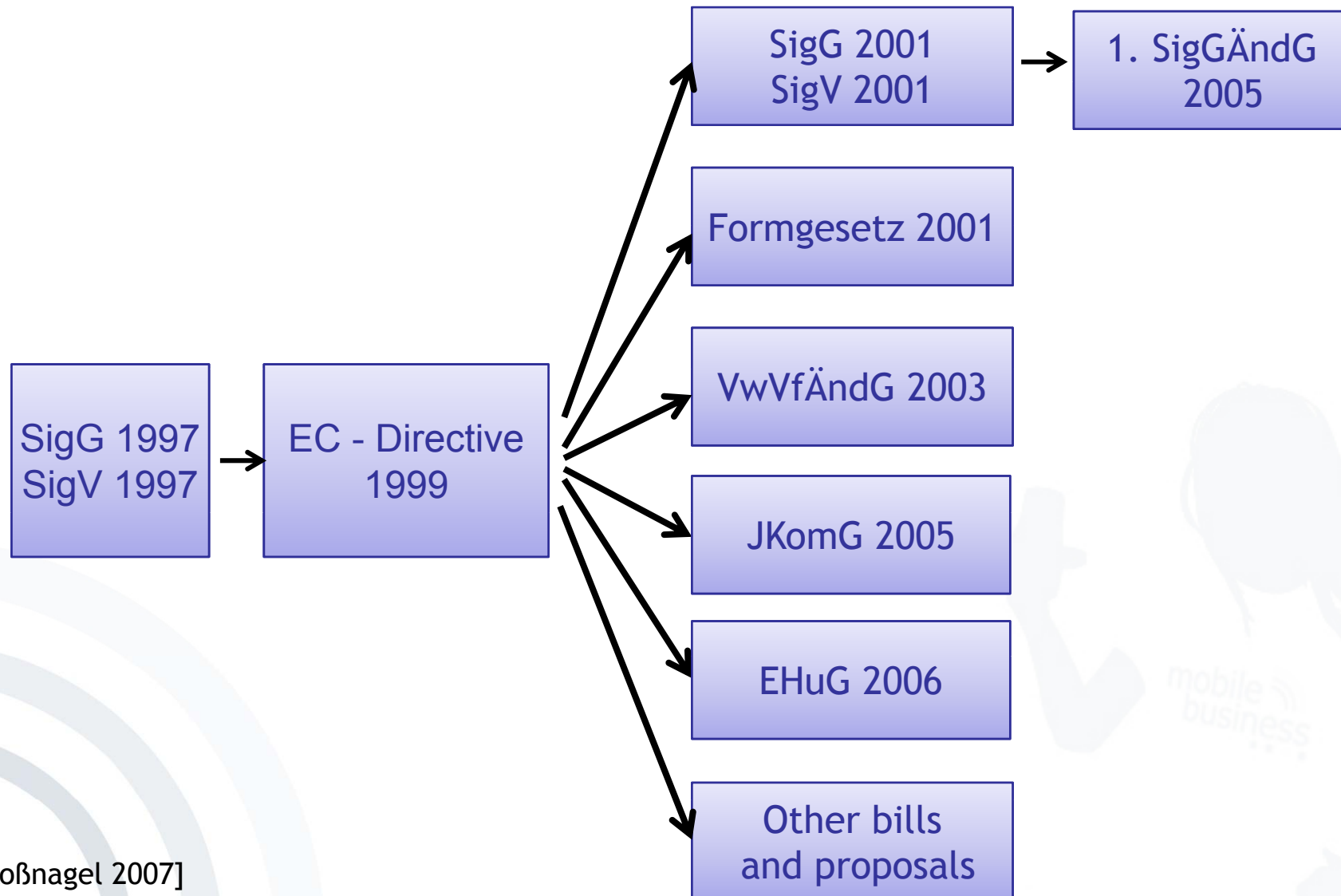
First version in 1997 as Article 3 of the IuKDG
“Informations- und Kommunikationsdienste-Gesetz”

- Excerpt from the text:

“ § 1 Zweck und Anwendungsbereich ”

(1) Zweck des Gesetzes ist es Rahmenbedingungen für digitale Signaturen zu schaffen, unter denen diese als sicher gelten und Fälschungen digitaler Signaturen oder Verfälschungen von signierten Daten zuverlässig festgestellt werden können.

- NB: The legal status of electronic signatures will be defined in sector specific regulation, e.g. the „Bürgerliches Gesetzbuch (BGB) for general commercial contracts“.



- 1.SigÄndG 1. Signaturänderungsgesetz
- EC-Directive Directive 1999/93/EC
- EHuG Gesetz über elektronische Handelsregister und Genossenschaftsregister sowie das Unternehmensregister
- JKomG Justizkommunikationsgesetz
- SigG Signaturgesetz
- SigV Signaturverordnung
- VwVfÄndG Gesetz zur Änderung verwaltungsverfahrenrechtlicher Vorschriften

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

The signature component must:

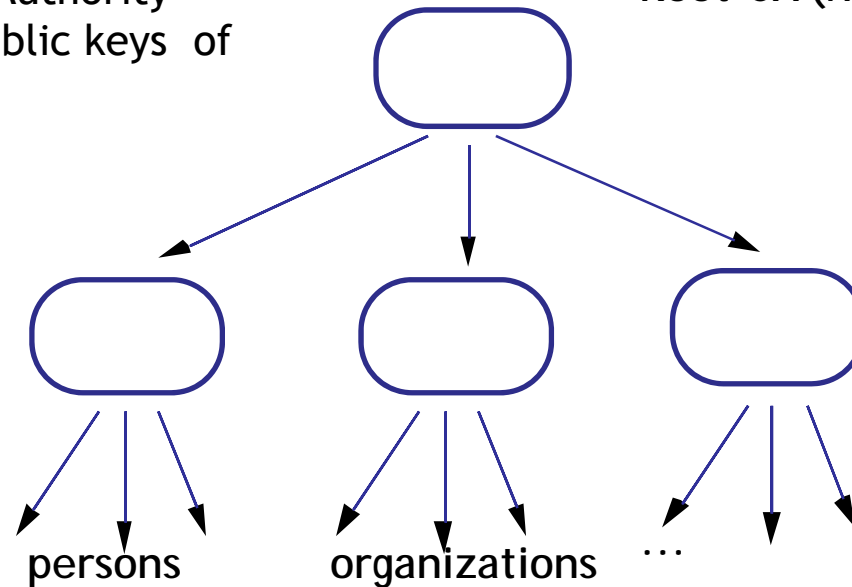
- Clearly notify the signer that a signature is created *before* the signature is created
- Make clearly perceptible which data the signature refers to
- Secure the accordance of displayed data and signed data (“What you see is what you sign.”)

Hierarchical Certification of Public Keys

(Example: German Signature Law)

Regulatory Authority
confirms public keys of
the CAs

Root-CA (Regulatory Authority)



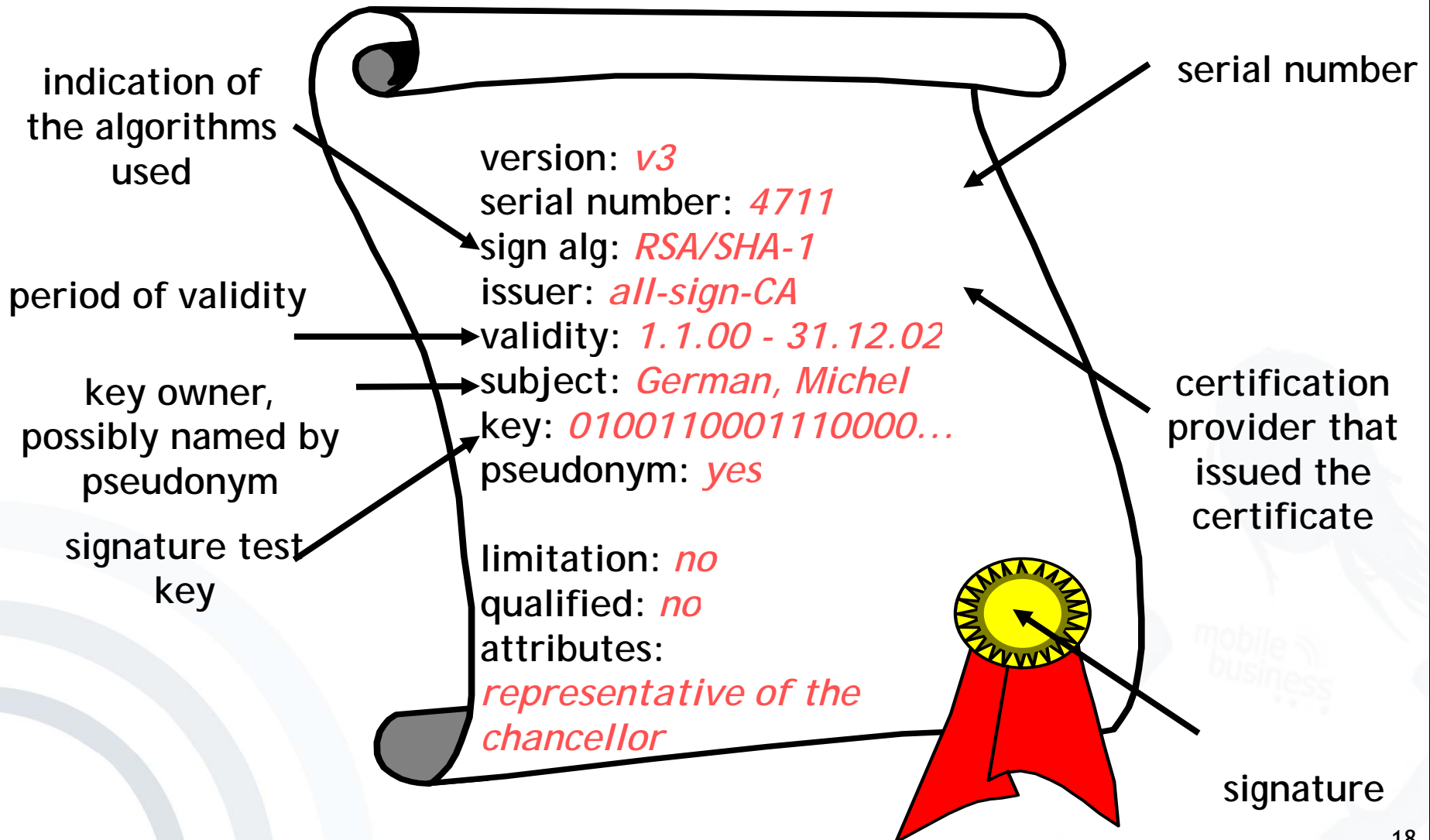
Certification
Authorities (CA)

TeleSec, D-Trust,
TC TrustCenter, ...

- 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)



- 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

- 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

- General Concept
- Algorithms
- Legal Framework
- German Signature Market
- Recent Initiatives in Europe
- Mobile Signatures
- New Price Model for electronic signatures
- Secure Display Components and Personal Security Assistants

- Legal and technical framework exists for years.
 - So far qualified electronic signatures are not successful in the market.
 - Only 30.000 certificates have been issued in Germany until January 2004.
- ➔ Expectations have not been fulfilled.

	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

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

- General Concept
- Algorithms
- Legal Framework
- German Signature Market
- Recent Initiatives in Europe
- Mobile Signatures
- New Price Model for electronic signatures
- Secure Display Components and Personal Security Assistants

- In Germany:
 - “Gesundheitskarte“
 - “Job card“
 - “Digitaler Personalausweis“
- In Austria:
 - “Bürgerkarte“
 - A1 Signature
- In Belgium:
 - Belgium eID Card (BELPIC)
- In Finland:
 - Universal eID Card
 - Mobile Signatures
- In Denmark:
 - OCES (“Offentlige Certifikater til Elektronisk Service“)
- And many more...

- All initiatives focus on high penetration rate of signature capable smart cards within the complete population.
- But high penetration rate of smart cards does not necessarily lead to adoption of electronic signatures
 - E.g. German “Geldkarte”
- Specific targeting of early adopters might be more successful.

- General Concept
- Algorithms
- Legal Framework
- German Signature Market
- Recent Initiatives in Europe
- Mobile Signatures
- New Price Model for electronic signatures
- Secure Display Components and Personal Security Assistants

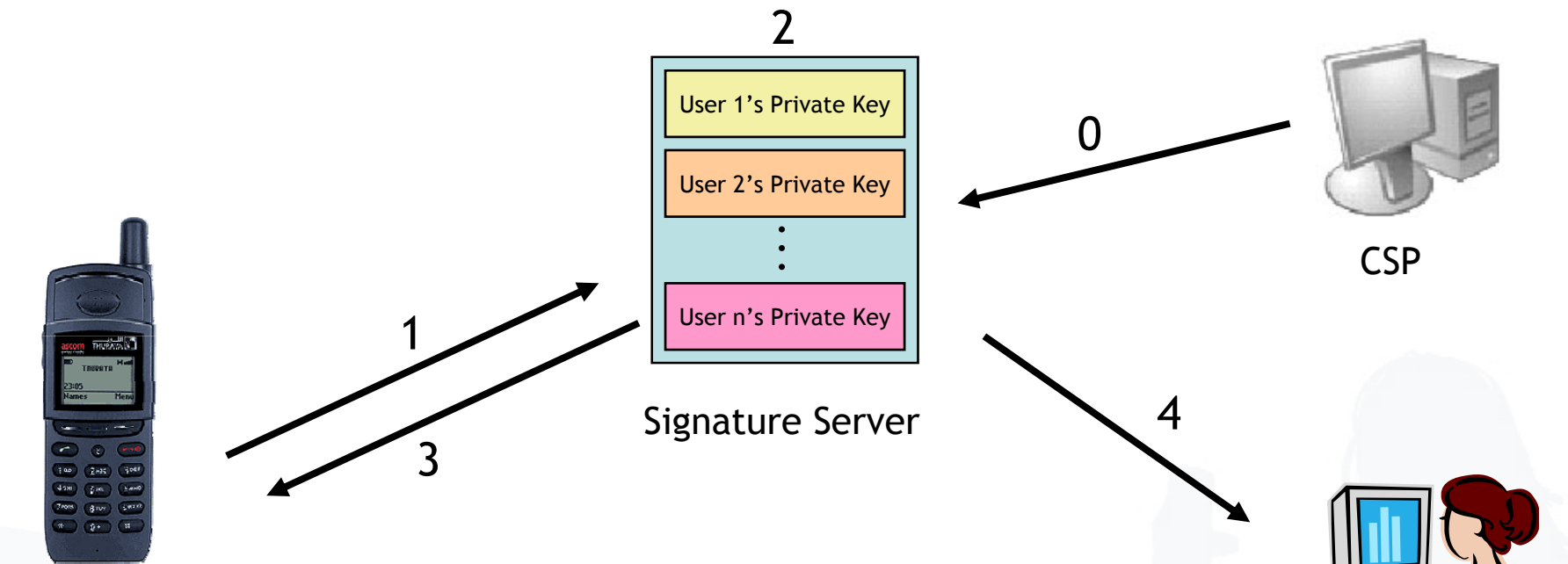
- Advanced electronic signatures:
 - Uniquely linked to the signatory
 - Capable of identifying the signatory
 - Created using means that the signatory maintains under his sole control
 - Linked to the data to which it relates in such a manner that any subsequent change of the data is detectable

- Qualified certificates:
 - Can be issued for advanced signatures by CSPs if they meet the requirements of Annex I of the EC Directive

- 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.

- 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.

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]

- Private key is under control of server.
 - This violates article 2,2 (c) of EC directive for advanced signatures:
“...by means the signatory can maintain under his
sole control.”
- Infrastructure to enforce secure authorization of server signatures has high complexity.

Use of separate smart cards for telephony and signature:

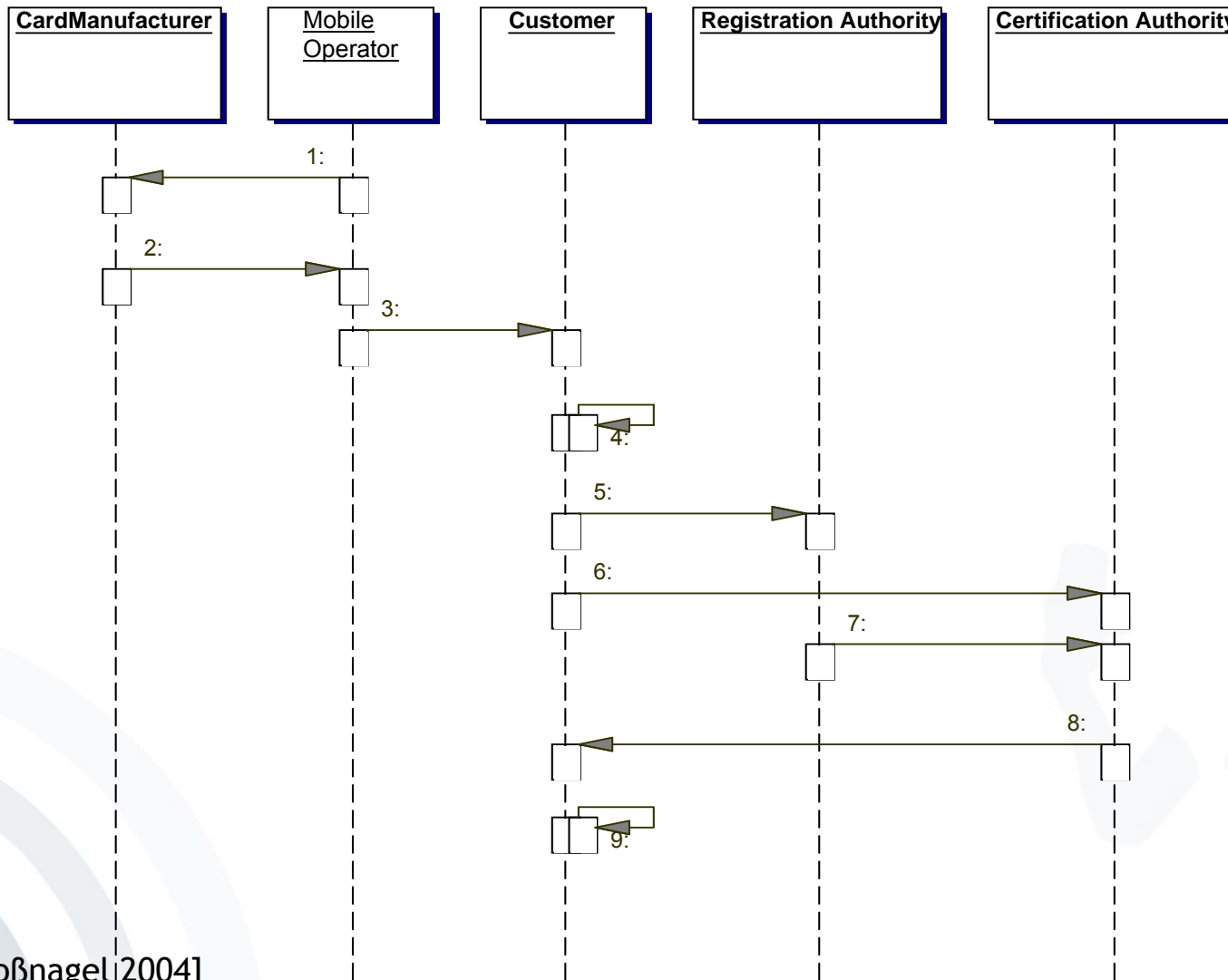
- Dual Card
Exchange of SIM against Secure Signature Creation Device (SSCD)
- Dual Slot
Mobile device carries two card readers for SIM and SSCD



- 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!

- 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.

- 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]

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

- 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

- 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 Phone are becoming open platforms
 - A trusted device is necessary (➔ TCG/Perseus)

- General Concept
- Algorithms
- Legal Framework
- German Signature Market
- Recent Initiatives in Europe
- Mobile Signatures
- New Price Model for electronic signatures
- Secure Display Components and Personal Security Assistants

- Improvement of distribution of costs and benefits through:
 - Market segmentation
 - Transaction-based billing for signature verification
 - Combination with significant smaller fixed annual fee
 - Price discrimination

Target Group	Tariff	Instalment Costs	Fixed Fee	Verification
(cons.) Private Customers	Starter	15 €	0 €	0,4 €
(prog.) Private Customers	Independence	0 €	15 €	0,25 €
Companies	Customer ¹	0 €	60 €	0,25 €
Public Administration	Public	0 €	60 €	0,05 €
Companies/ Administration	Business	0 €	30 €	0,1 €
Companies/ Administration	Flat rate	0 €	85 €	0 €

[1] This tariff offers cost free verification of the companies' certificates to their customers

[Lippmann and Roßnagel 2005]

Tariff	No. of Customers	Income based on fixed Annual Fee
Starter	1.260.000	6.300.000 €
Independence	758.000	11.370.000 €
Customer	10.000	600.000 €
Public	10.000	600.000 €
Business	10.000	300.000 €
Flatrate	10.000	850.000 €
Total	2.028.000	20.020.000 €

Purchases (2.028.000 * 5 €)	10.140.000,00 €
Personnel	2.022.274,76 €
Deprecation of immaterial goods	811.166,03 €
Other operating costs	1.537.591.89 €
Interest fees and similar costs	656.764.71 €
Total costs	15.167.797, 39 €

- General Concept
- Algorithms
- Legal Framework
- German Signature Market
- Recent Initiatives in Europe
- Mobile Signatures
- New Price Model for electronic signatures
- Secure Display Components and Personal Security Assistants



Mr. Schulz

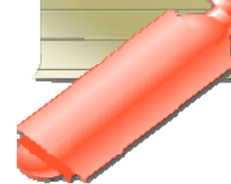
Winword document
Receipt for Ms. Meier:
Ms. Meier has paid
100.000 ,- € to Mr. Schulz.
Schulz



Mrs. Meier



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



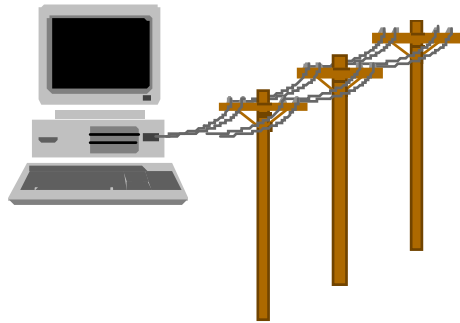
But check for hidden text !!!!

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

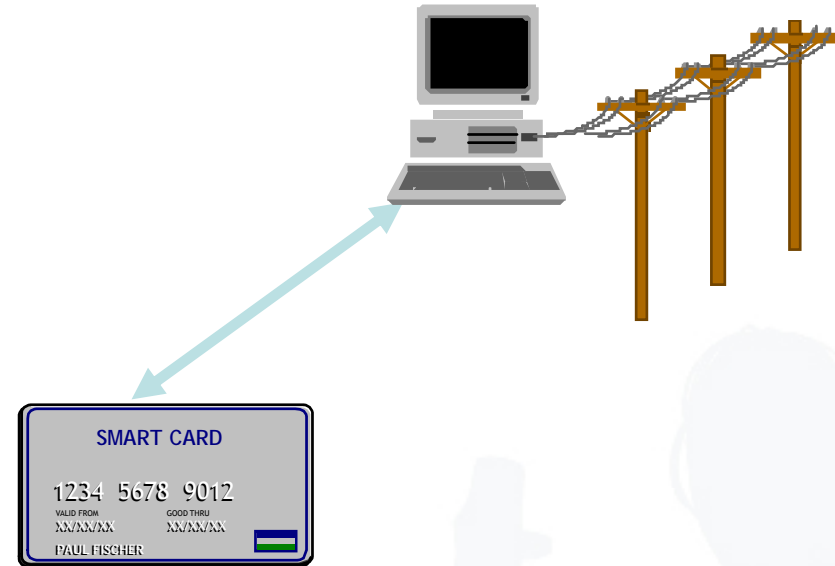
The signature component must:

- 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

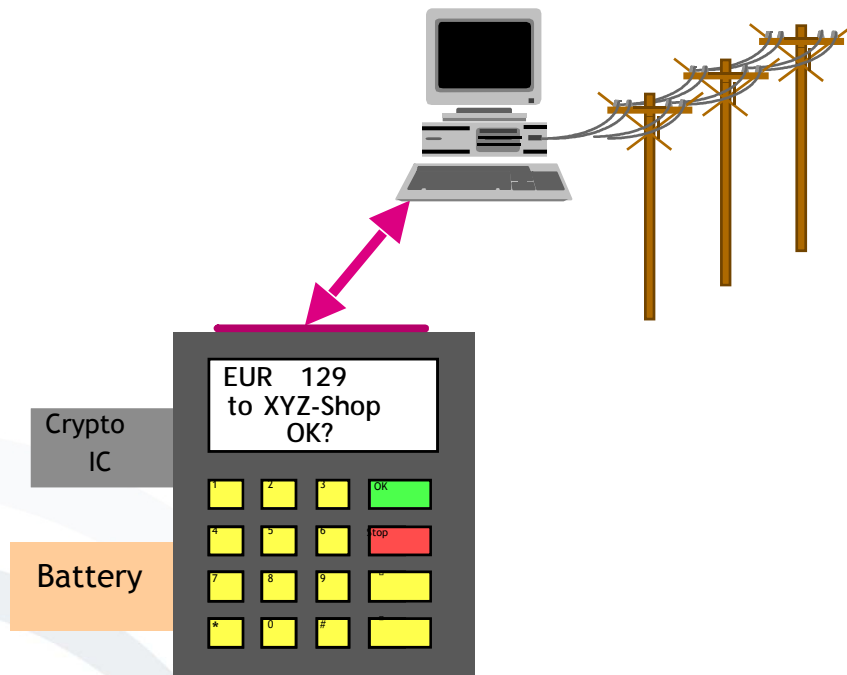


Private key
on HD, in memory



Private key and
signature function in chip card

Secure Equipment: Avoiding Threats from Trojan Horses



Wallet with private key and signature function

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

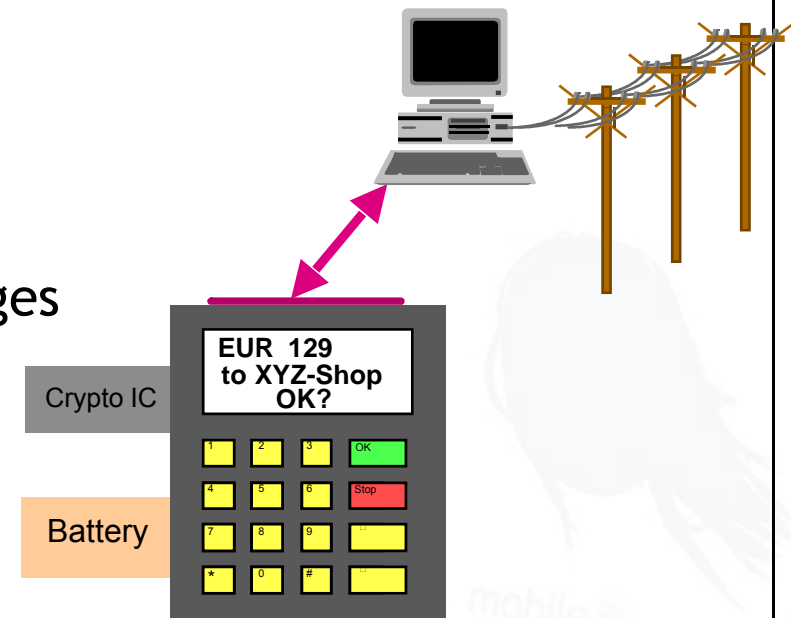
Total

Currency

Signature

A popular vision: Security Assistants

- Storing personal data
 - Addresses, calendars
 - Money, keys
 - Preferences ...
- Performs sensitive processes
 - Decoding of confidential messages
 - Signature creation
 - Contract confirmation
- 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 saved 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 digital assistants
- Mobile phones
- Watches
- Pens
- Chip cards
- ...



- 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.
- 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.
- 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.