openHPI – Confidential Communication in the Internet

Digital Signatures

Prof. Dr. Christoph Meinel

Hasso Plattner Institute
University of Potsdam, Germany

Signatures (1/2)

Signatures play a central role in traditional life, especially in legal relations, in state administration, in business, in the personal sphere ...

- With classic communication on paper, the written/printed text and the ink of the signature by hand are both undissolvable connected with the paper

What could be a counterpart in digital communication?

Problem:

- The bits carrying a message are not bound to any particular medium …

Signatures (2/2)

Signatures should have the following **characteristics**:

- Authentic – expression of the will of the signee
- Forgery-proof
- Verifiable for authenticity
- Non-reusable and unchangeable
- Legal Binding – not to be disputed

By the way: signatures by hand on paper fulfil these characteristics only moderately well ...

Digital Signatures
Overview (1/2)

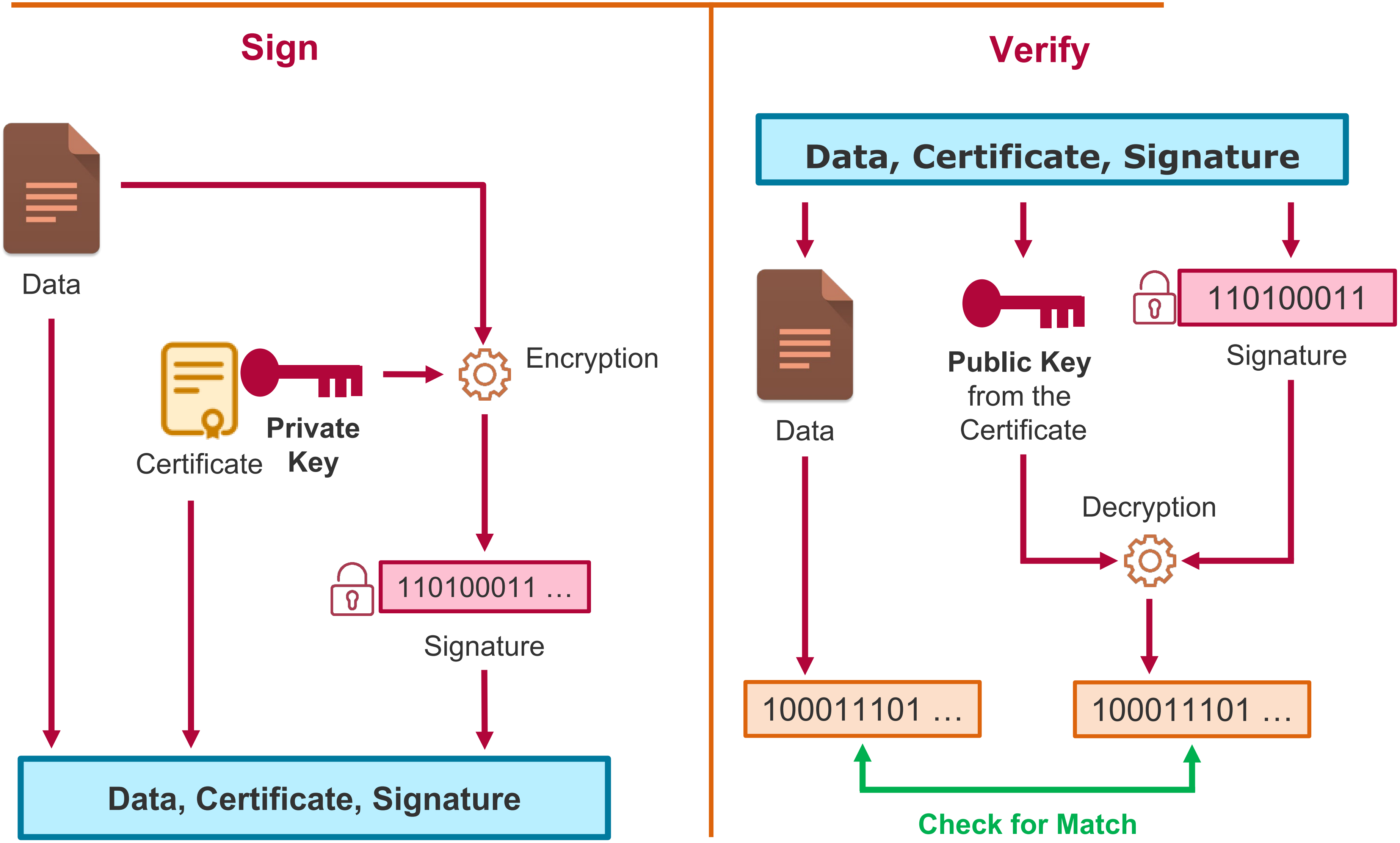
Digital signatures or **electronic signature** are …

- **Cryptoprotocols** that fulfil the requirements for a signature for digital documents
- The **string** generated when a digital signature cryptoprotocol is executed

Digital Signatures consist of the signed document and the digital string by the cryptoprotocol

The common cryptoprotocols for **digital signatures** are mostly based on **public-key cryptosystems**

Digital Signatures
Overview (2/2)



Digital Signatures
Does They Fulfil the Requirements? (1/3)

Authenticity:

- Only Alice can encrypt the message (hash) with her private key such that it can be decrypted with her public key

Forgery-proof

- Alice alone has access to her private key

Verifiable for authenticity

- Everyone – not only Bob – can verify the authenticity by decrypting the digital signature with Alice's public key

Not reusable

- Digital signature is distinctly linked to the "signed" document via encryption

Digital Signatures
Does They Fulfil the Requirements? (2/3)

Unchangeable

- Any change to the digital signature after being decrypted with the public key results in a recognisable distortion
- The signed text is therefore not changeable afterwards

Binding

- Alice alone has acccess to her private key
- If the document can be decrypted with Alice's public key, it must have been encrypted with her private key
- Alice cannot deny her signature

Digital Signatures
Does They Fulfil the Requirements? (3/3)

- Digital signatures provide a viable counterpart to signatures by hand
- If a suitable cryptosystem is chosen, the security of a digital signature is even significantly higher than that of a manual signature ...

Two basic problems remain:

- Encryption of extensive digital documents with a public-key cryptosystem requires enormous computing effort ...
- The recipient who wants to verify the signed document must be sure that he/she really can get the "correct" public key from Alice ...