

Lecture 5

Application Domains III: (Mobile) Electronic Signatures

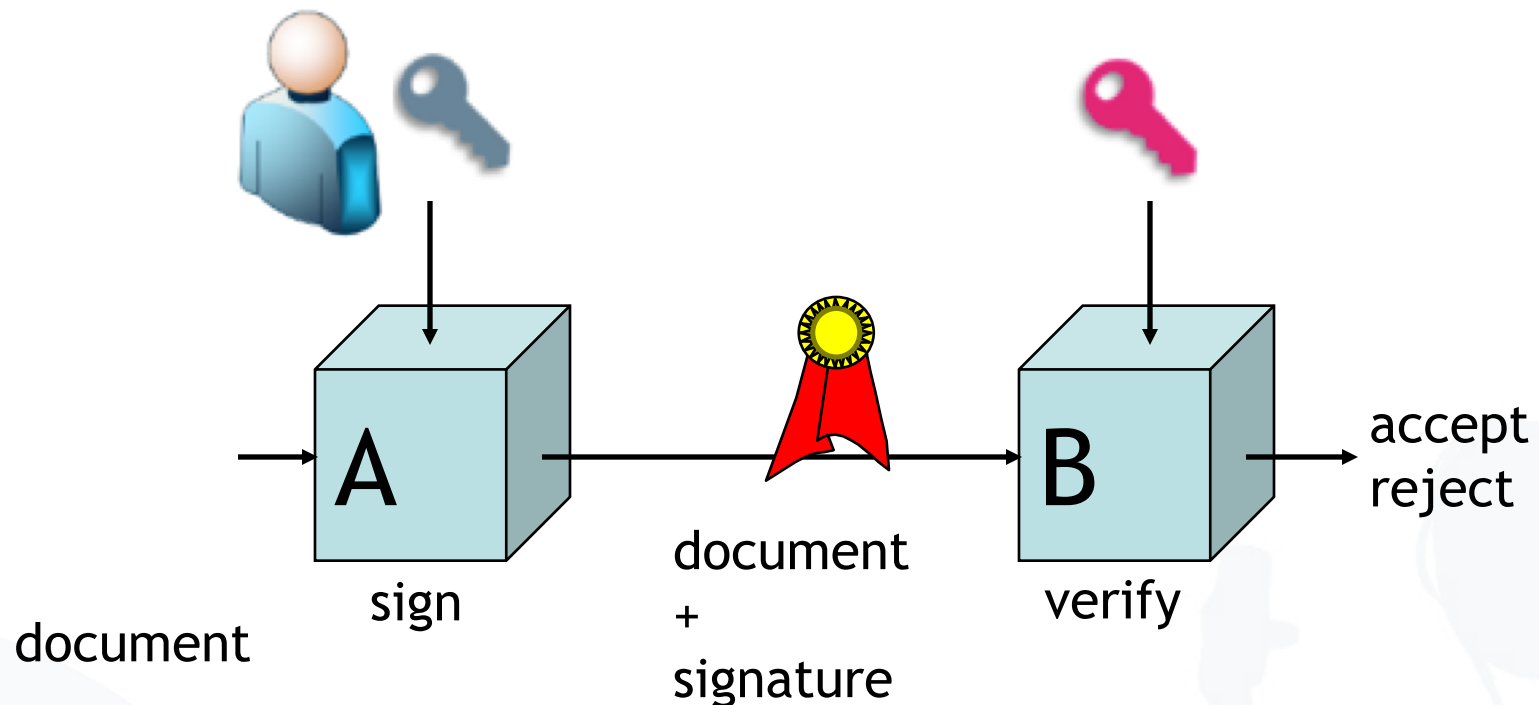


Mobile Business II (SS 2023)

Prof. Dr. Kai Rannenberg

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

- General Concept & Applications
- Algorithms
- Legal Framework
- Mobile Signatures
- Secure Display Components and Personal Security Assistants
- Wallets
- Annexes



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

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.



ELSTER Ihr Online-Finanzamt

Hilfe Suchen

[Benutzerkonto erstellen](#) [Login](#)

Meine Steuer mach ich online!*

Noch nicht registriert? [Benutzerkonto erstellen](#) Mein ELSTER [jetzt einloggen](#)

✓ Ohne Ausdrucke und Postversand ✓ Kein Herunterladen und Installieren ✓ Auch auf Tablet und Smartphone ✓ Kostenloser Service aller Finanzämter

ELSTER

- Mein ELSTER
- Formulare & Leistungen
- Benutzergruppen
- Benutzerkonto-Service
- Weitere Softwareprodukte

Was kann ich hier machen?
Formulare, Profile, Steuerkonsultation, Belegabruf

Leistungen >

Für wen ist ELSTER?
Privatpersonen, Arbeitgeber, Unternehmer, Vereine, steuerberatende Berufe

Benutzergruppen >

Wie finde ich Hilfe?
Hilfelines, Info-Assistent, ELSTER-Hotline, ELSTER Anwender Forum

Hilfe >

Neues

Neue Formulare für den Veranlagungszeitraum 2016:

- Körperschaftsteuererklärung (KSt 1 A/B/C)

ElsterOnline-Portal wird zu Mein ELSTER

- bisheriger Funktionsumfang bleibt vollständig erhalten
- bereits registrierte Nutzer müssen sich nicht neu registrieren

weitere geplante Release- und Bereitstellungstermine

Belegabruf - Vorausgefüllte Steuererklärung

- kostenloses Serviceangebot der Steuerverwaltung
- elektronische Bereitstellung der gespeicherten Daten/Belege bei der Steuerverwaltung
- Abruf der Daten/Belege in Mein ELSTER und Übernahme in ihre Einkommensteuererklärung

[Belegabruf](#)

Schon gewusst?

Mit dem neuen Personalausweis, können Sie sich schnell und bequem für ein Konto registrieren. In wenigen Klicks erhalten Sie ein Konto und können Ihre Steuerdaten eingeben.

ElsterFormular
Das Steuerprogramm - eine Alternative zu Mein ELSTER

- herunterladen und installieren
- Offline bearbeiten und elektronisch übernehmen
- kostenlos

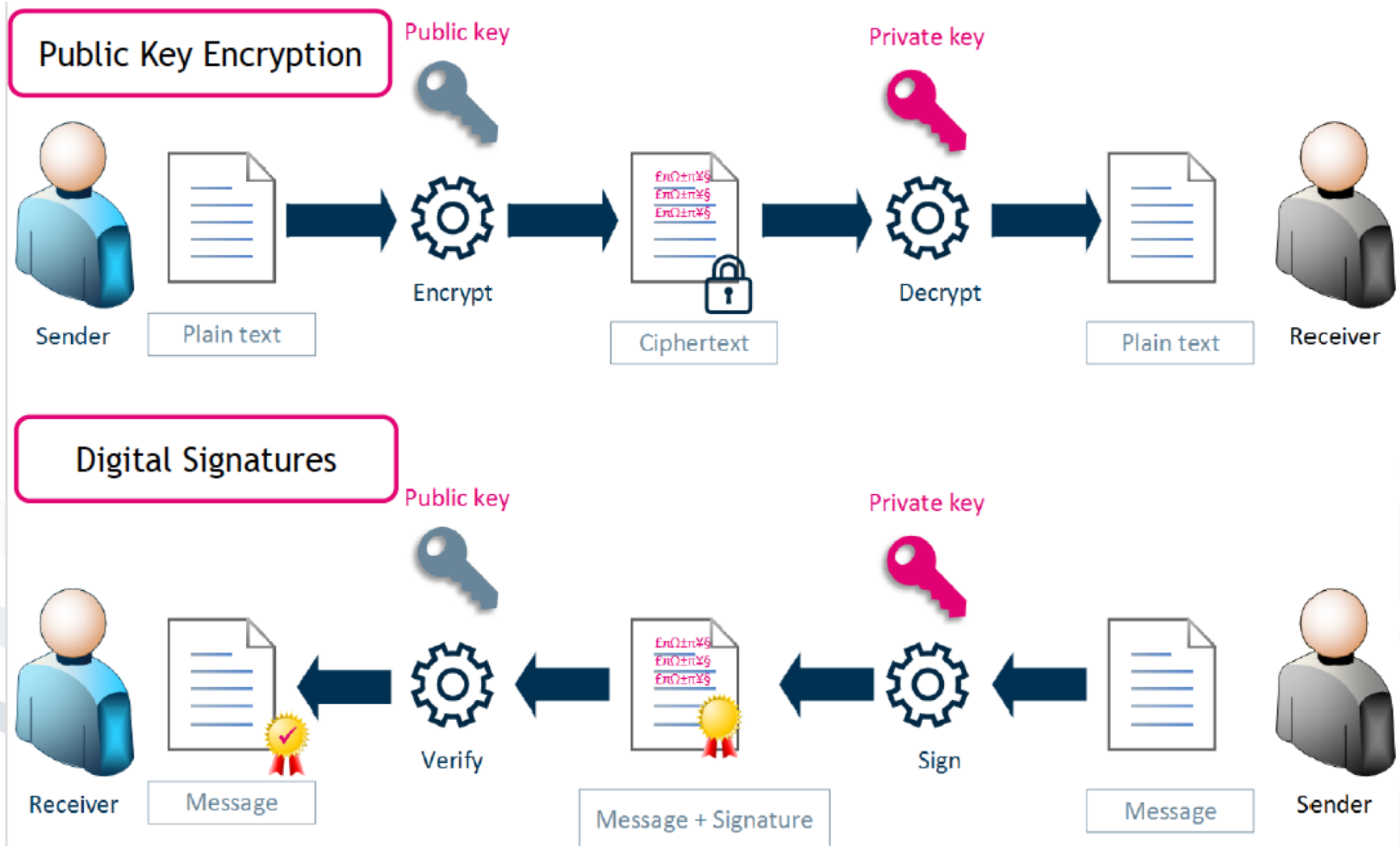
[Zum Download](#)



<https://insights.mgm-tp.com/de/elster-de-bringt-als-relaunch-des-elsteronline-portals-ein-neues-design-und-unterstuetzung-fuer-mobile-geraete/>

<https://wesignature.com/industries/banking/>

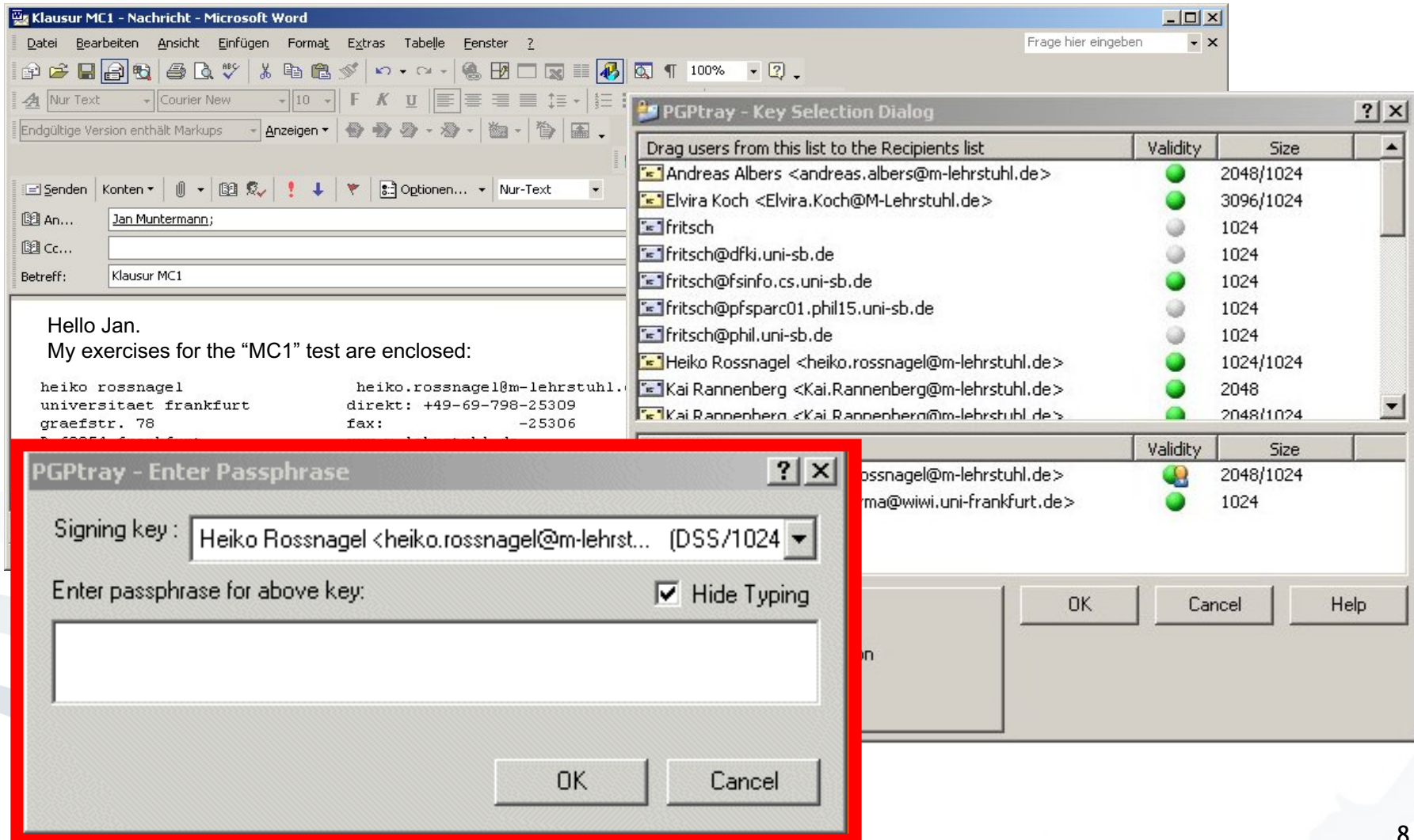
Asymmetric Signature System



Asymmetric Signature system

Digital signatures	Public-key Encryption
The holder of the private key (sender) signs the message.	“Anyone” can encrypt a message.
“Anyone” 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

Von: Heiko Rossnagel
Betreff: Klausur MC1

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

hQCMA5/VPPI3satAQP+LqxvxFSk4G/TAexpMLX436biwBp6xP8pa89R7ro5Z
uHEs07/tFrJFQJpPBcUWouy47p4sR2FO+IXqJuJyHp5ExMGIdmQCpGXEOs2I
B5TXKtUB8YJdpPnck61as78RBP1sq8VDrAlYopEAeqMMw2pkBuoxyo3KCiRk
Ag4DIYlowhVX6ZwQCAD2L9WAA97xEUBWMET6kR9n5+oafTBF+R0lv6UOz2TO
Alkh23iQ0LI9Drye/uygpcQpT2HhTtZY1AjjudLvi+GsegOlWmBjY8q8G1Y6
kDP3GEanyDiDU6R9F1XFOvxPNMk6Ek8hH6qZ37hhDNDcXkxkSjM3nJ2VuuLv
uOuXNA9iAC96dhg7NpvzCJI2J7xRMtuBc9BUI8LXODrvGLwnLtaD5+EvgL1x7
dfvQ3NiGrUEQs0HVxwjQdMtr8C09kREYLuAdD7j/05WtsAdbAVMn72PYFOIR
i77MitBfAbxXF0gFS7/b2LccbaK8fx6e1VNFNVO7B/9qpdOGg5WZVP2eQA5fk
h2oTOSjWCRp/v5s9Og1aUtcAxc
m39jRjPE9Ob/HLjMwPAXUHyne
cr1rhf6ht7SwGgfgGW2aL8HyiF
E1IJGt9QLiWmXormxcOg+WR21
Njwtr+1SkqMCXs+PzcAHDsiuG2
pE3huhK5cfvu1Ug7+Oa9SUAY4J
NZncI3vJgkZeZrlbh+pi4dRjsC
=hCO9

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

heiko rossnagel
frankfurt direkt:
-25306 D-60054 frankfurt

PGPTray - Enter Passphrase

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

Text Viewer

*** 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 ***

Hello Jan.

My exercises for the "MC1" test are enclosed:

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

- General Concept & Applications
- Algorithms
- Legal Framework
- Mobile Signatures
- Secure Display Components and Personal Security Assistants
- Wallets
- Annexes

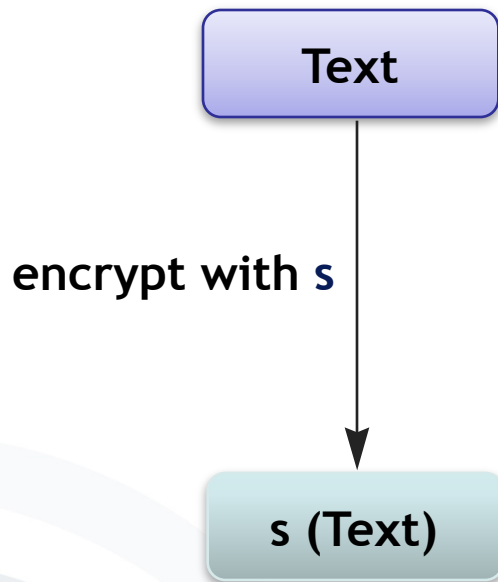
- **RSA: Rivest, Shamir, Adleman**
 - Asymmetric encryption system which also can be used as a signature system via “inverted use”,
 - Message encrypted with the private key (= signing key) gives the signature,
 - Decoding with the public key (=testing key) has to produce the message.

[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.

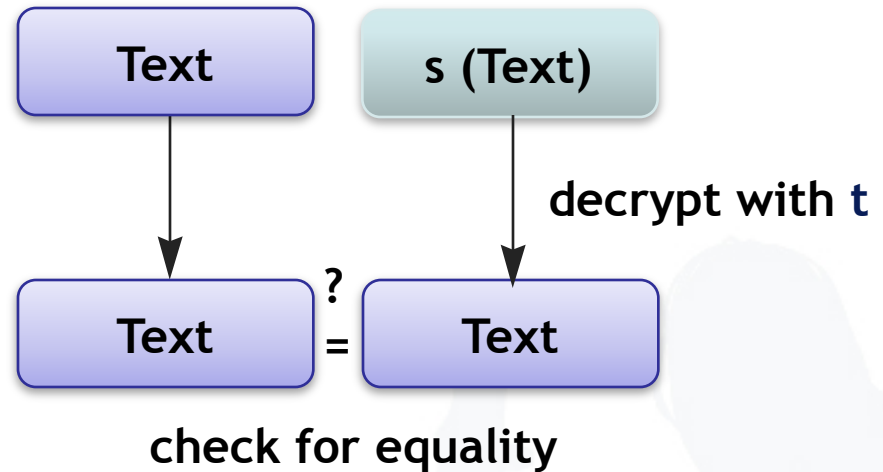
Algorithm	Algorithm family
RSA	Integer factorization
Digital Signature Algorithm (DSA)	Discrete logarithm
Elliptic Curve Digital Signature Algorithm (ECDSA)	Elliptic curves

Asymmetric Signature System (Simplified Example RSA)

Sender / Signer



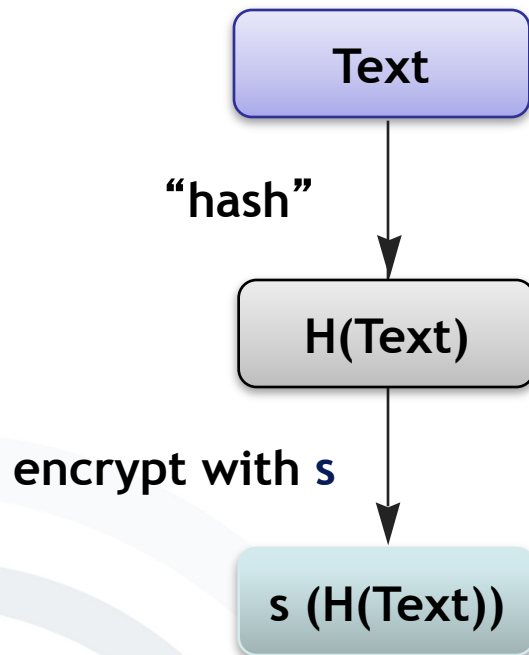
Addressee / Verifier



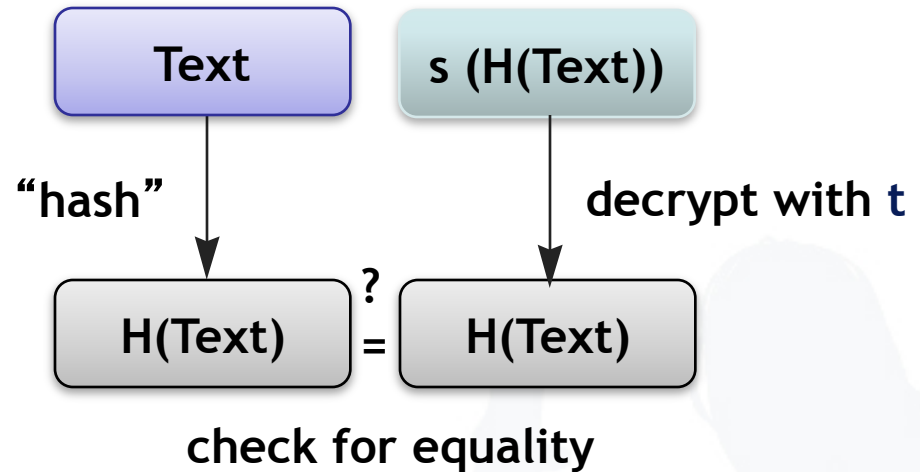
- ➔ Signing key **s** only with the sender, test key **t** public
- ➔ Example is often mistakenly generalized.

Asymmetric Signature System (Example RSA)

Sender / Signer



Addressee / Verifier



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

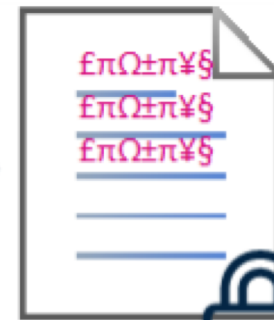
One way cryptography



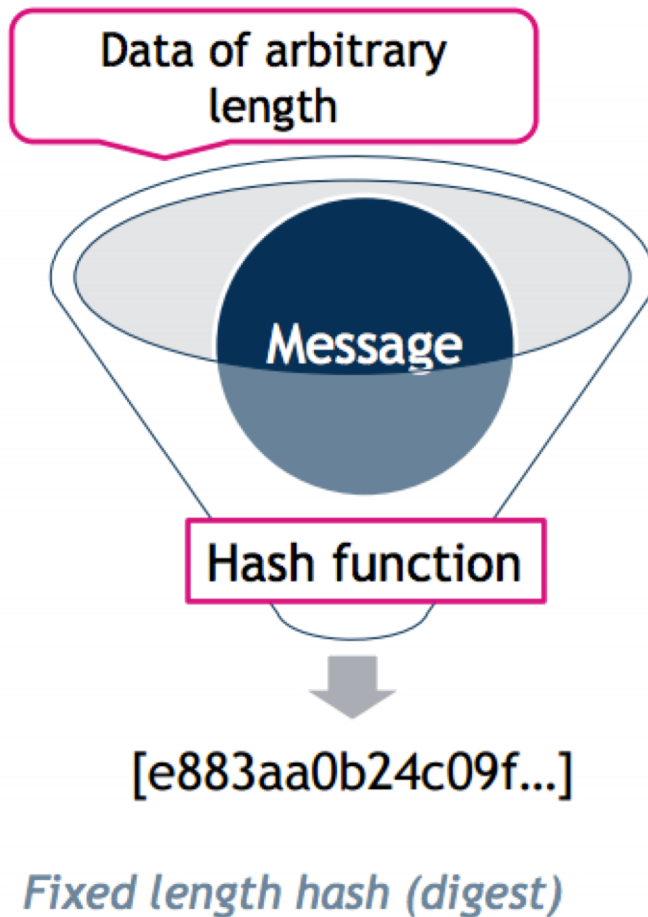
Plain text



Hash function



Ciphertext



General hash functions

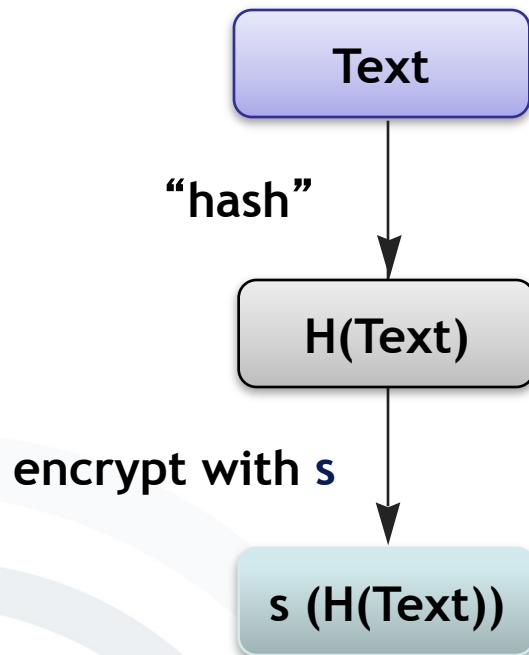
$(H(s))$

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

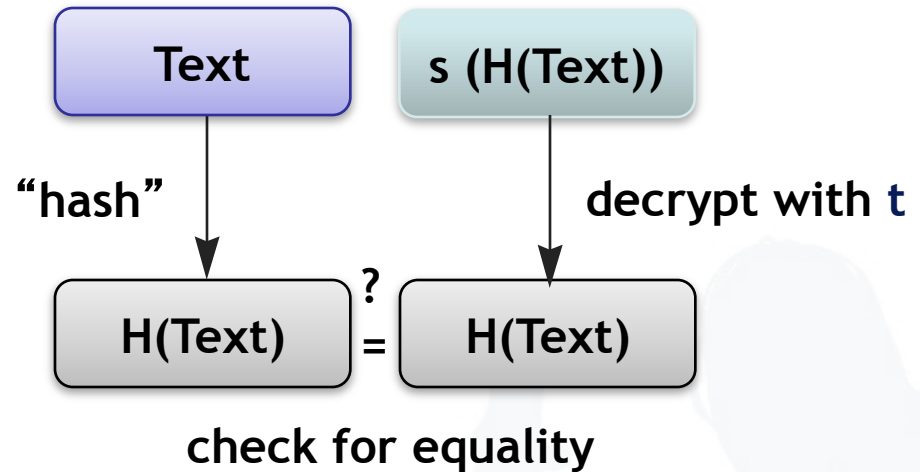
Example: mod 10 in the decimal system

Asymmetric Signature System (Example RSA)

Sender / Signer



Addressee / Verifier



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

- General Concept & Applications
- Algorithms
- Legal Framework
- Mobile Signatures
- Secure Display Components and Personal Security Assistants
- Wallets
- Annexes

- 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"

- The Confidence Services Law (VDG) implements the EU REGULATION (EU) No 910/2014 on electronic signatures in Part 3 (qualified electronic signatures and seals).

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]

▪ 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.

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

The signature component must:

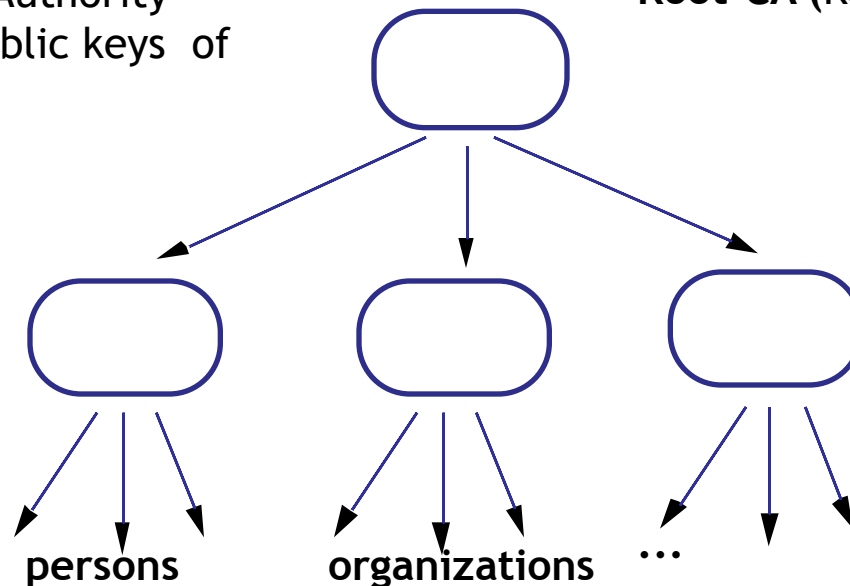
- Clearly notify the signer that a signature is to be created *before* the signature is created
- Make clearly perceptible which data the signature refers to
- Secure the accordance of displayed data and signed data (“What you see is what you sign.”)

Hierarchical Certification of Public Keys

(Example: German Signature Law)

Regulatory Authority
confirms public keys of
the CAs

Root-CA (Regulatory Authority)



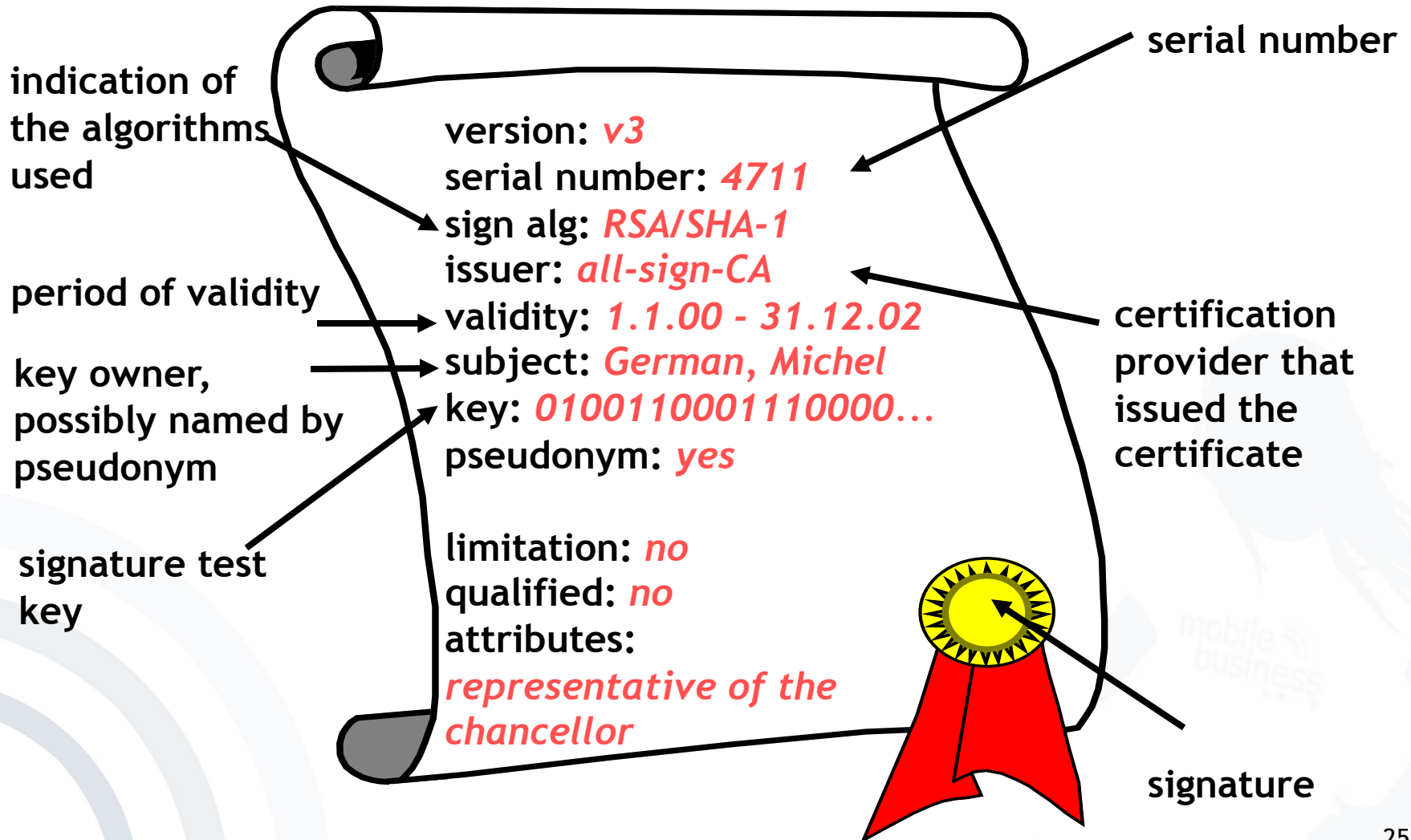
Certification
Authorities (CA)

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

- 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)
- Invalidation 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

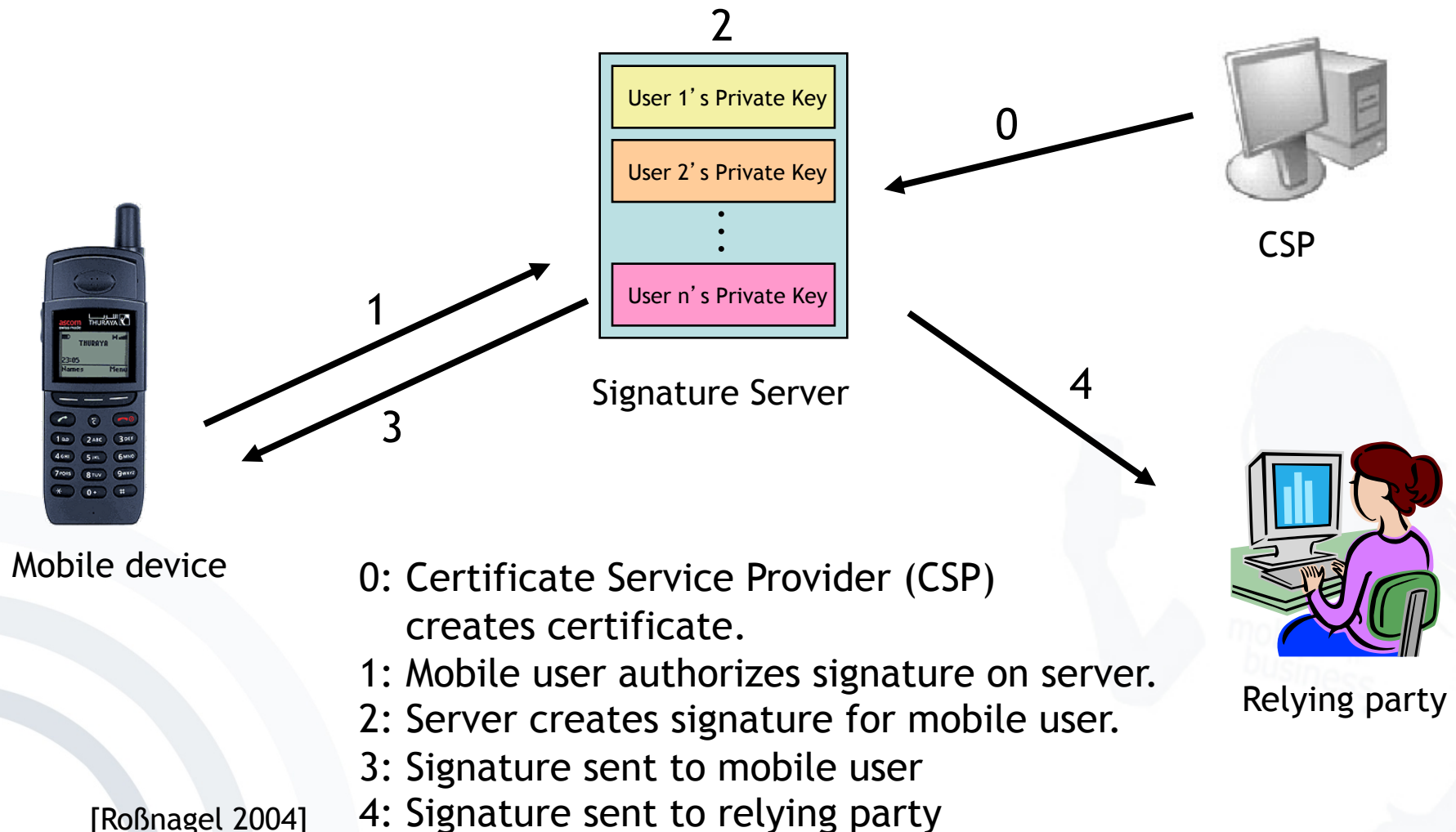
- General Concept & Applications
- Algorithms
- Legal Framework
- Mobile Signatures
- Secure Display Components and Personal Security Assistants
- Wallets
- Annexes

- 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.

- 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 Signatures 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.



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]

Use of separate smart cards for telephony and signature:

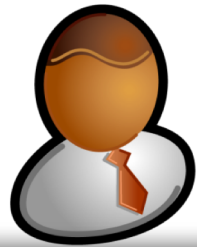
- Dual Card
Exchange of SIM against Secure Signature Creation Device (SSCD)
- Dual Slot
Mobile device carries two card readers for SIM and SSCD



- Restrictions in mobile devices
 - Visualization of complex “Document To Be Signed” (DTBS) on mobile devices’ relatively small displays is tricky.
 - Limited memory may hinder the proper processing of revocation lists.
 - Bandwidth problems used to hinder data transfers for e.g. certification.
- Platform security
 - Mobile phones are becoming open platforms
 - A trusted device is necessary (➔ TCG/Perseus)

- General Concept & Applications
- Algorithms
- Legal Framework
- Mobile Signatures
- Secure Display Components and Personal Security Assistants
- Wallets
- Annexes

Presentation Problems



Mr. Schulz

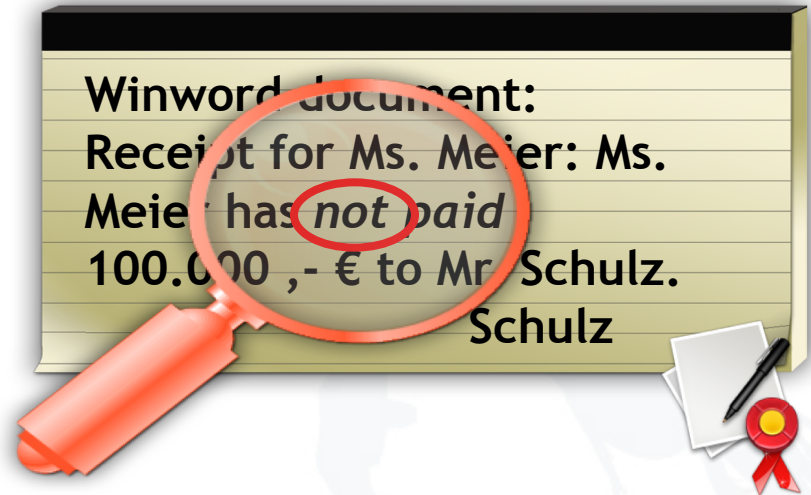
Winword document
Receipt for Ms. Meier:
Ms. Meier has paid
100.000 ,- € to Mr. Schulz.
Schulz



Ms. Meier



[Based on IsRo]



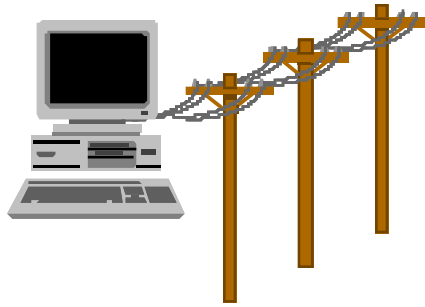
But check for hidden text !!!!

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

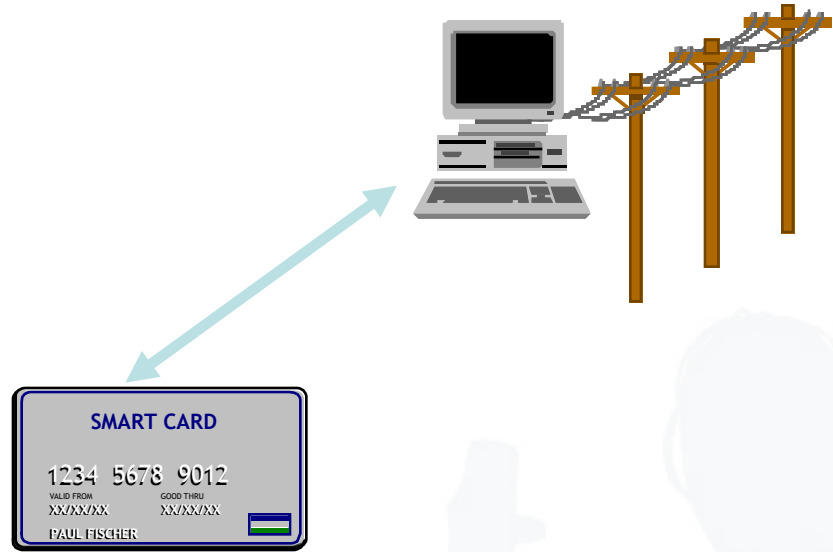
The signature component must:

- 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

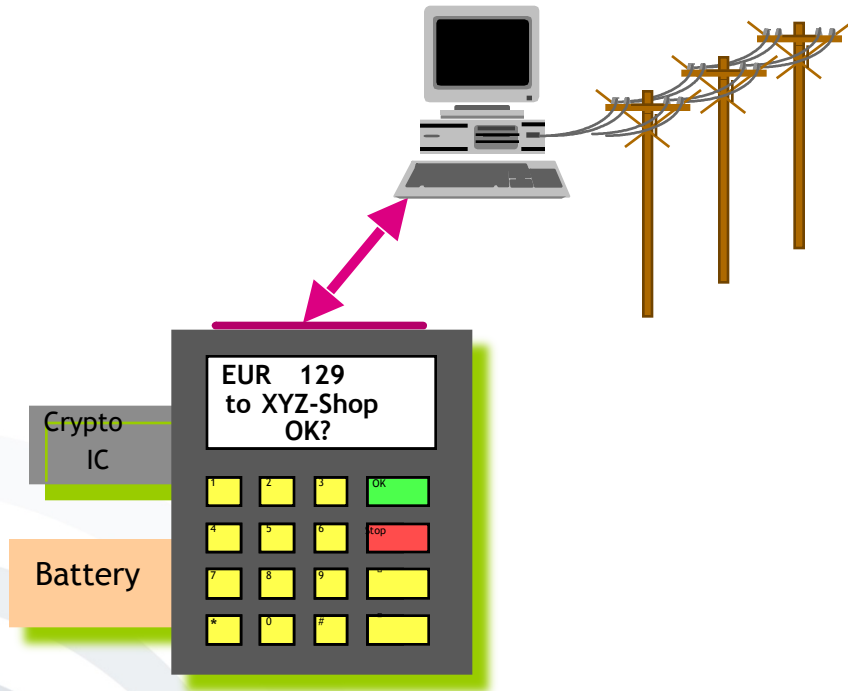


**Private key
on HD, in memory**



**Private key and
signature function in chip card**

Secure Equipment: Avoiding Threats from Trojan Horses



Wallet with
private key and
signature function

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

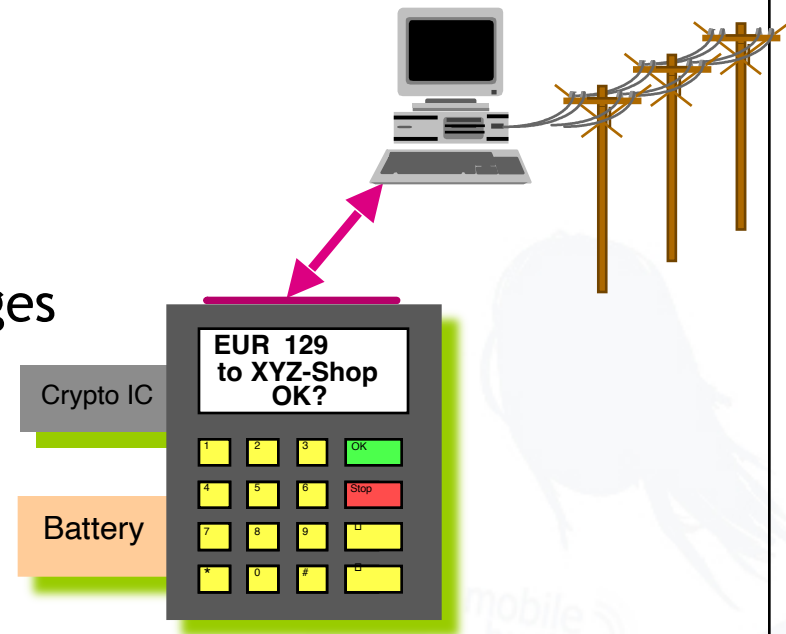


Order

Buyer
 Certificate
 Date
 Description
 Total
 Currency
 Signature

A popular vision: Security Assistants

- Storing personal data (wallet)
 - Addresses, calendars
 - Money, keys, certificates
 - 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 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
- ...



- General Concept & Applications
- Algorithms
- Legal Framework
- Mobile Signatures
- Secure Display Components and Personal Security Assistants
- Wallets
- Annexes

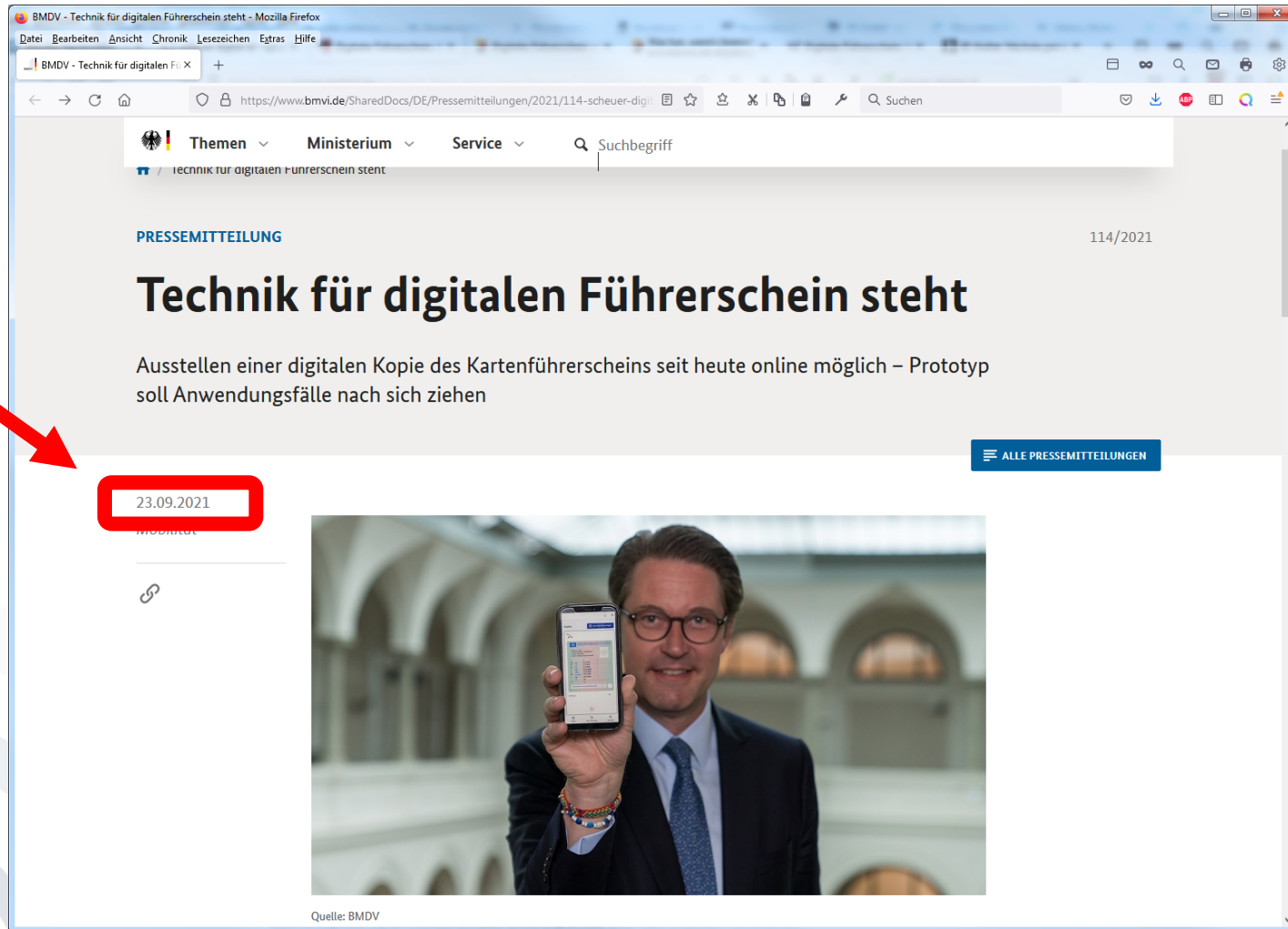
EU Regulation COM(2021) 281

- European Digital Identity Wallets (EDIW) as a means to identify citizens online and offline in multiple contexts (e.g., online shopping, opening a bank account, checking into a hotel or renting a car) (<https://digital-strategy.ec.europa.eu/en/library/trusted-and-secure-european-e-id-regulation>)
- Amends Regulation (EU) No 910/2014 for establishing a European Digital Identity
- Great initiative as it
 - Enables users to control their digital services
 - Strengthens European Digital Sovereignty
 - Improves the security of identity management
 - Shows an example of better security for ICT devices.

- Full control of users of the digital identity is crucial from a security and privacy point of view
 - Only full control by users can create the necessary trust by users
- No explicit design decision in the amendment with respect to the wallet
 - Initial interpretations imply a storage space provided by (cloud) providers (or ledgers) which are accessed by users via an app on their smartphones
 - How much control can be ensured in such a scenario?
- The wallet and the related services are an essential infrastructure.
 - Have decisions done by those decision makers that offer maximum transparency!
 - Consider and budget for Open Source solutions!

- Economic and operational issues as appropriately protected ICT is (often) not directly honored by the market
 - “Free” options often convenient but insecure
 - No level playing field.
- Some solutions may create market domination due to limited availability of essential
 - Hardware
 - Software
- Ensure that the implementation has sufficient resources
 - Money (Proposed 31 Million EUR look very limited)
 - Time (6 - 12 months is much too hurried)

What time pressure can do the ambiguity of "standing"



What time pressure can do the ambiguity of "standing"

DER TAGESSPIEGEL

SUCHE

„Digitale Briefftasche“ der Bundesregierung

01.10.2021, 15:30 Uhr

Scheitern mit Ansage?

Der Handy-Führerschein musste nach wenigen Tagen gestoppt werden. Bei der dazugehörigen „digitalen Briefftasche“ der Bundesregierung gibt es Fehler und Sicherheitsbedenken. Dabei gab es schon im Vorfeld Zweifel an der Technik. VON OLIVER VOSS



Stolz präsentierte Andreas Scheuer den digitalen Führerschein. Tage darauf ist der Minister "stocksauer" über die Probleme. FOTO: RUI CARDOSO/BMVI

[<https://www.tagesspiegel.de/wirtschaft/digitale-briefftasche-der-bundesregierung-scheitern-mit-ansage/27665302.html>]

- General Concept & Applications
- Algorithms
- Legal Framework
- Mobile Signatures
- Secure Display Components and Personal Security Assistants
- Wallets
- Annexes

- Annex I
 - EU eIDAS regulation 2014,
requirements for qualified certificate
- Annex II
 - Client Signatures
SIM based
- Annex III
 - Certification on Demand

Annex I

EU eIDAS regulation 2014, requirements for qualified certificate

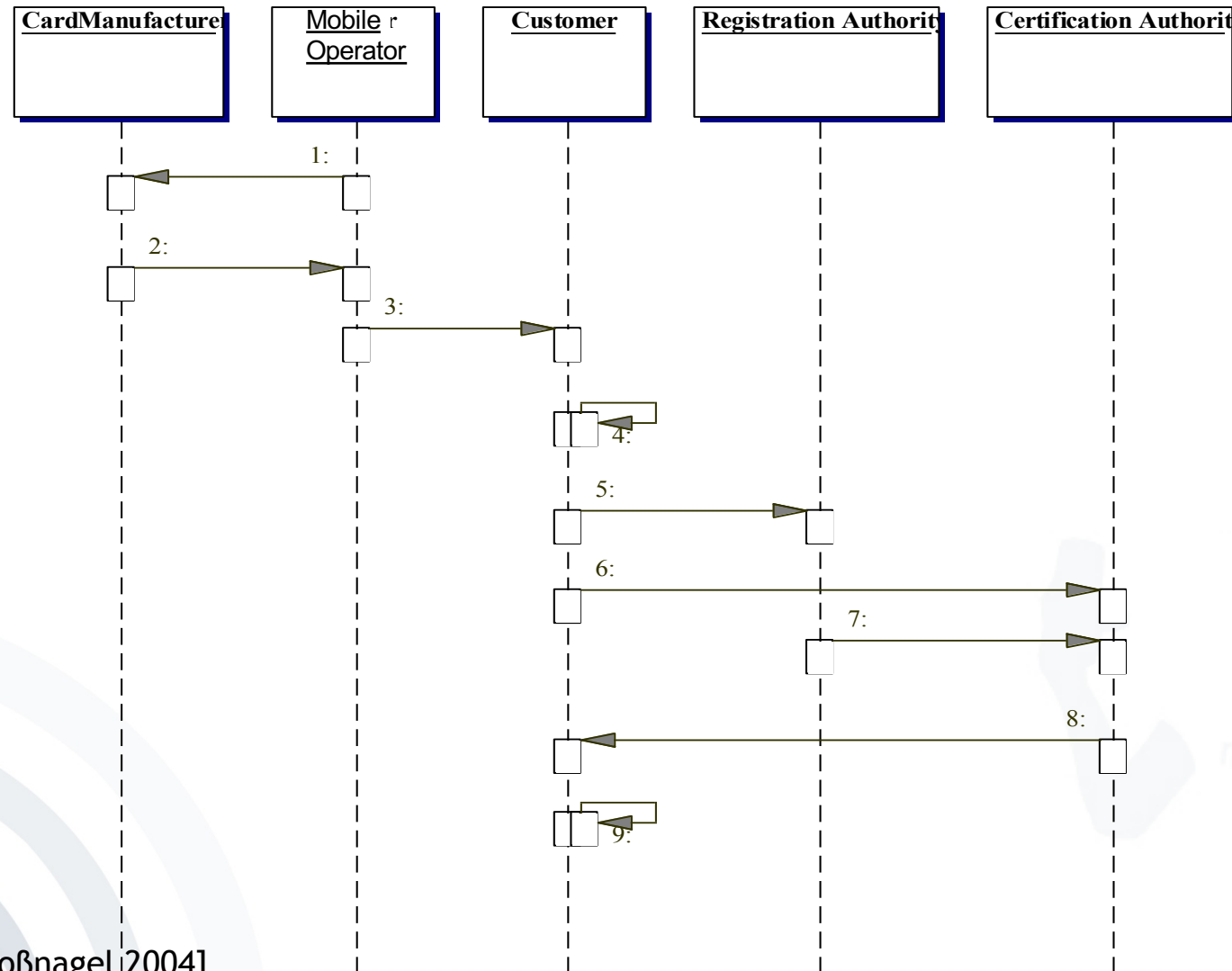
- an indication that the certificate has been issued as a qualified certificate ...
- Data about the qualified trust service provider issuing the qualified certificates ...
- ... name of the creator of the seal and, where applicable, registration number as stated in the official records;
- ... validation 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...

- 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?

Certification on Demand



[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.

- 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
- [SigG01] Gesetz über Rahmenbedingungen für elektronischen Signaturen, 16. May 2001
- [VDG17] Vertrauensdienstegesetz, 18. July 2017 (BGBl. I S. 2745)