mobile business

GOETHE UNIVERSITÄT FRANKFURT AM MAIN

Information & Communication Security (SS 15)

Electronic Signatures

Dr. Jetzabel Serna-Olvera
@sernaolverajm
Chair of Mobile Business & Multilateral Security
Goethe University Frankfurt
www.m-chair.de

mobile business

Agenda

- Digital Signature Overview
- Algorithms
- Hash Functions
- Electronic Signatures - Legal Framework
- Recent Initiatives in Europe
- Use Case Scenario

mobile business

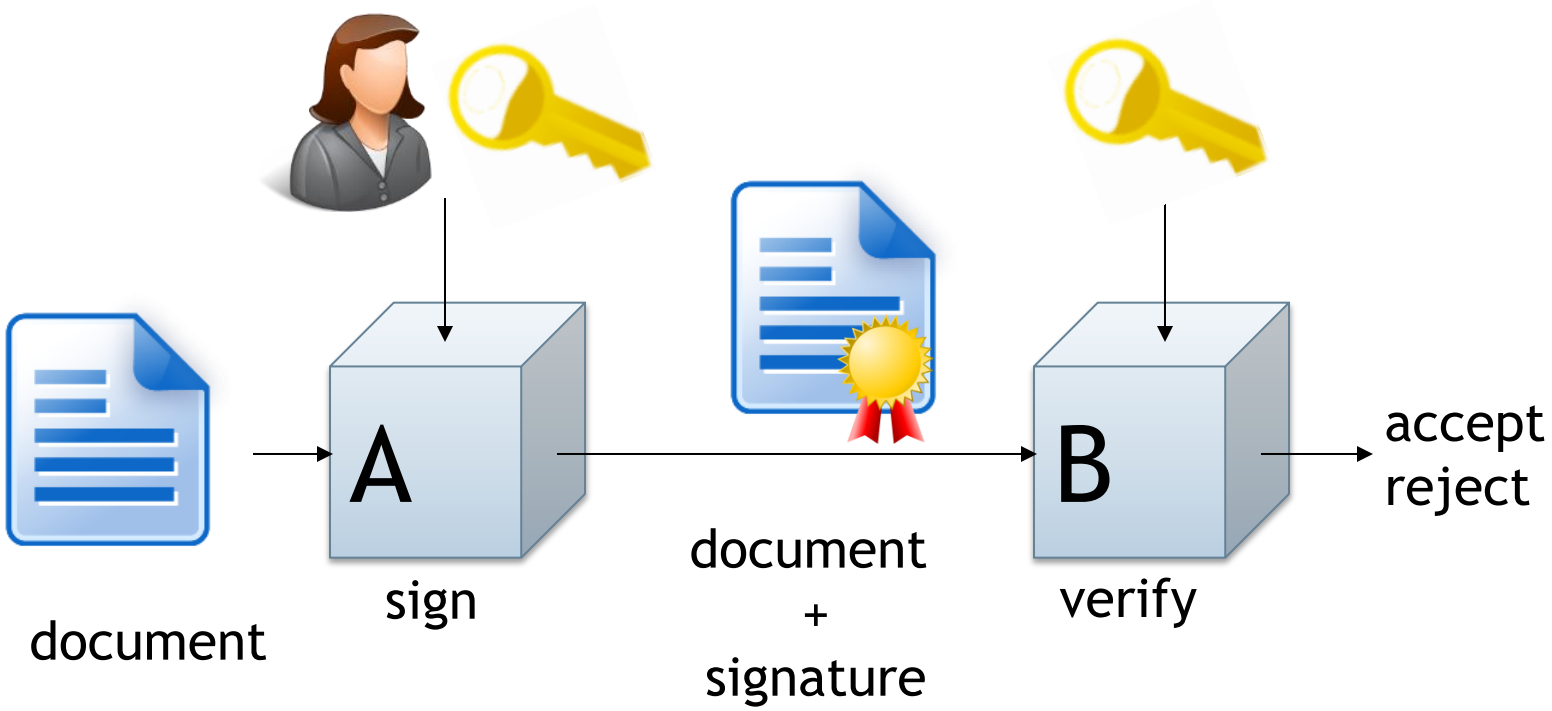
Digital Signatures

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

[Bishop 1978]

Only the entity who creates a digital message must be capable of generating a valid signature

Digital Signatures



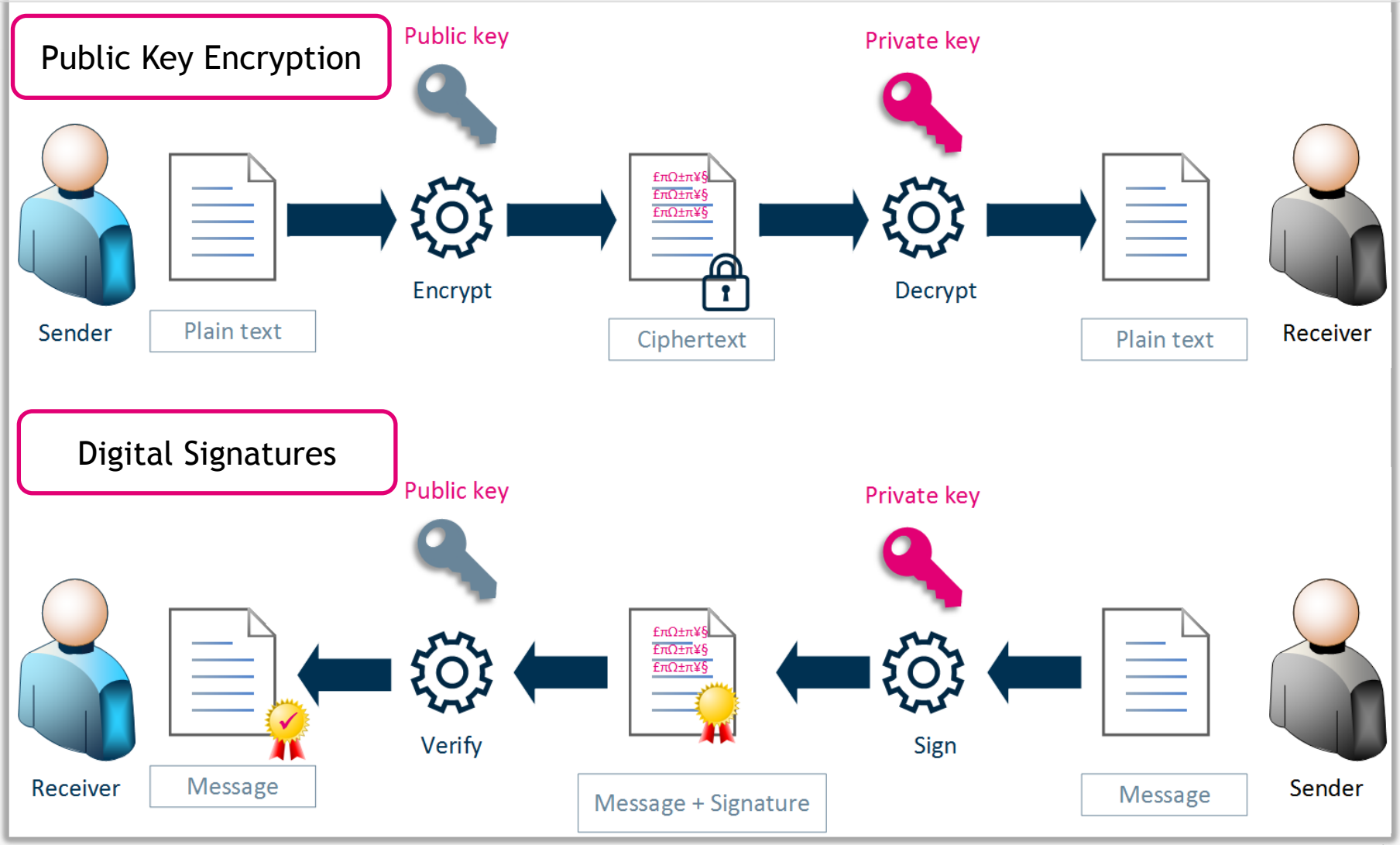
- Protect the authenticity and integrity of documents signed by A
- B has to get an authentic copy of A's public key.

mobile business

Security Properties

- Message Authentication (*data origin authentication*): The sender of the message is authentic.
- Integrity: Messages have not been modified in transit.
- Non-repudiation: The sender of the message cannot deny the creation of the message.

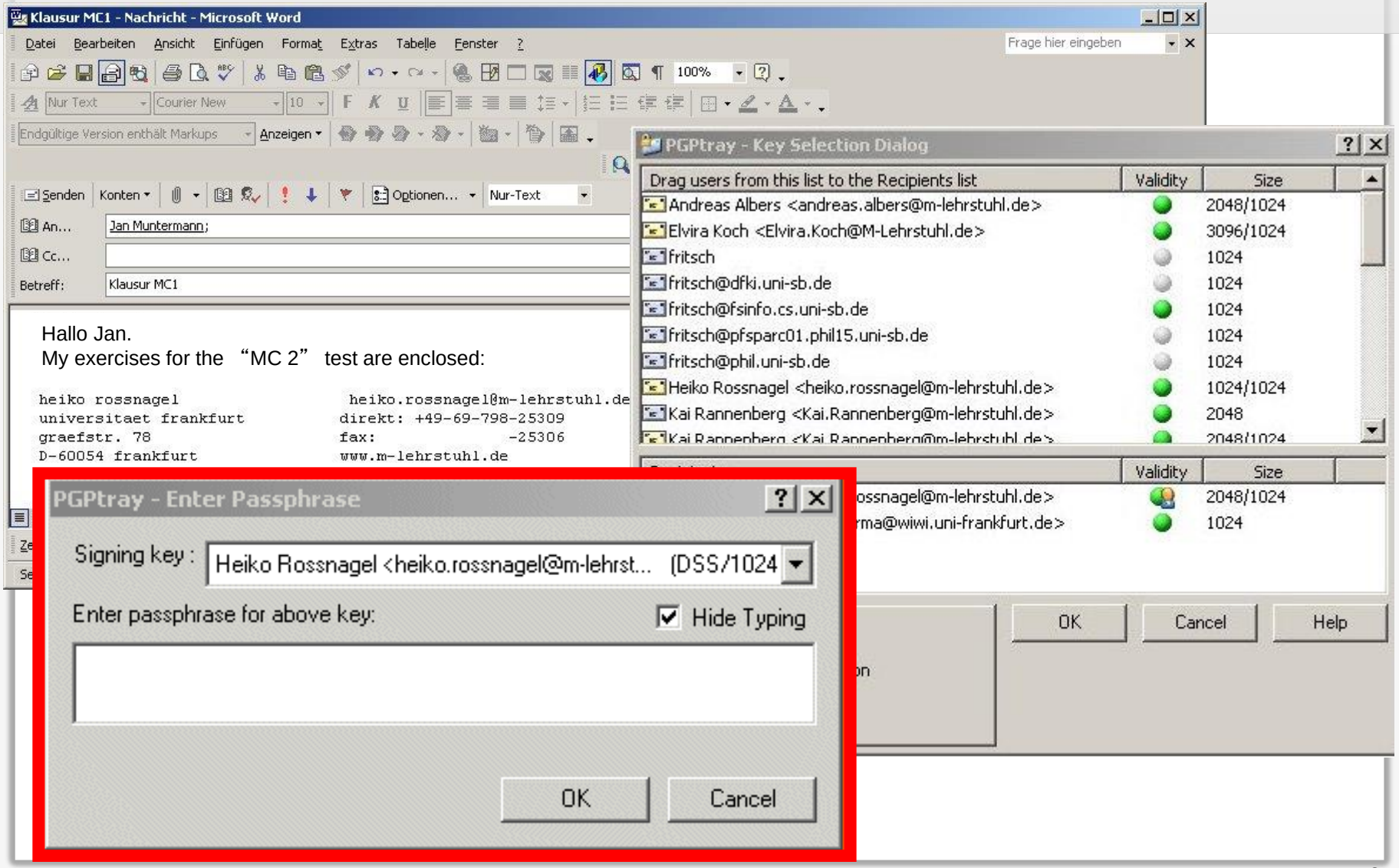
Asymmetric Signature System



Asymmetric Signature System

Digital Signatures	Public Key Encryption
▪ The holder of the secret key (sender) signs the message ▪ "Anyone" can verify that a signature is valid	▪ "Anyone" can encrypt a message ▪ Only the holder of the secret key (receiver) can decrypt a message

Example PGP: Encrypt and Sign a Message



Example PGP: Decrypt and Check a Message

mobile business

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

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

hQCMA5/VPPIP3satAQP+LqxvxFSk4G/TAexpMLX436biwBp6xP8pa89R7ro
uHEsO7/tFrJFQJpPBcUWouy47p4sR2FO+IXqJuJyHp5ExMGIdmQCpGXEoS2
B5TXKtUB8YJdpPnck61as78RBP1sq8VDrAlYopEAeqMMw2pkBuoxyo3KCiR
Ag4DIYlowhVX6ZwQCAD2L9WAA97xEUBWMET6kR9n5+oafTBF+ROlv6UOz2T
Alkh23iQOlI9Drye/uygpcQpT2HhTtZYlAjjudLvi+GsegOlWmBjY8q8G1Y
kDP3GEanyDiDU6R9FlXFOvxPNMk6Ek8hH6qZ37hhDNDCXkxkSjM3nJ2VuuL
uOuXNA9iAC96dhg7NpvzCJI2J7xRMtuBc9BUI8LXODrvGLwnLtaD5+EvgL1
dfvQ3NiGrUEQsOHVxwjQdMtr8CO9kREYLuAdD7j/O5WtsAdbAVMn72PYFOI
i77MitBfAbxXFOgFS7/b2LccbaK8fx6e1VNFnVO7B/9qpdOGg5WZVP2eQA5
h2oTOSjWCRp/v5s9Og1aUtcAxdlRAjQPHpVsFS2eXXMnC9ZZvNIFMh6Ktqm
m39jRjPE9Ob/HLjMwPAXUHyneh9QrCX1X5qHORNcjIYVrnQyZGIk8t39059
cr1rhf6ht7SwGgfgGW2aL8HyiF
E1IJGt9QLiwMmXormxcOg+WR2I
NjwtR+1SkqMCXs+PzcAHDsiuGz
pE3huhK5cfvu1Ug7+Oa9SUAy4J
NZncI3vJgkZeZrlbh+pi4dRjsO
=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

OK Cancel

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 ***
```

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

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

Copy to Clipboard OK

mobile business

Agenda

- Digital Signature Overview
- Algorithms
- Hash Functions
- Electronic Signatures - Legal Framework
- Recent Initiatives in Europe
- Use Case Scenario

Public Key Algorithms

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

Asymmetric Signature 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]

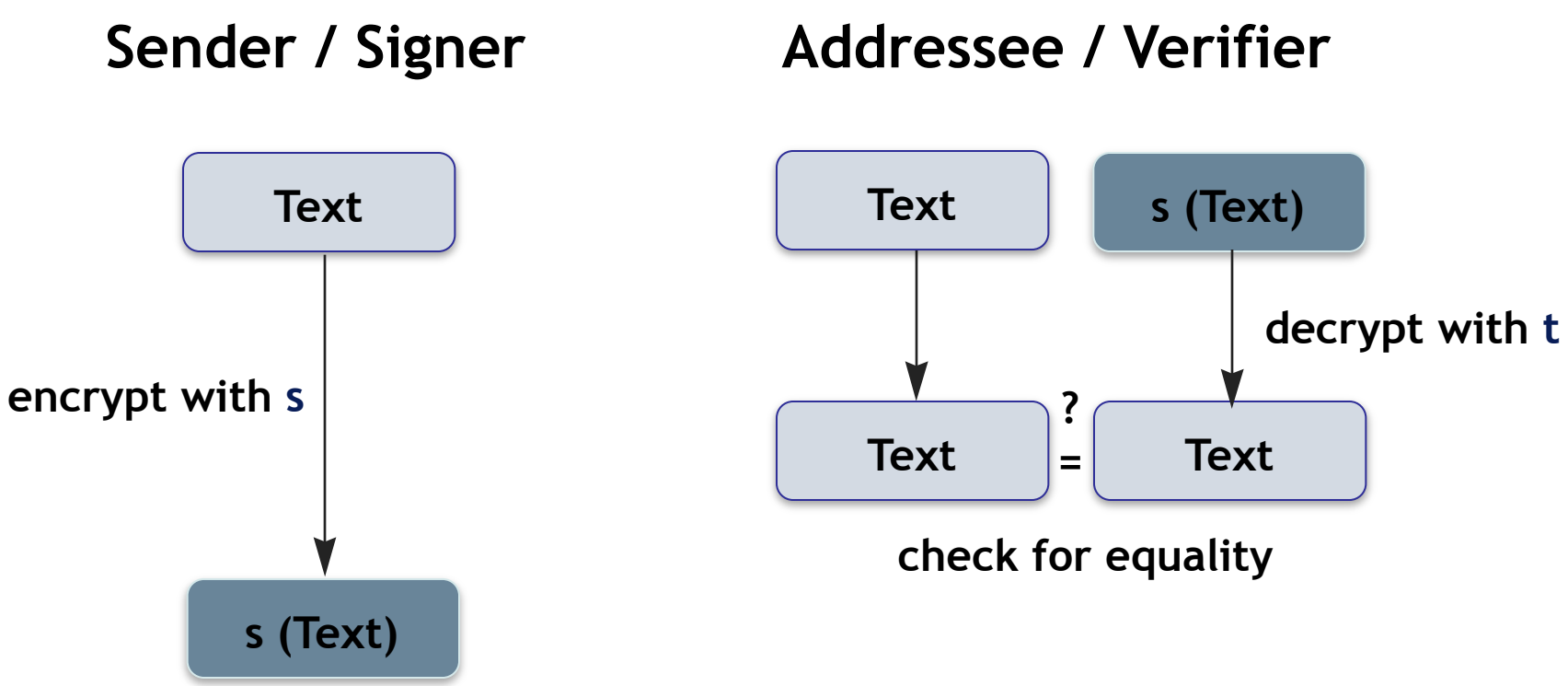
Asymmetric Signature Systems: Examples

- DSA: **D**igital **S**ignature **A**lgorithm
  - 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 Systems: Examples

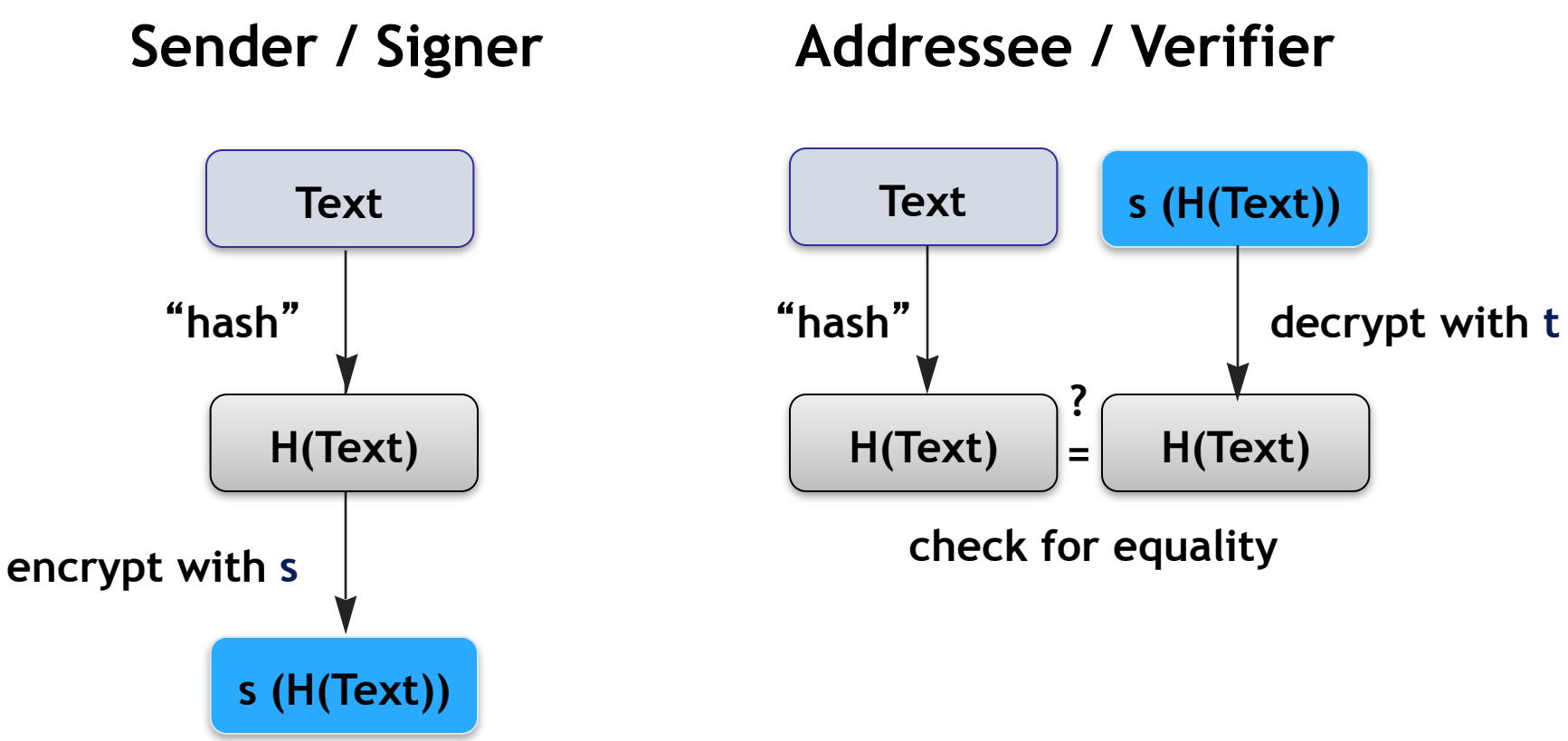
- ECDSA **E**lliptic **C**urve **D**igital **S**ignature Algorithm
  - Shorter keys and shorter signatures, which leads to better performance
  - Standardized in the US by the American National Standards Institute (ANSI) 1998.

Asymmetric Signature System (Simplified Example RSA)



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

Asymmetric Signature System (Example RSA)



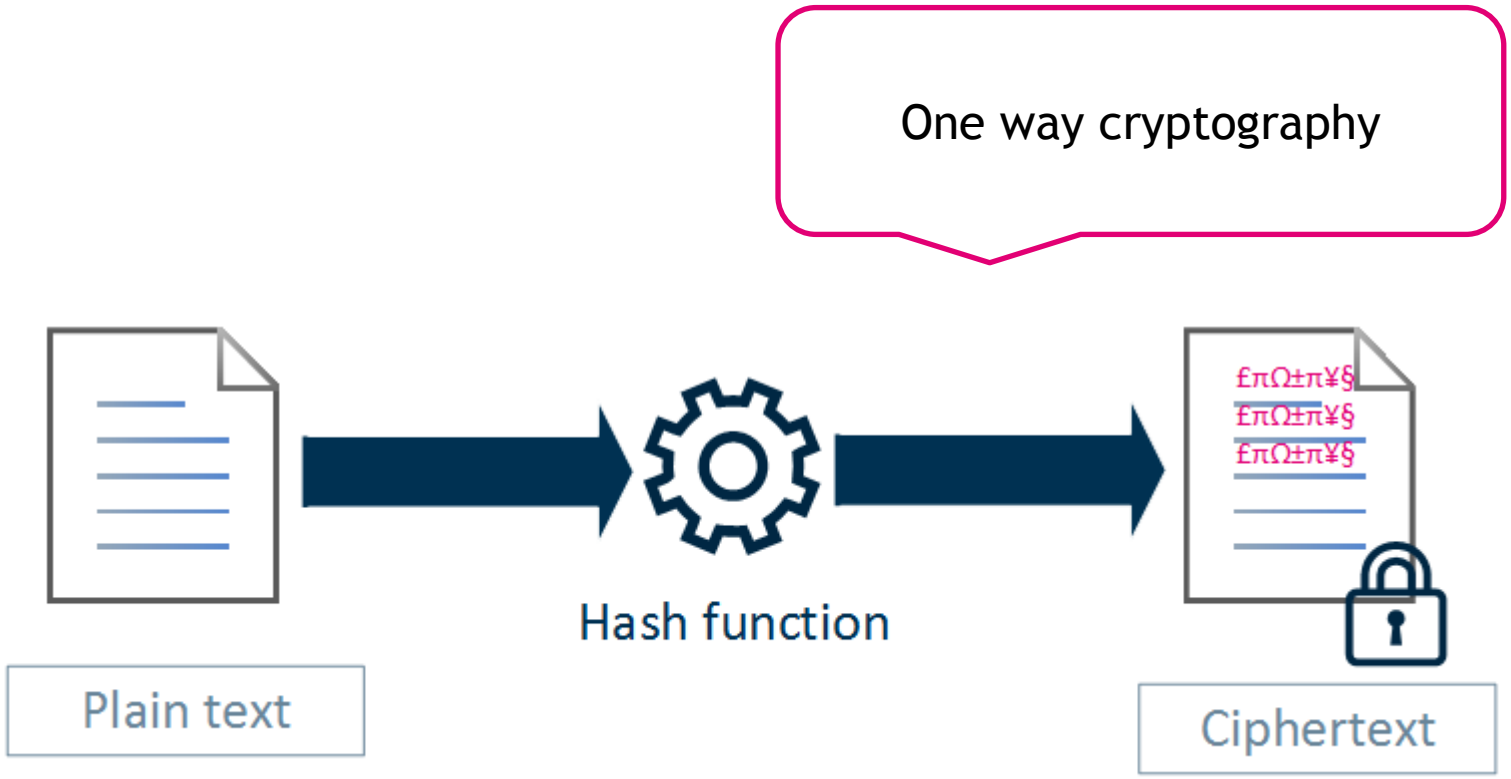
➲ Signing key s only with the sender, test key t public

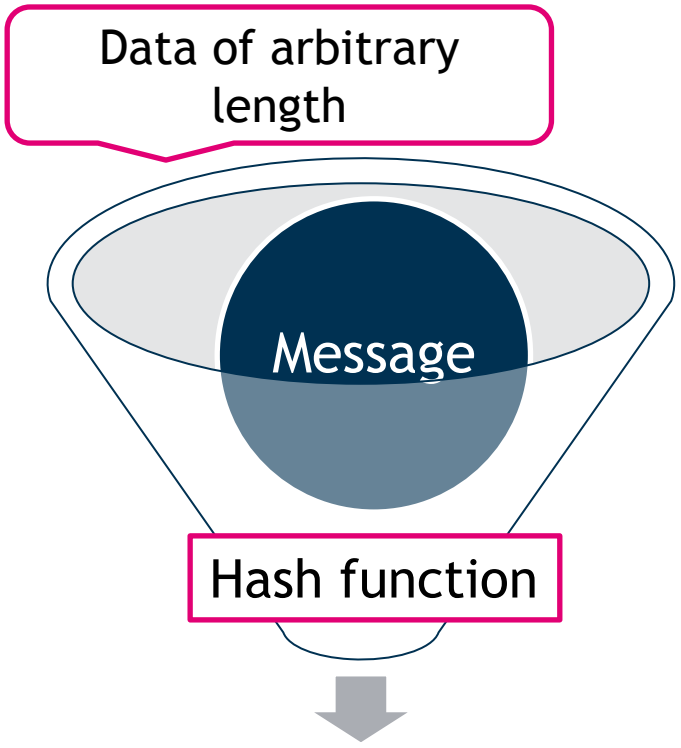
mobile business

Agenda

- Digital Signature Overview
- Algorithms
- Hash Functions
- Electronic Signatures - Legal Framework
- Recent Initiatives in Europe
- Use Case Scenario

Hash Functions





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.

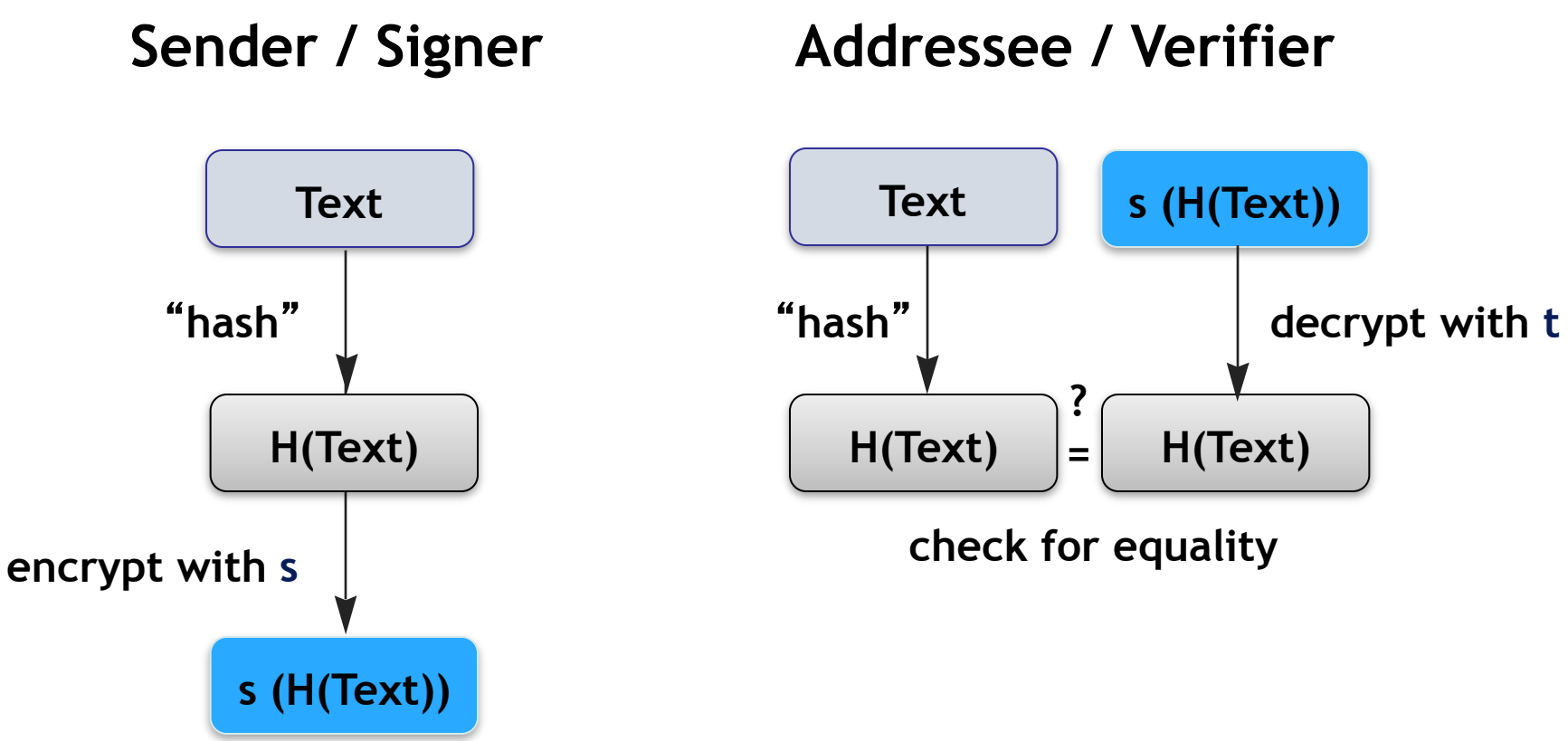
Example: mod 10 in the decimal system

mobile business

Hash Functions

- **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

Asymmetric Signature System (Example RSA)



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

mobile business

Agenda

- Digital Signature Overview
- Algorithms
- Hash Functions
- Electronic Signatures - Legal Framework
- Recent Initiatives in Europe
- Use Case Scenario

Directive 1999/93/EC

- The European Community Directive on electronic signatures refers to the concept of an **electronic signature** as:

> "data in electronic form which attached to, or logically associated with other electronic data and which serves as a method of authentication"

[EC-Directive 1999]

Directive 1999/93/EC

- **The advanced electronic signature** requirements:
  - 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]

Directive 1999/93/EC

The qualified certificate

- .. the identification of the certification service provider;
- the name of the signatory;
- provision for a specific attribute of the signatory to be included if relevant;

- signature-verification data;
- period of validity of the certificate;
- the identity code of the certificate;
- the advanced electronic signature of the issuing CSP.

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

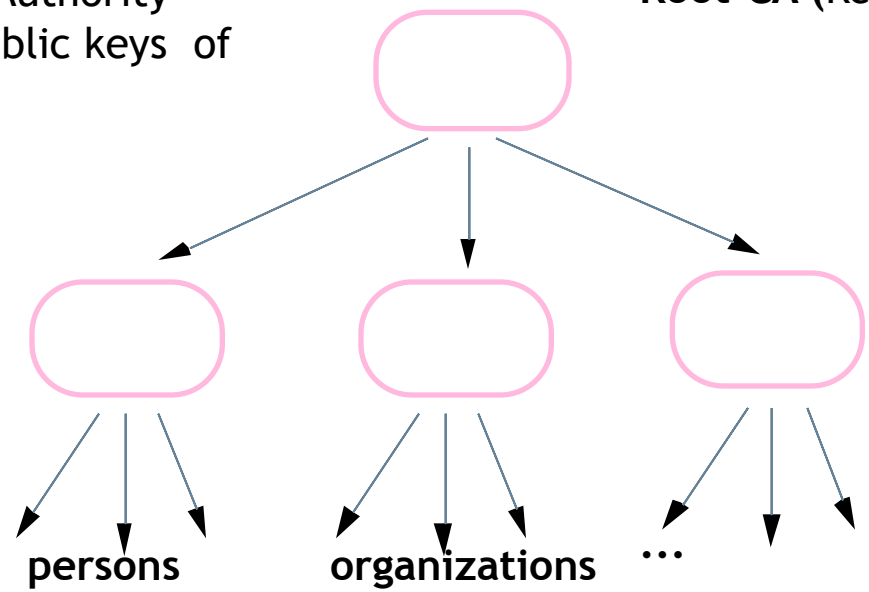
Example: display of data (§ 17(2)) [SigG01]

The signature component must:

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

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

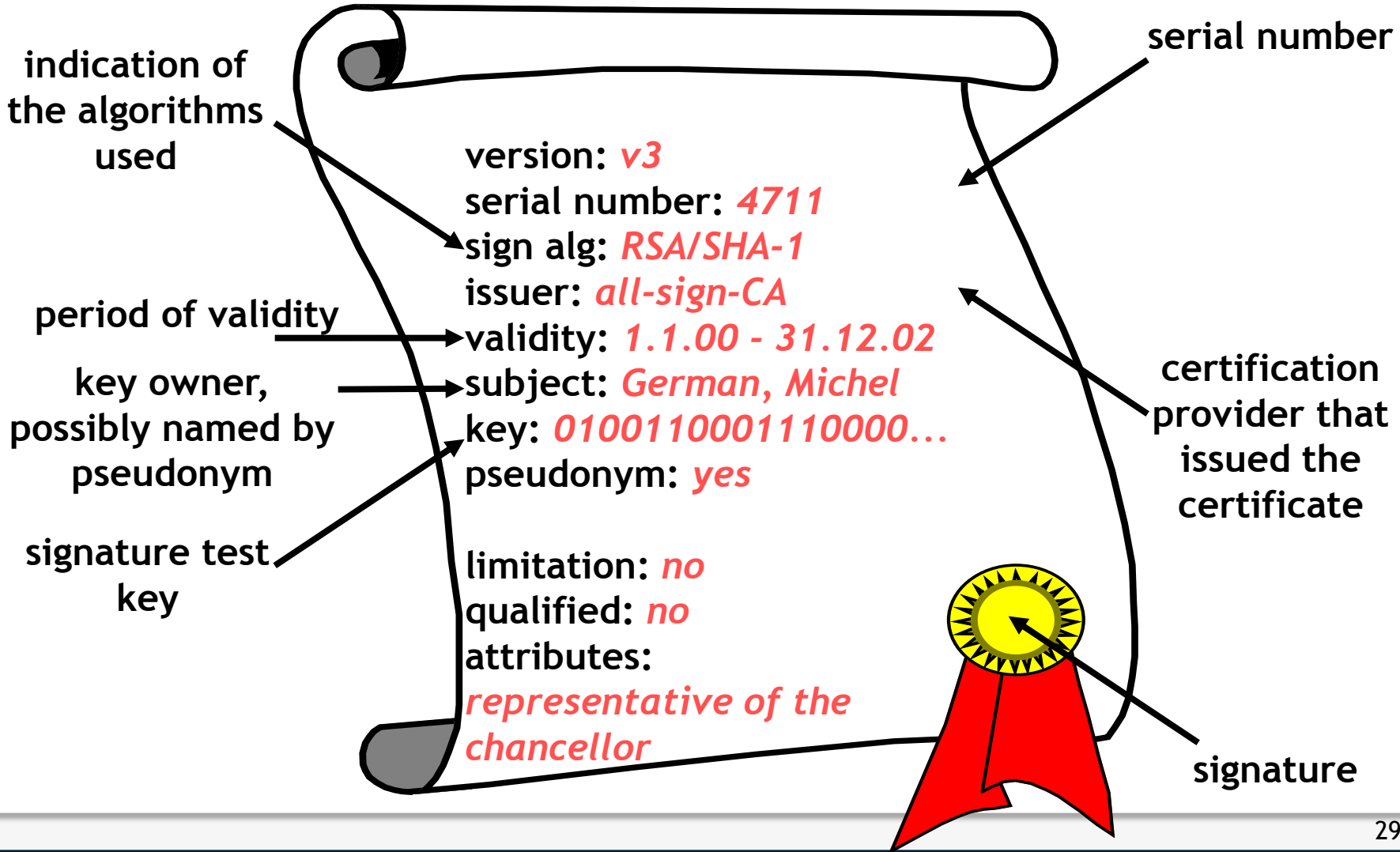
Regulatory Authority confirms public keys of the CAs



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

Content of a Key Certificate

(according to German Signature Law and Regulation)



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

- Reliable identification of persons who apply for a certificate
- Information on necessary methods for fraud resistant creation of a signature
- Provision for secure storage of the private key
  - At least Smartcard (protected with PIN)
- Publication of the certificate (if wanted)
- Barring of certificates
- 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

mobile business

Agenda

- Digital Signature Overview
- Algorithms
- Hash Functions
- Electronic Signatures - Legal Framework
- Recent Initiatives in Europe
- Use Case Scenario

European Initiatives

- 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 12 other European countries. [www.eurosmart.com]

European Initiatives

- 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.

[Fritsch and Roßnagel 2005]

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.

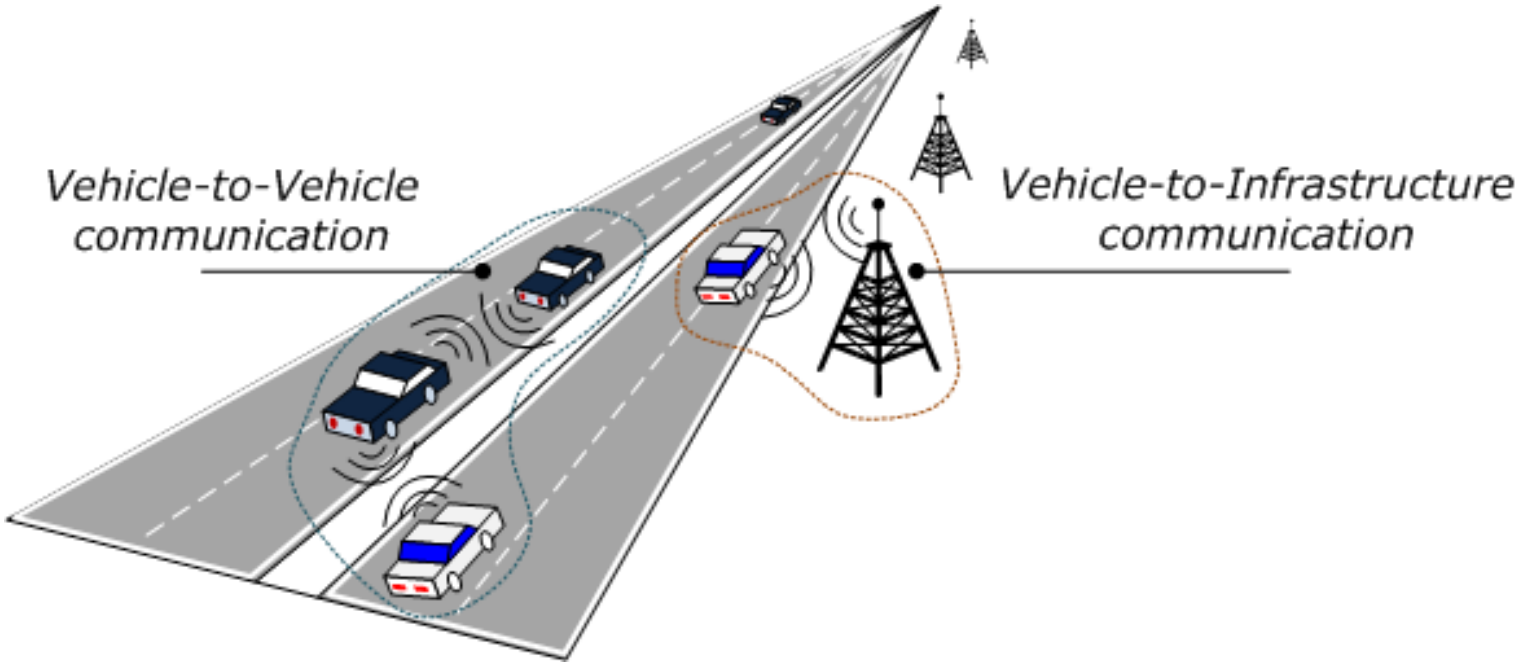
mobile business

Agenda

- Digital Signature Overview
- Algorithms
- Hash Functions
- Electronic Signatures - Legal Framework
- Recent Initiatives in Europe
- Use Case Scenario

Use Case Scenario – Vehicular Ad Hoc Networks (VANETs)

- *"A VANET consists of vehicles and roadside base stations that exchange primarily safety messages to give drivers the time to react to **life-endangering** events"*



VANETs' Applications

Security in VANETs (I)

- Despite the wide number of potential applications, VANETs also raise a broad range of **critical security challenges**.

✧ authentication,

✧ integrity,

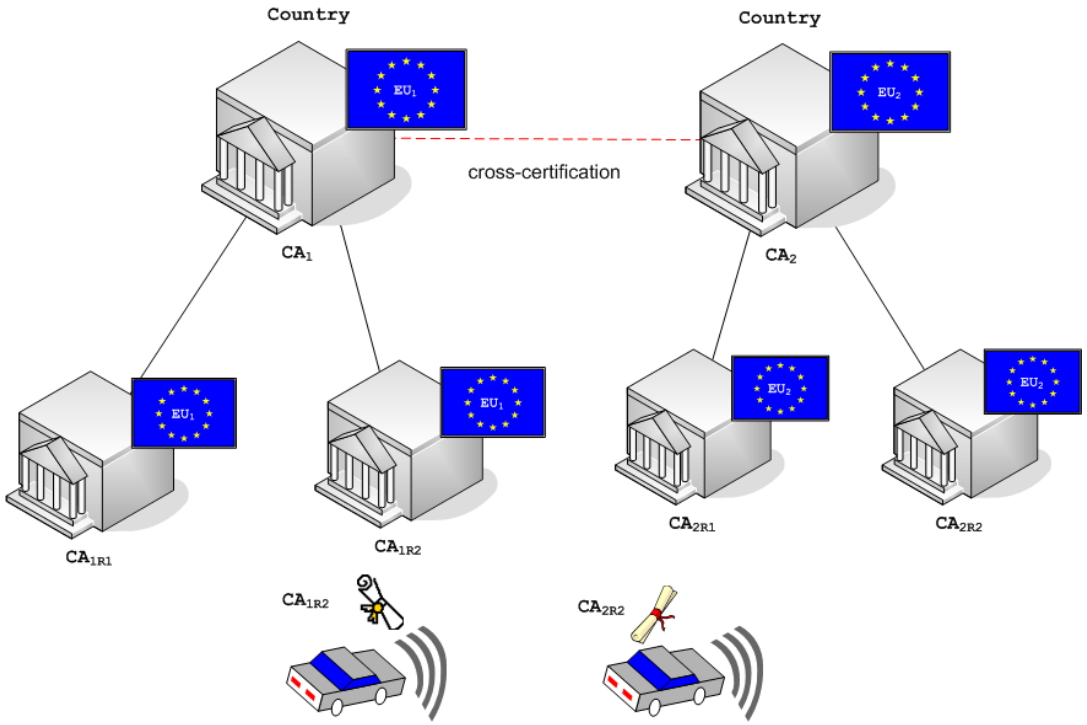
✧ confidentiality,

✧ authorization and,

✧ non-repudiation

Security in VANETs (II)

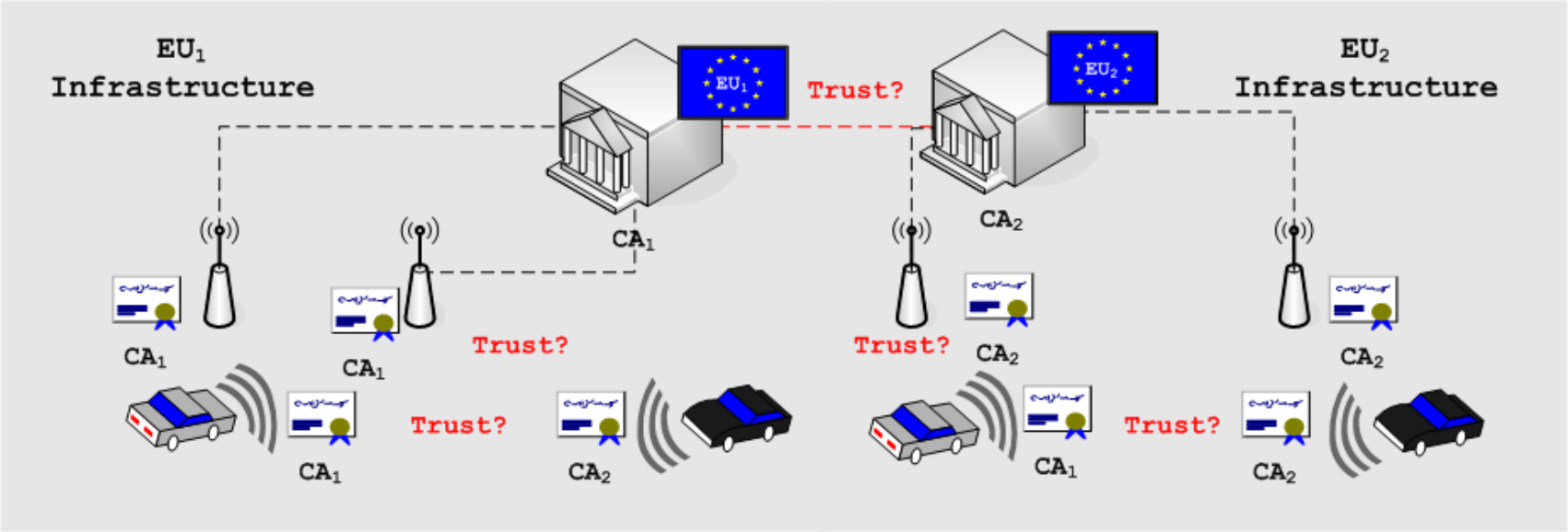
VANETs' PKI (VPKI) relying on a large set of regional Certification Authorities (CAs)



Security IEEE 1609.2 elliptic curves digital signature (ECDSA)

Interoperability

PKI **interoperability** among vehicles from different domains



Literature

- 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.
- 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. (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

Deutsche Telekom Chair of Mobile Business & Multilateral Security

Dr. Jetzabel M. Serna-Olvera
Goethe University Frankfurt
E-Mail: Jetzabel.Serna-Olvera@m-chair.de
WWW: www.m-chair.de