![mobile business]

Lecture 5

Application Domains III: (Mobile) Electronic Signatures

Mobile Business II (SS 2024)

Prof. Dr. Kai Rannenberg

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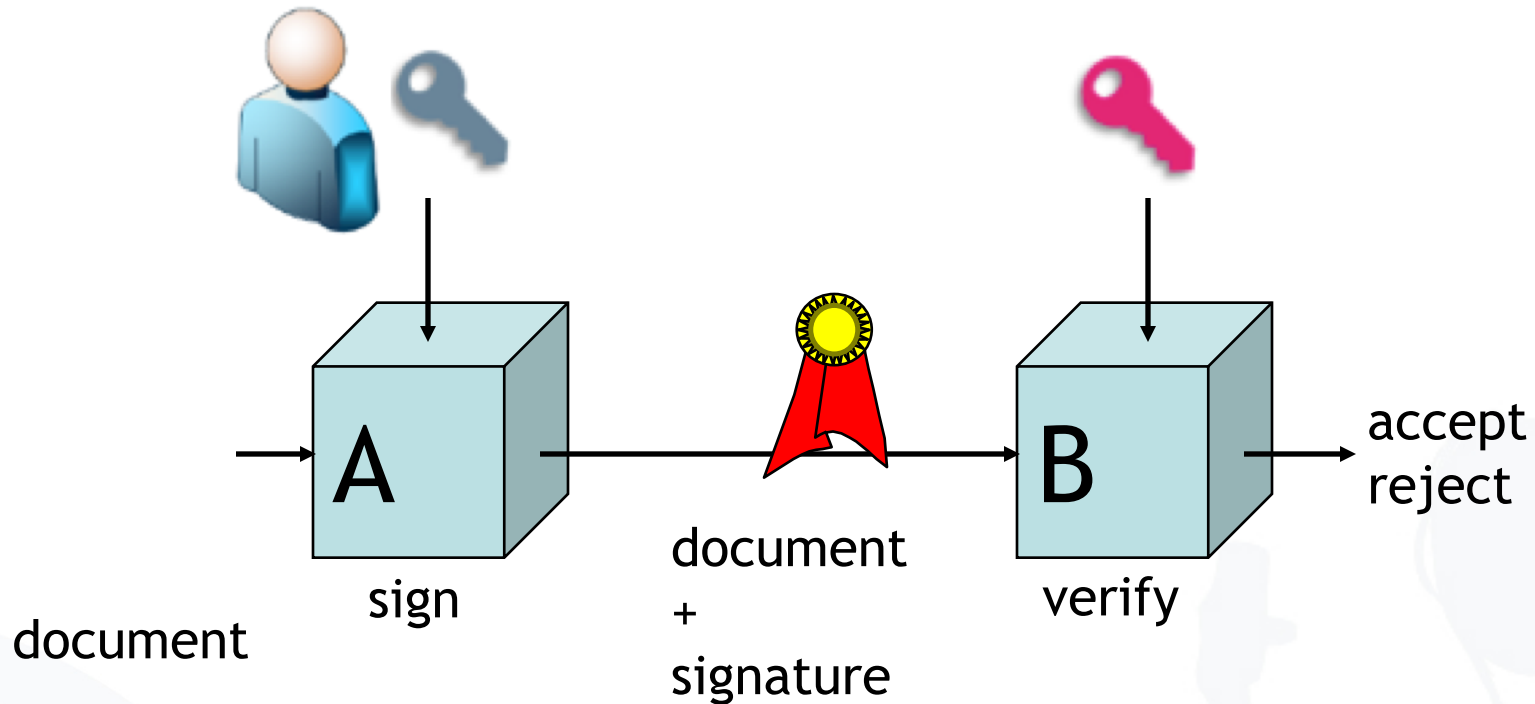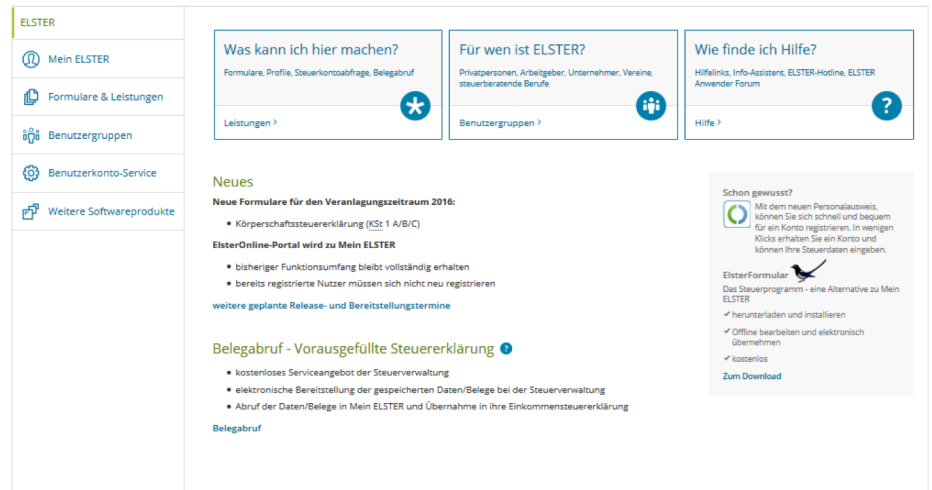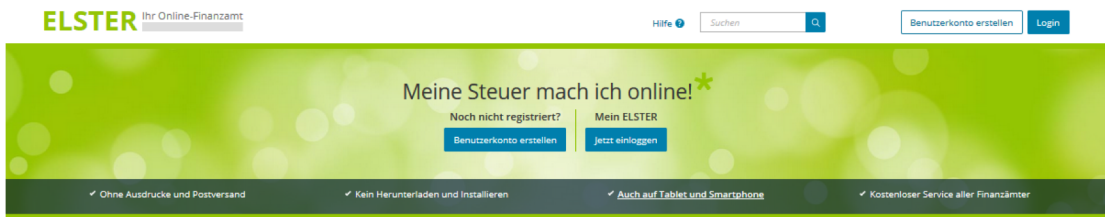Goethe University Frankfurt a. M.

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

sign

document

document
+
signature

verify

accept
reject

➲ 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.
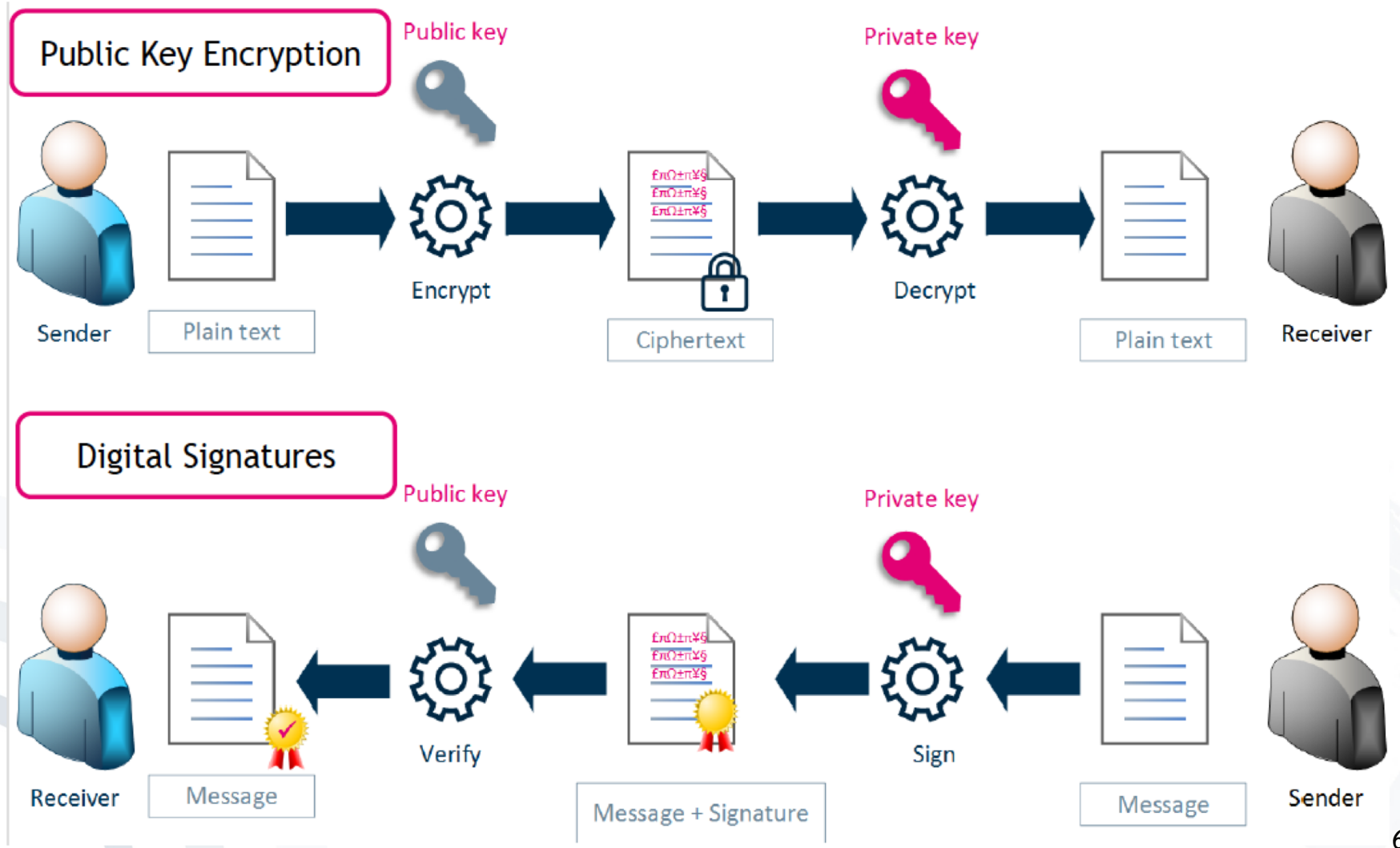
[Bishop2005]

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

Public Key Encryption

Public key   Private key

Sender — Plain text — Encrypt — Ciphertext — Decrypt — Plain text — Receiver

Digital Signatures

Public key   Private key

Receiver — Message — Verify — Message + Signature — Sign — Message — Sender

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.

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

- ## 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.

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
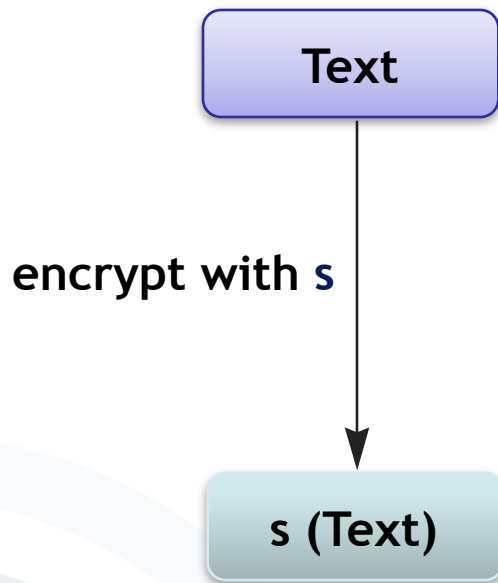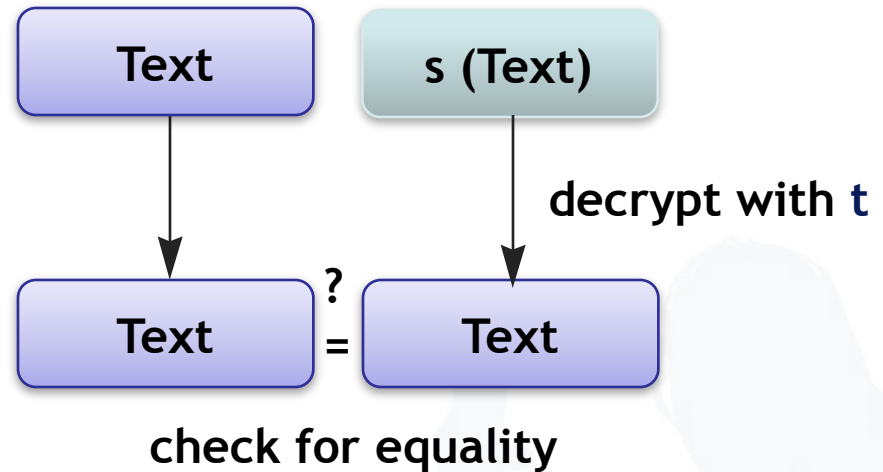
Addressee / Verifier

Text

encrypt with **s**

s (Text)

Text

s (Text)

decrypt with **t**

Text

$\overset{?}{=}$

Text

check for equality

➲ **Signing key s only with the sender, test key t public**

➲ **Example is often mistakenly generalized.**

Asymmetric Signature System (Example RSA)
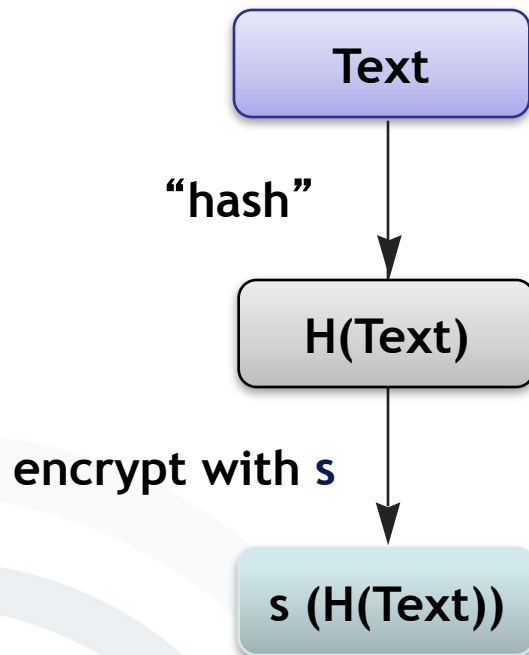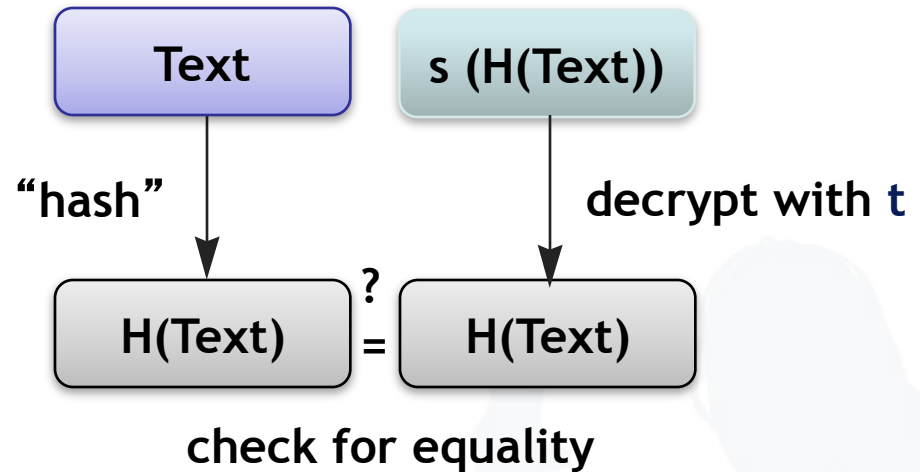
Sender / Signer

Addressee / Verifier

Text

"hash"

H(Text)

encrypt with **s**

s (H(Text))

Text   s (H(Text))

"hash"   decrypt with **t**

H(Text) $\overset{?}{=}$ H(Text)

check for equality

➲ **Signing key s only with the** sender, **test key t** public

➲ **Example is often mistakenly generalized.**

One way cryptography

Plain text → Hash function → Ciphertext

£πΩ±π¥§
£πΩ±π¥§
£πΩ±π¥§

Data of arbitrary length

Message

Hash function

[e883aa0b24c09f...]
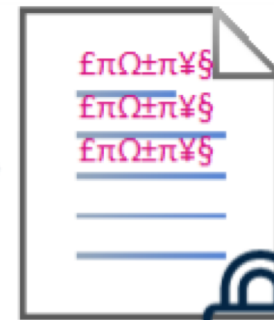
Fixed length hash (digest)
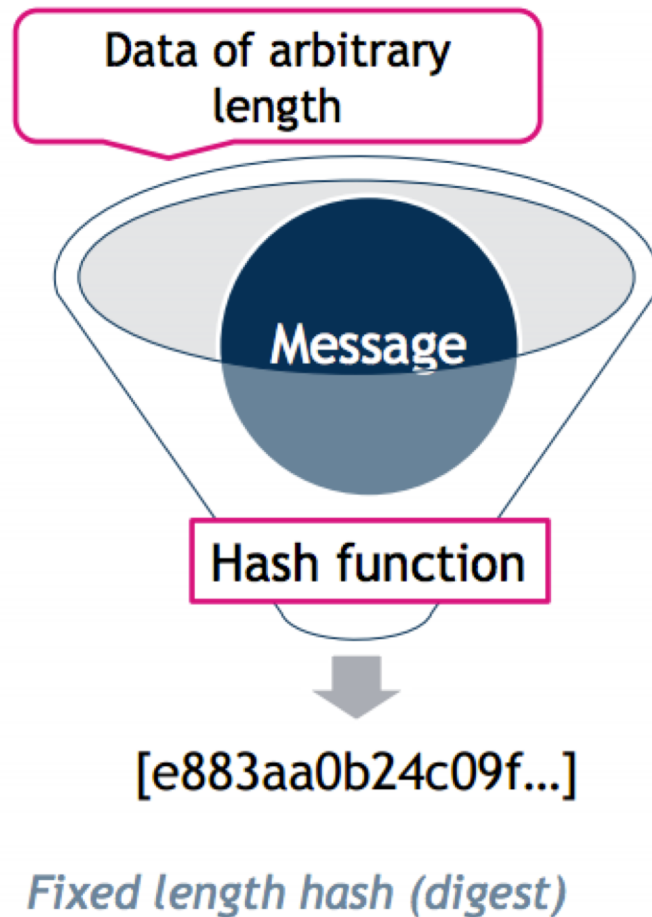
General hash functions *(H(s))*
Transformation of an input string *s* into an output string *h* **of fixed length** which is called hash value.
Example: mod 10 in the decimal system

Asymmetric Signature System (Example RSA)
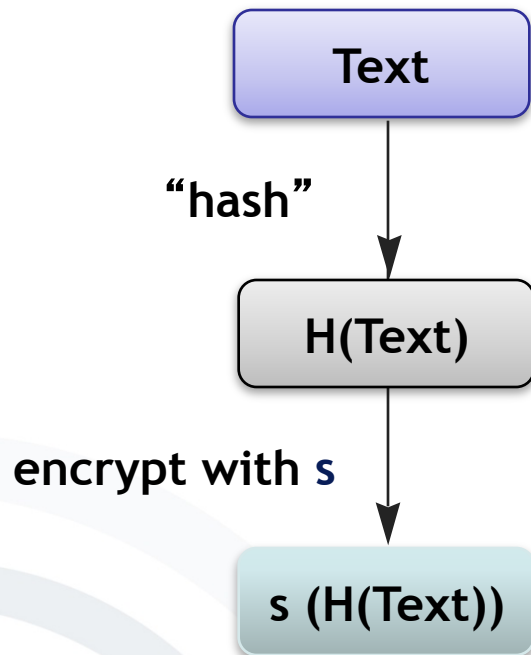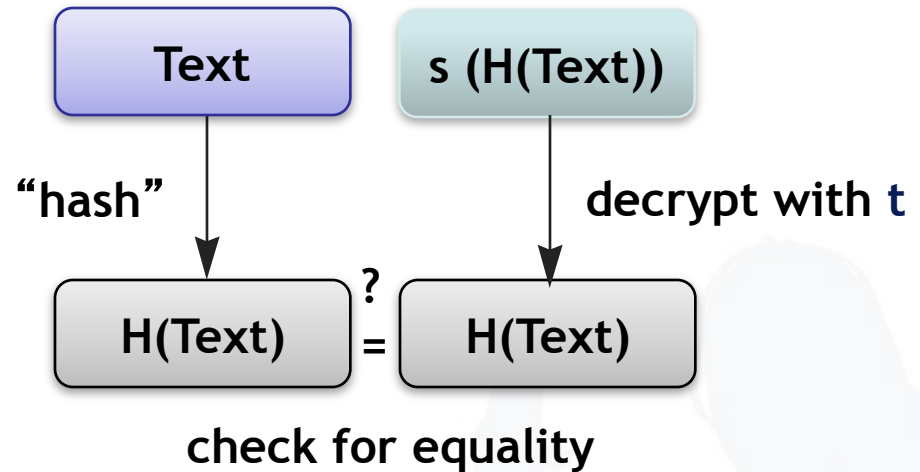
Sender / Signer

Addressee / Verifier

Text

"hash"

H(Text)

encrypt with **s**

s (H(Text))

Text   s (H(Text))

"hash"   decrypt with **t**

H(Text) $\overset{?}{=}$ H(Text)

check for equality

➲ **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).

[EU eIDAS Regulation 2014], [VDG17]

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.")

Regulatory Authority confirms public keys of the CAs

Root-CA (Regulatory Authority**)**
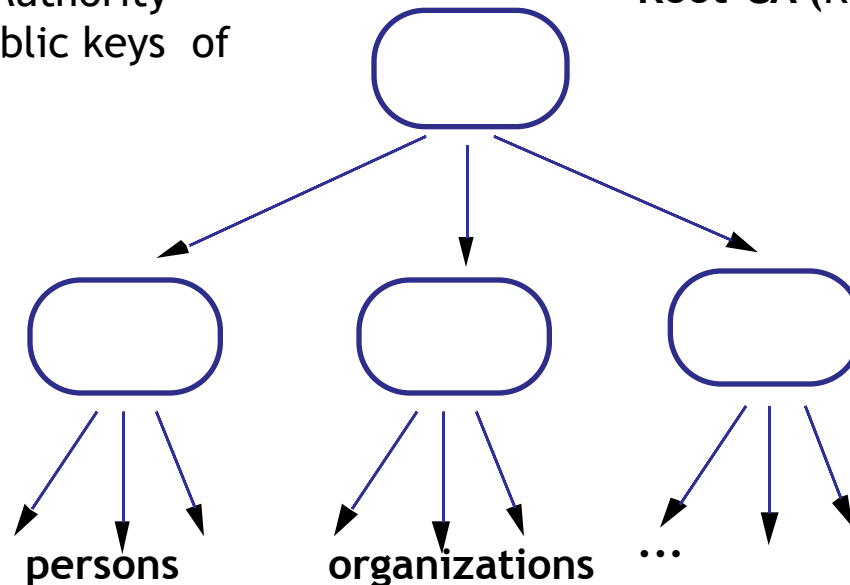
Certification Authorities (CA)

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

serial number

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

certification provider that issued the certificate

signature

- 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

- **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.

[EU eIDAS regulation 2014]

- 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 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]

Mobile device

Signature Server

CSP
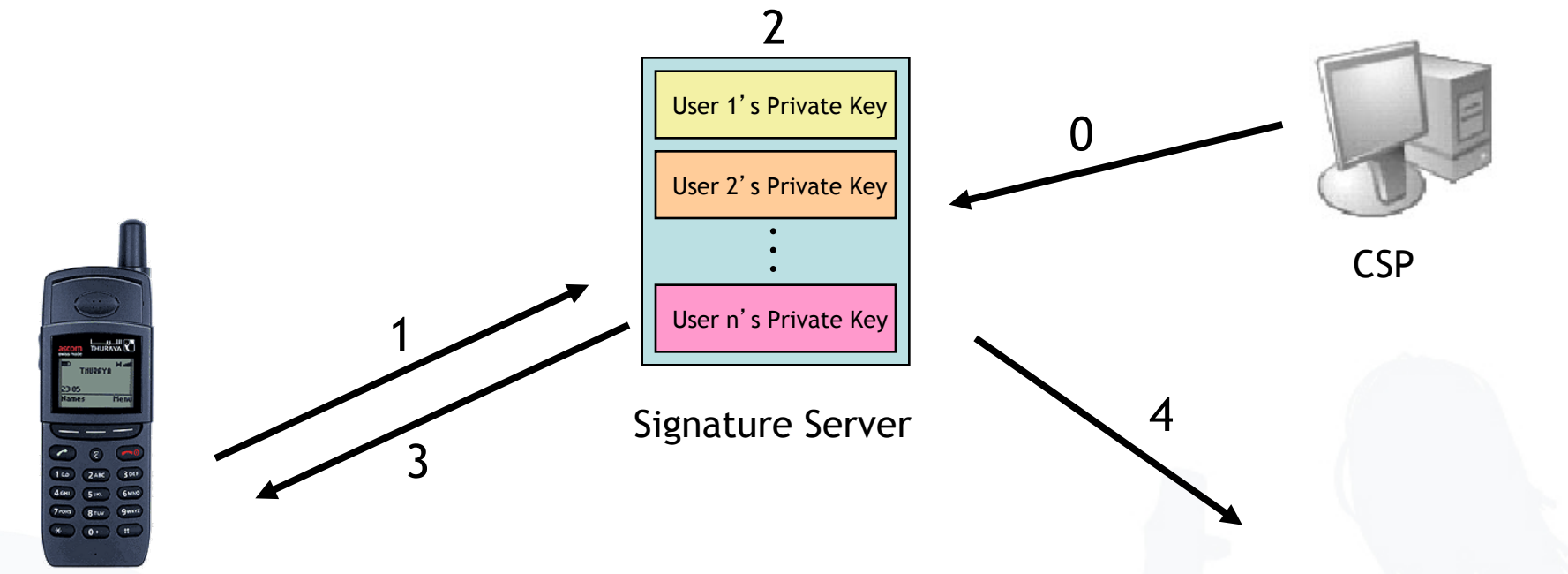
Relying party

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]

Directive 1999/93/EC

REGULATION (EU) No 910/2014 repealing 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."

- 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."

[EC Directive 1999]

[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

COVER für

2 oder 3 Simkarten

[Roßnagel 2004]

- **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)

[Roßnagel 2004]

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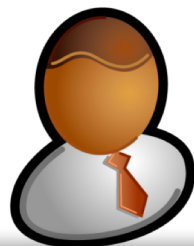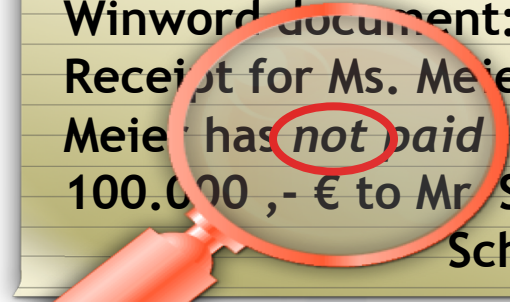
Mr. Schulz

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 !!!!

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.")
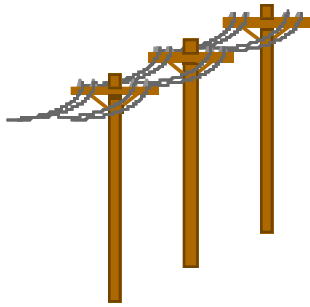
**Private key
on HD, in memory**

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

mobile business

EUR   129
to XYZ-Shop
OK?

Crypto IC

Battery
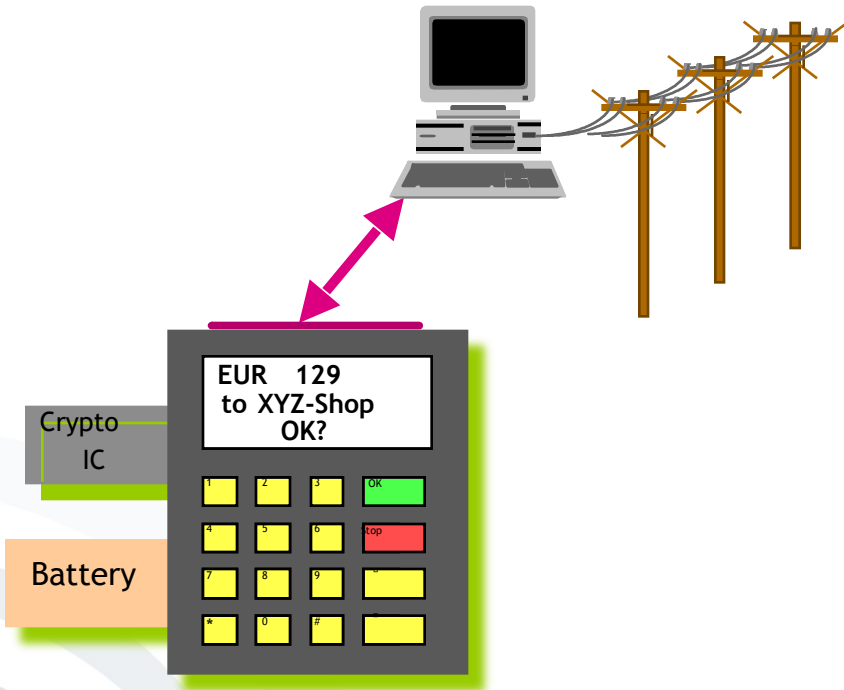
Wallet with private key and signature function

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 (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
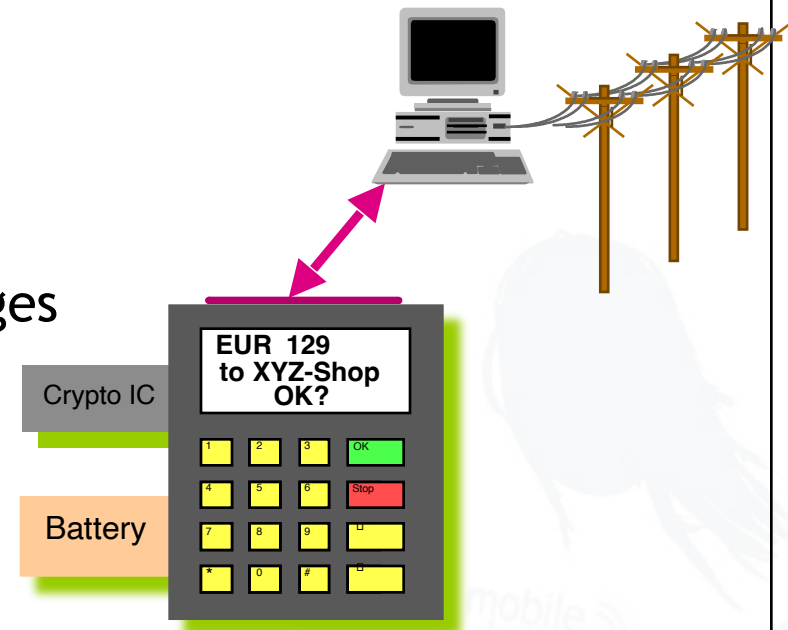
- Usability
  - Portability
  - Good visibility of important information ("new network")
  - Adequate representation of the functionality

- 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 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

EC Regulation Proposal 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 <u>control</u> 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 ...
... a related initiative to learn from

What time pressure can do ...
... a related initiative to learn from

DER TAGESSPIEGEL

SUCHE 🔍

01.10.2021, 15:?0 Uhr

„Digitale Brieftasche" der Bundesregierung

Scheitern mit Ansage?

Der Handy-Führerschein musste nach wenigen Tagen gestoppt werden. Bei der dazugehörigen „digitalen Brieftasche" 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-brieftasche-der-bundesregierung-scheitern-mit-ansage/27665302.html]

Digital Identity for all Europeans

A personal digital wallet for EU citizens and residents

- The EU Digital Identity will be available to EU citizens, residents, and businesses who want to identify themselves or provide confirmation of certain personal information. It can be used for both online and offline public and private services across the EU.

- The EU Digital Identity Toolbox will further secure your digital identity and establish trust in online transactions.

- The Toolbox will complement the legislative proposal on a trusted and secure Digital Identity and is a crucial first step that will enable the creation of a robust framework for digital identification and authentication based on common standards across the EU.

- With a click of a button on the phone it will be possible to securely share information stored in digital versions of their driving licence, professional or educational credentials, and medical prescriptions.

[DigiEu2023a,b]

European Commission

- European Digital Identity wallet (EUDI) wallet for travel, health, banking, education and more.

- The European Commission is investing supporting 4 pan-European pilot projects that will develop and test the usage of the EUDI wallet for individuals and businesses around a diverse range of everyday use-cases.

- Everyday scenarios include:
  - providing identification to online and offline public and private services;
  - displaying your mobile driving licence;
  - authorising payments;
  - signing documents electronically;
  - presenting medical prescriptions.

[DigiEu2023c]

- **The 4 Pilot Projects to test EUDI Wallet:**

  1. **POTENTIAL – Pilots for European Digital Identity Wallet Consortium**

     - Coordinated by Germany and France with the involvement of 17 Member States

     - The project will apply the EUDI wallet to 6 use-cases, including: **Access to government services**, **Opening of a bank account**, **Registration for a SIM card**, **Mobile driving licence**, **eSignatures**, and **ePrescriptions**

  2. **EWC – EU Digital Identity Wallet Consortium**

     - Coordinated by Sweden with the involvement of 18 Member States and Ukraine

     - The project will test 3 use-cases, including: **Storage and display of digital travel credentials**, **Organisation of digital wallets**, **Organisation of payments**

European Commission

- **The 4 Pilot Projects to test EUDI Wallet...**

  3. **NOBID – Nordic-Baltic eID Wallet Consortium**
     - Coordinated by Norway with the involvement of 8 Member States and EEA countries
     - The project will focus on a single use-case: the use of the EUDI **wallet** for the **authorisation of payments** for products and services by the wallet user, the **issuance of wallets**, the **provision of payment means** by financial institutions, and the **acceptance of payment** in a retail context.

  4. **DC4EU – Digital Credentials for Europe Consortium**
     - Coordinated by Spain with the involvement of 23 Member States and Ukraine
     - The project will test the use of the EUDI wallet in the **educational sector** and the **social security domain**. The pilot project will align with the **European Social Security Pass** and the **European Learning Model**. It will use the European Blockchain Services Infrastructure (EBSI) in the context of the EUDI wallet.

- Browsers forced to accept EU member state web certificates without any security check (Article 45 and newly introduced Article 45a-1)

- Risk for of web (https) encryption, if member states misuse certificates for establishing keys to listen into https traffic

- Unlinkability of wallet use not guaranteed

➢ „Homework" for standardisation

[Council of European Professional Informatics Societies (CEPIS) 2023]

CEPIS 55

- 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
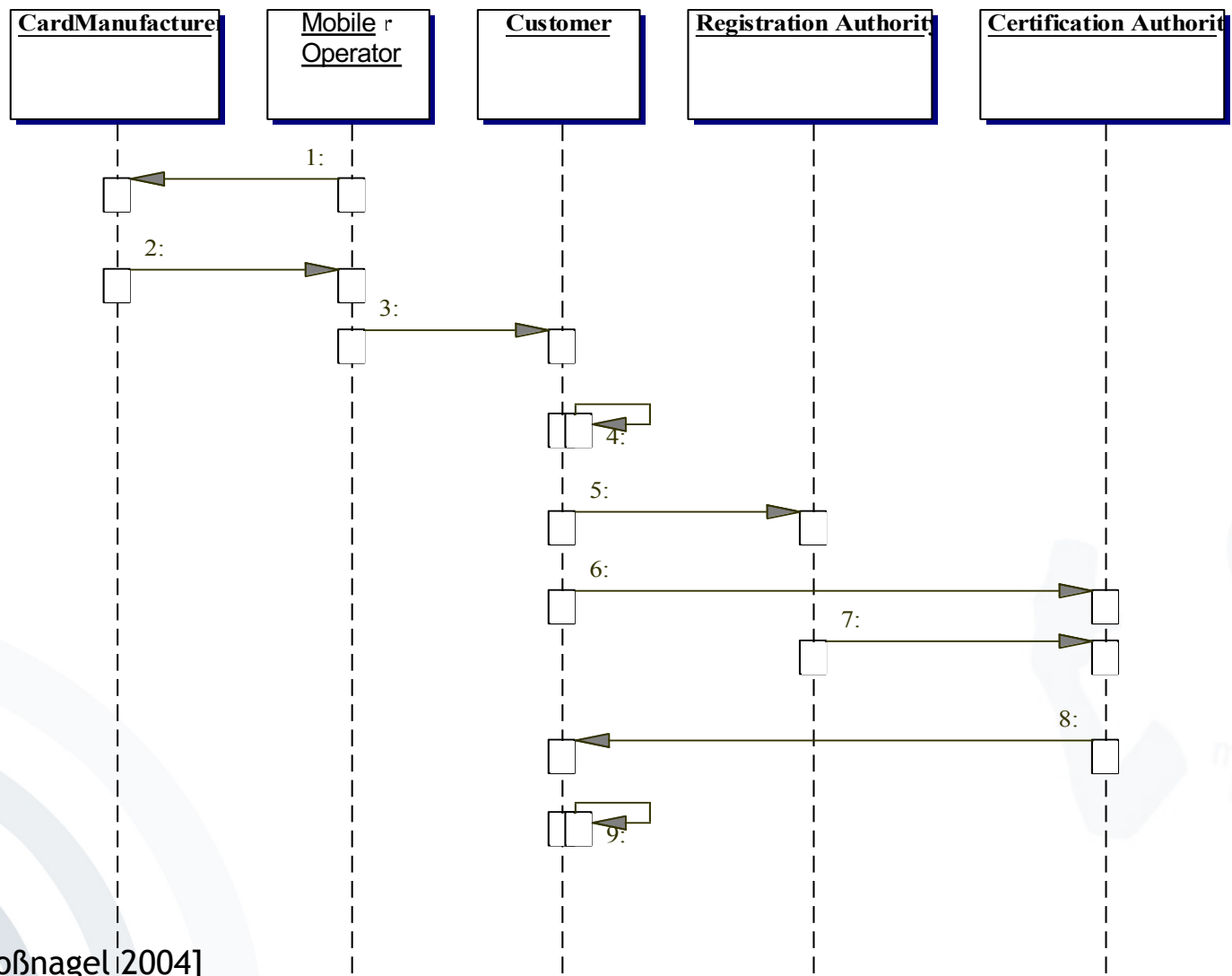 - ### Certification on Demand

- 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]

- 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]

- 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]

- 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]

CardManufacturer | Mobile Operator | Customer | Registration Authority | Certification Authority

[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

[Roßnagel 2004]

- 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]

- Bishop, Matt (2005): Introduction to Computer Security. Boston: Addison Wesley, 2005.
- Council of European Professional Informatics Societies (CEPIS) (2023): CEPIS suggests improvements on amendment to eIDAS regulation, 2023-11-28, https://cepis.org/cepis-suggests-improvements-on-amendment-to-eidas-regulation/
- 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.
- [DigiEu2023a] https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en (accessed 2024-01-08)
- [DigiEu2023b] https://digital-strategy.ec.europa.eu/en/policies/eudi-wallet-toolbox (accessed 2024-01-08)
- [DigiEu2023c] https://digital-strategy.ec.europa.eu/en/news/eu-digital-identity-4-projects-launched-test-eudi-wallet (accessed 2024-01-08)
- 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)