Trustworthy Communication by Means of Public Key Cryptography

Leibniz Universität Hannover (LUH), Certification Authority (UH-CA)

Birgit F. S. Gersbeck-Schierholz

What is Cryptography?

- Cryptography characterises a process of encrypting information so that its meaning is hidden from unintended recipients. The concept of cryptography exist for as long humans have communicated.
- Over thousands of years many different cryptographic methods have been devised ranging from basic shifting of alphabetical letters to complex mechanical and electronic encryption methods.

Fig. 1 A scytale Source: Wikipedia

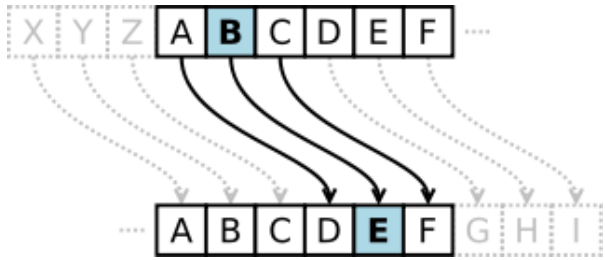

Fig. 2 Caesar cipher Source: Wikipedia

- Symmetric encryption is a cryptographic approach where both the sending and receiving parties are in possession of the (secret) key used to encrypt the data.
- A wide selection of symmetric key algorithms are currently in use, the most established of which are 3DES, IDEA, Blowfish, AES (keylength **128 – 196 Bit**)

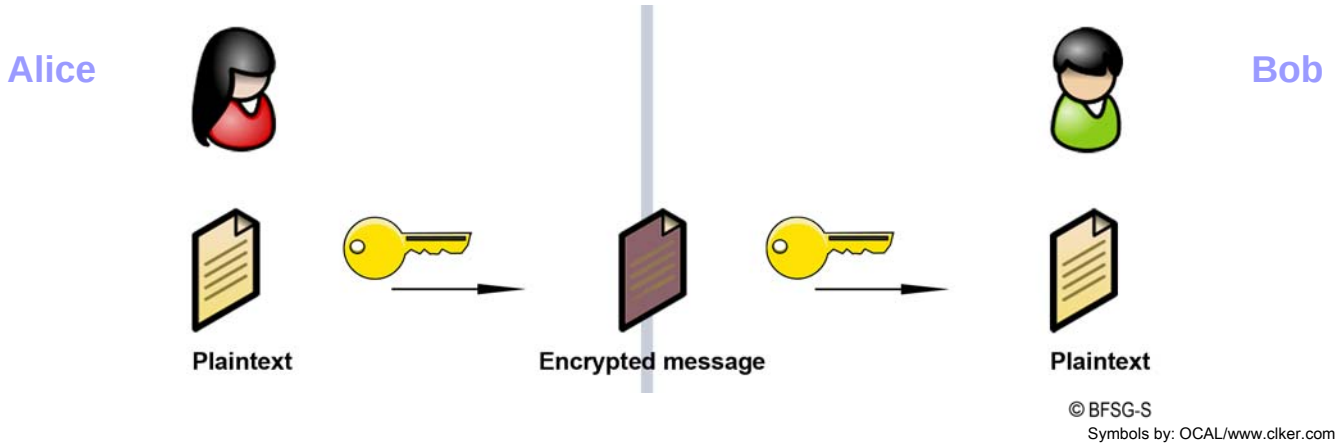

Fig. 3 Symmetric encryption model

- Asymmetric Encryption (also known as Public Key Encryption) was invented in 1975 by Whitfield Diffie and Martin Hellman and make use of two related but different keys, one private and one public. One of the keys in this pair decrypts what the other encrypts. The advantage of asymmetric over symmetric encryption is that the public key can be stored in a public repository without the risk that its interception will compromise encrypted data.

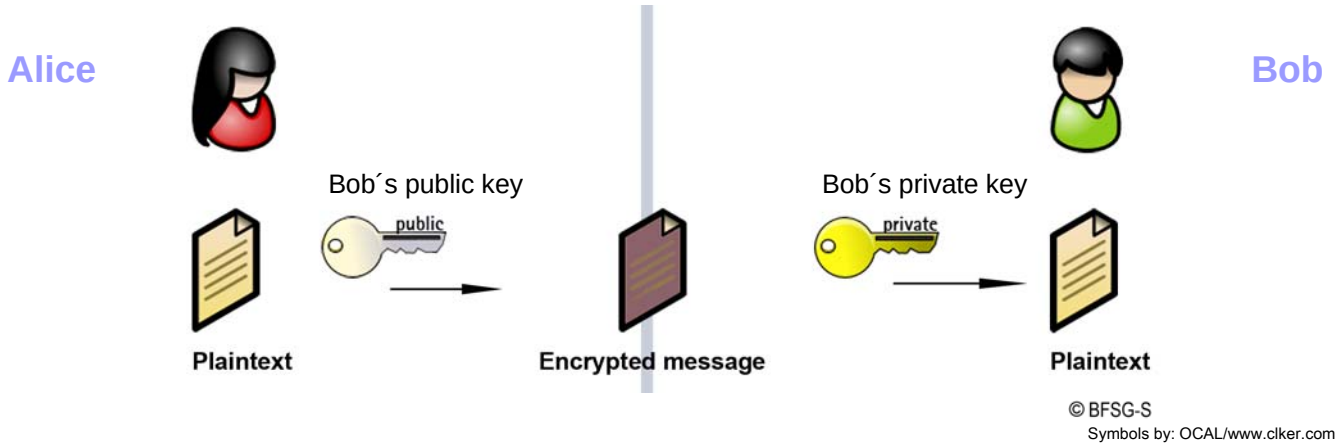

Fig. 4 Asymmetric encryption model

- A number of asymmetric encryption algorithms have been developed since the Diffie and Hellman invented the concept over 30 years ago, the most well-known examples are
  - RSA
  - Diffie-Hellman
  - ElGamal
  - Elliptic Curve Cryptography (ECC)

- The RSA algorithm invented by Ron Rivest, Adi Shamir and Leonard Adleman, was first published in 1977 and works by multiplying two very large prime numbers. Through further mathematical calculations public and private keys are generated.

Fig. 5 Ron Rivest, Adi Shamir, Leonard Adleman Source: Wikipedia

- A hash is a mathematical algorithm designed to perform one-way encryption. That means that once the information has been encrypted there is no way to retrieve the original information from the hashed form. Hashing is commonly used in password files and for ensuring the integrity of data.
- The most common hash methods are as follows:

    - HAVAL (based on MD5)
    - HMAC
    - MD2, MD4, MD5
    - RIPEMD-160
    - SHA-1 (based on MD4)
    - SHA-256 (based on MD4)
    - SHA-512 (based on MD4)
    - SNEFRU

- A digital signature relies on the concept of a key pair in combination with hash functions.
- To verify that a document was signed by the apparent document sender the hash is encrypted using the senders private key. If the recipient is able to decrypt the hash using the senders public key then the message is assured to be authentic [Fig. 6].

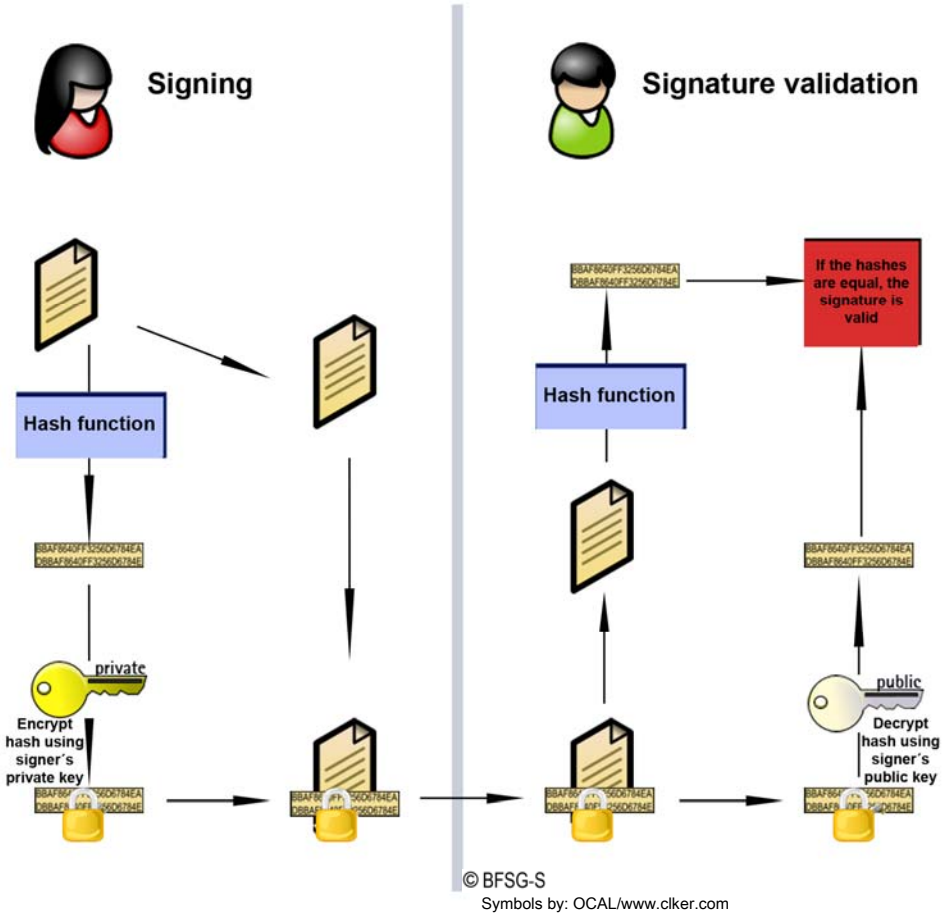

Fig. 6 Digital signature using public key cryptography

- SSL (Secure Socket Layer) and TLS (Transport Layer Security) as an upgrade to SSL Version 3.0, provide endpoint authentication and communications confidentiality over the Internet using a combination of asymmetric cryptography, hash functions, and symmetric cryptography [Fig.].

- When a SSL/TLS connection is established, a handshaking, known as the **SSL/TLS Handshake Protocol**, occurs [Fig.].

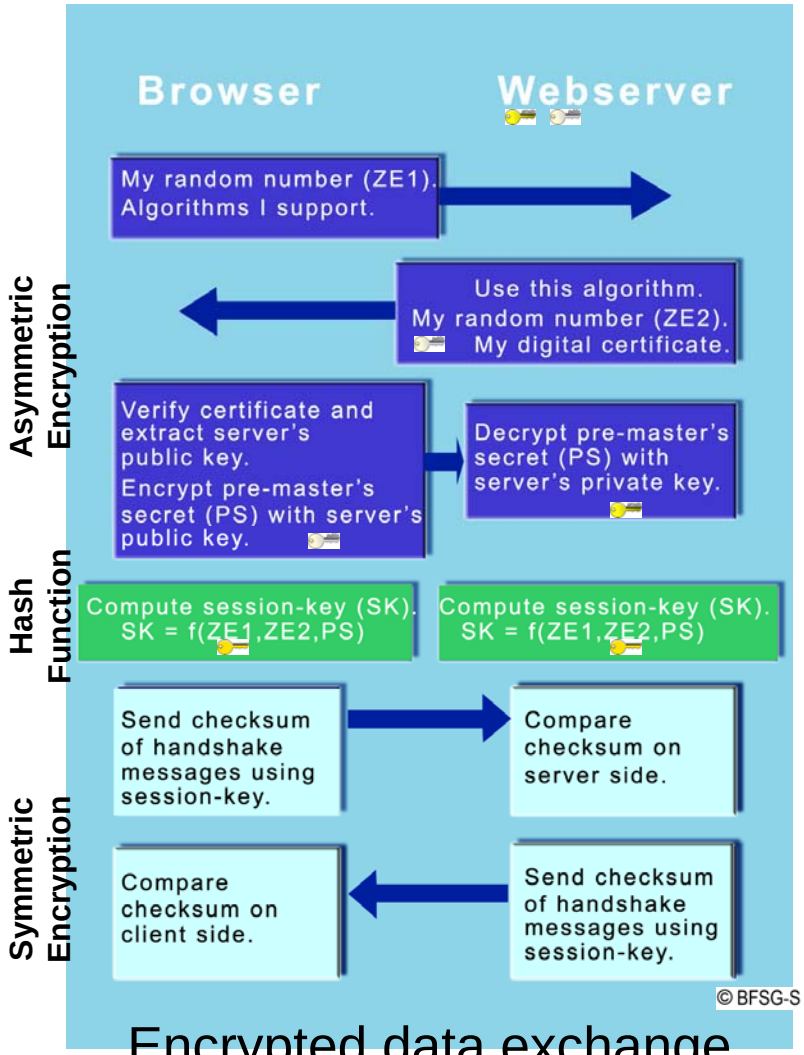

Fig. 7 SSL/TSL handshake scheme

- A PKI solves the problem regarding trust and proof of identity in public key cryptography environments. Without a PKI the sender has no way to validate that the person who provided them with the public key is who they say they are.

- A PKI involves the participation of trusted third parties who verify the identity of the parties wishing to engage in a secure communication through the issuing of digital certificates.

- A trusted third party called a Certificate Authority (CA) verifies the identity of a person or entity and issues a digital certificate which also contains that entities public key. This digital certificate is also referred to as Public Key Certificate (PKC).

- This PKC (and the public key contained therein) may subsequently be used to prove the subject‘s identity and enable secure transactions with other parties.

- **A Public Key Certificate (PKC) binds together real world identity with digital identity.**

- A certificate authority (CA) is the trusted third party responsible for validating the identity of a person. Once the identity has been verified a certificate server generates a digital certificate containing the subject's public key. The digital certificate is then digitally signed with the CA's private key.

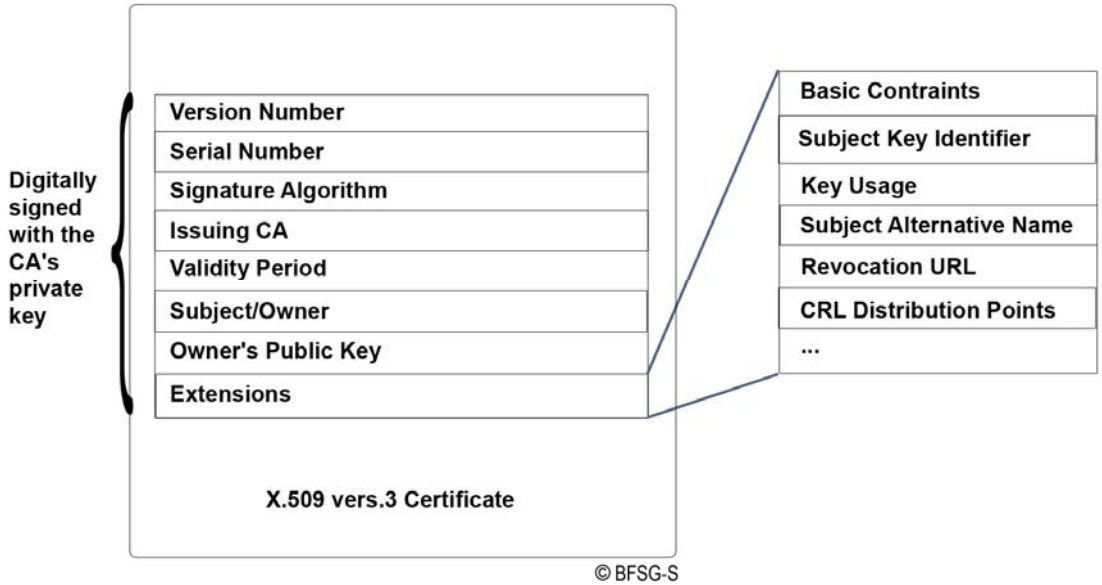

Fig. 8 Public Key Certificate (PKC) Structure

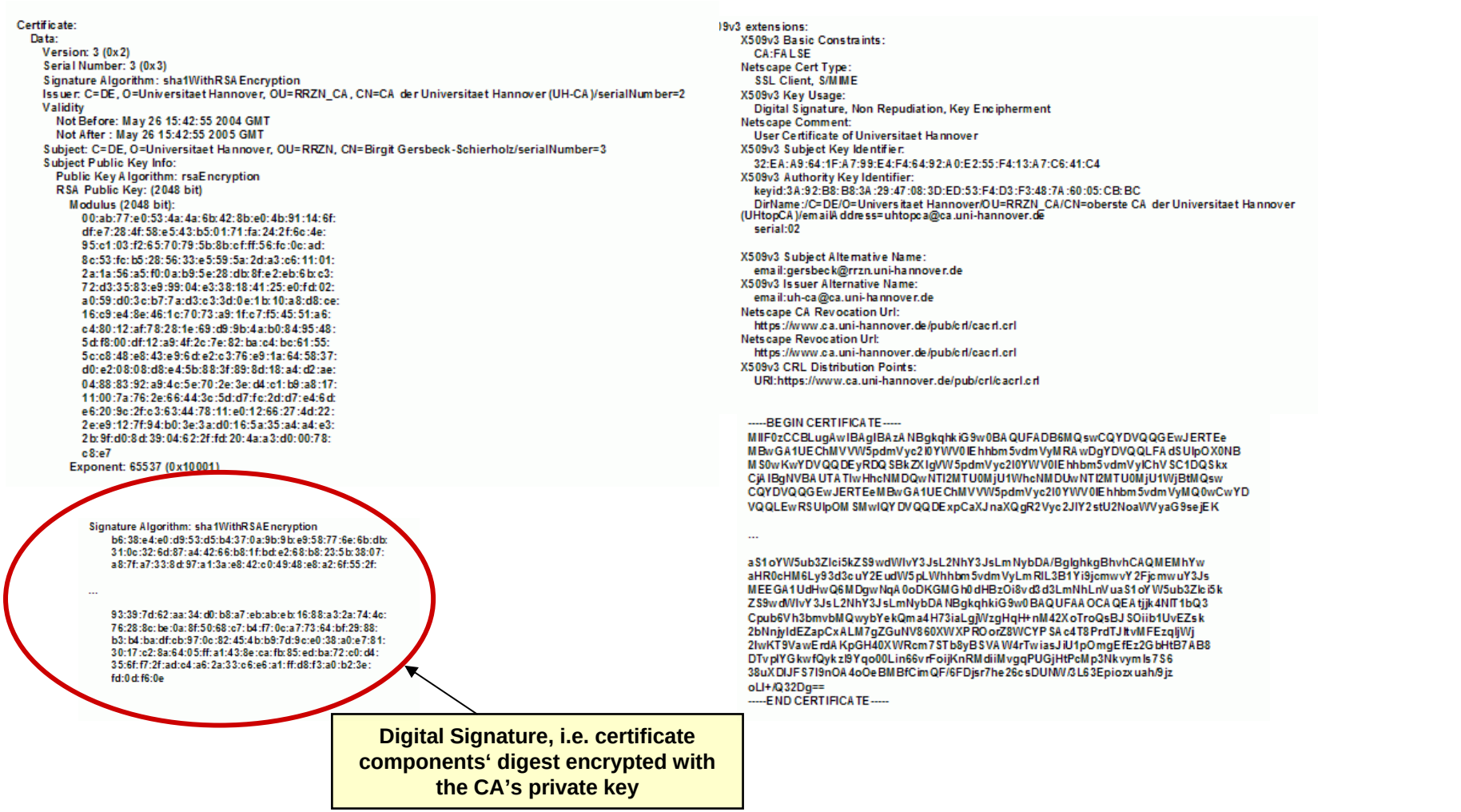

Fig. 9 Public Key Certificate (PKC) specifications

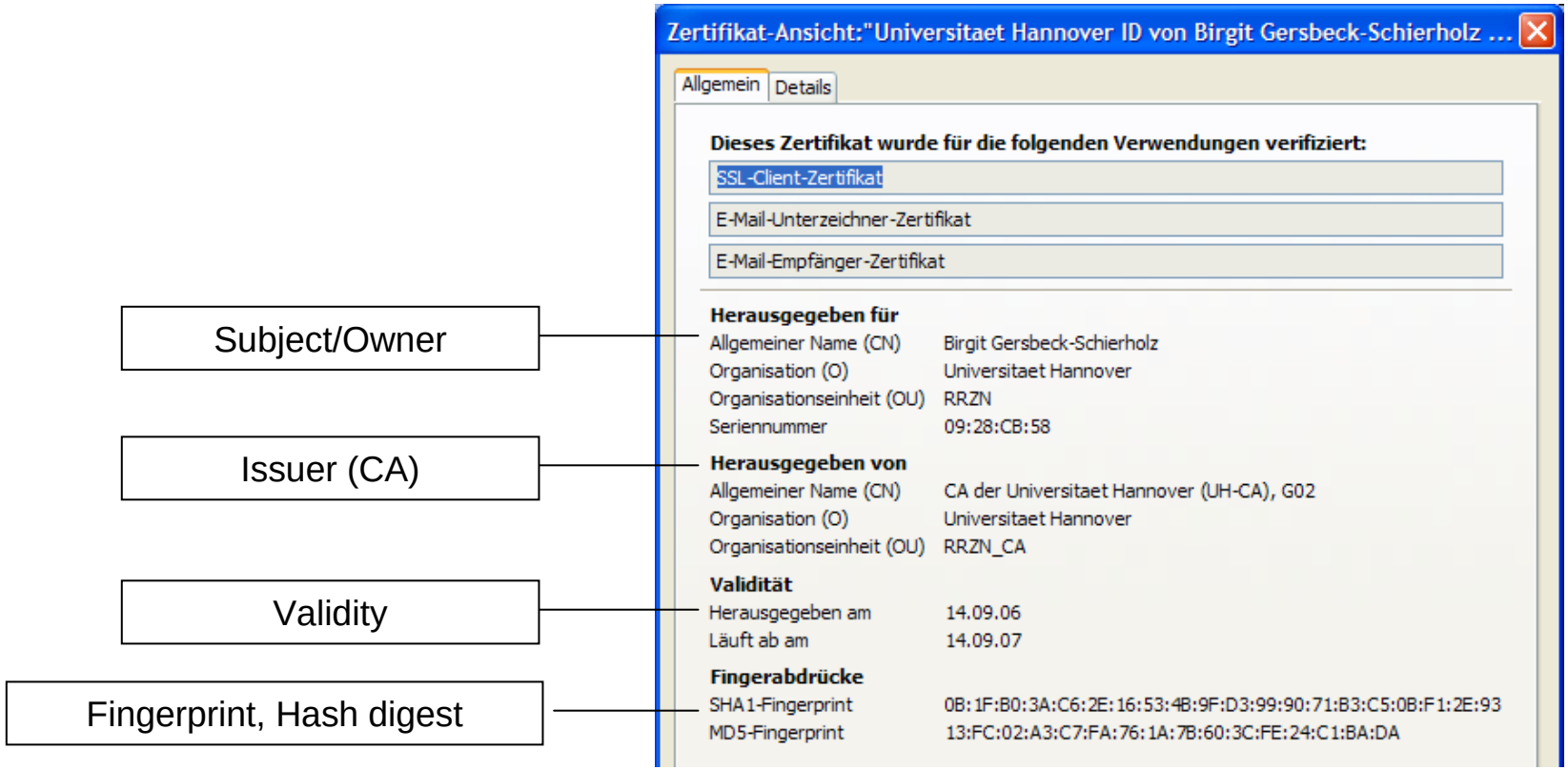

Fig. 10 Browser and mailclient PKC specifications using the example of Mozilla Thunderbird

- The certificate chain of trust, also known as the certification path, is a list of certificates used to authenticate an entity. Each certificate in the chain is signed by the subsequent certificate. The last certificate in the chain is normally a self-signed certificate.

- A path starts with the subject certificate and proceeds through a number of intermediate certificates issued by trusted Certification Authorities (CAs) up to a trusted root certificate, issued by a trusted Root Certification Authority (Root CA) [Fig.].

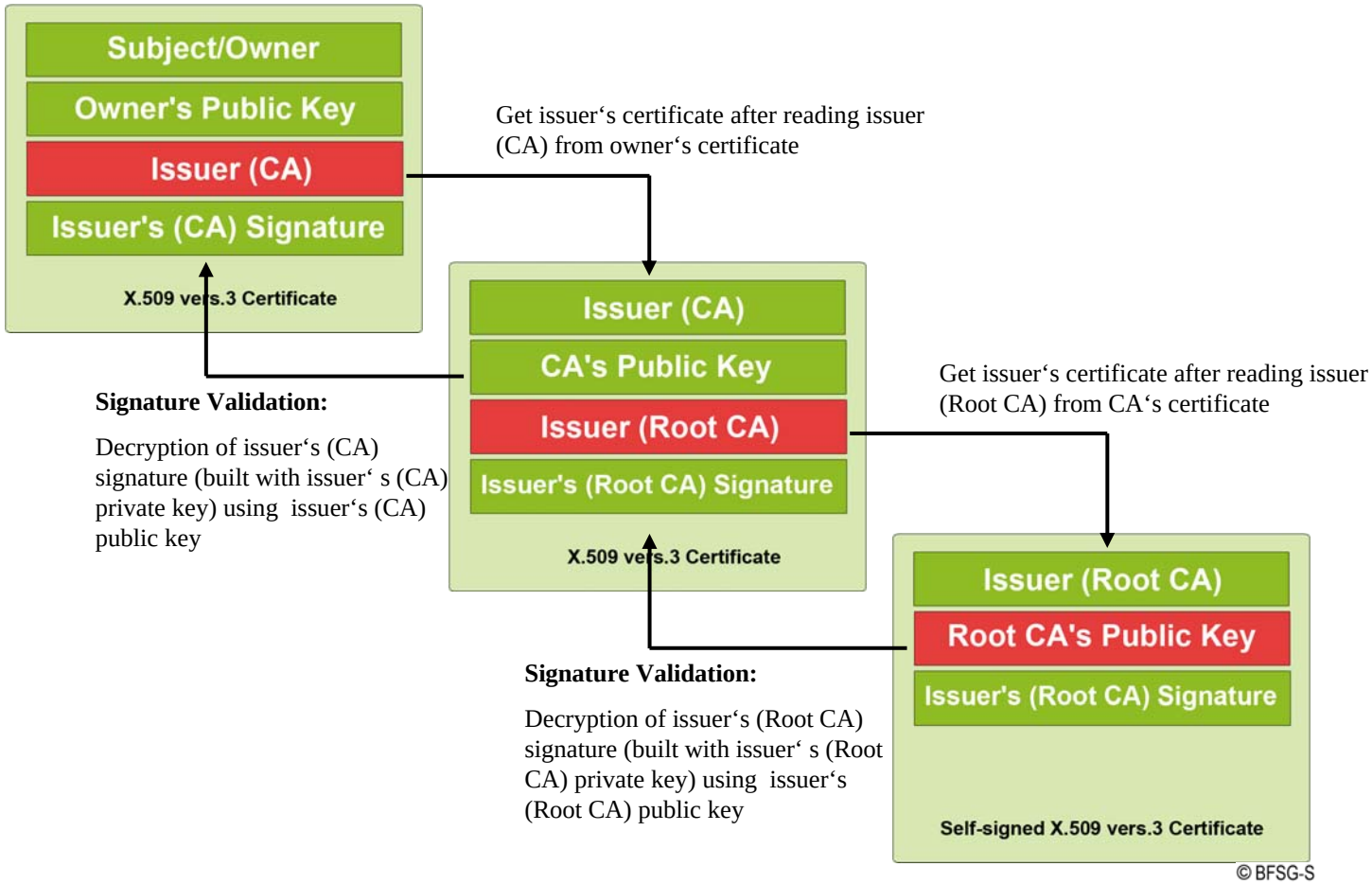

Fig. 11 Certification path from the certificate owner to the root CA, where the chain of trust begins - each certificate in the chain is signed by the entity identified by the next certificate in the chain

- PKI of Deutsches Forschungsnetz (DFN), the German National Research and Education Network, which provides PKI for universities and research institutions in Germany.

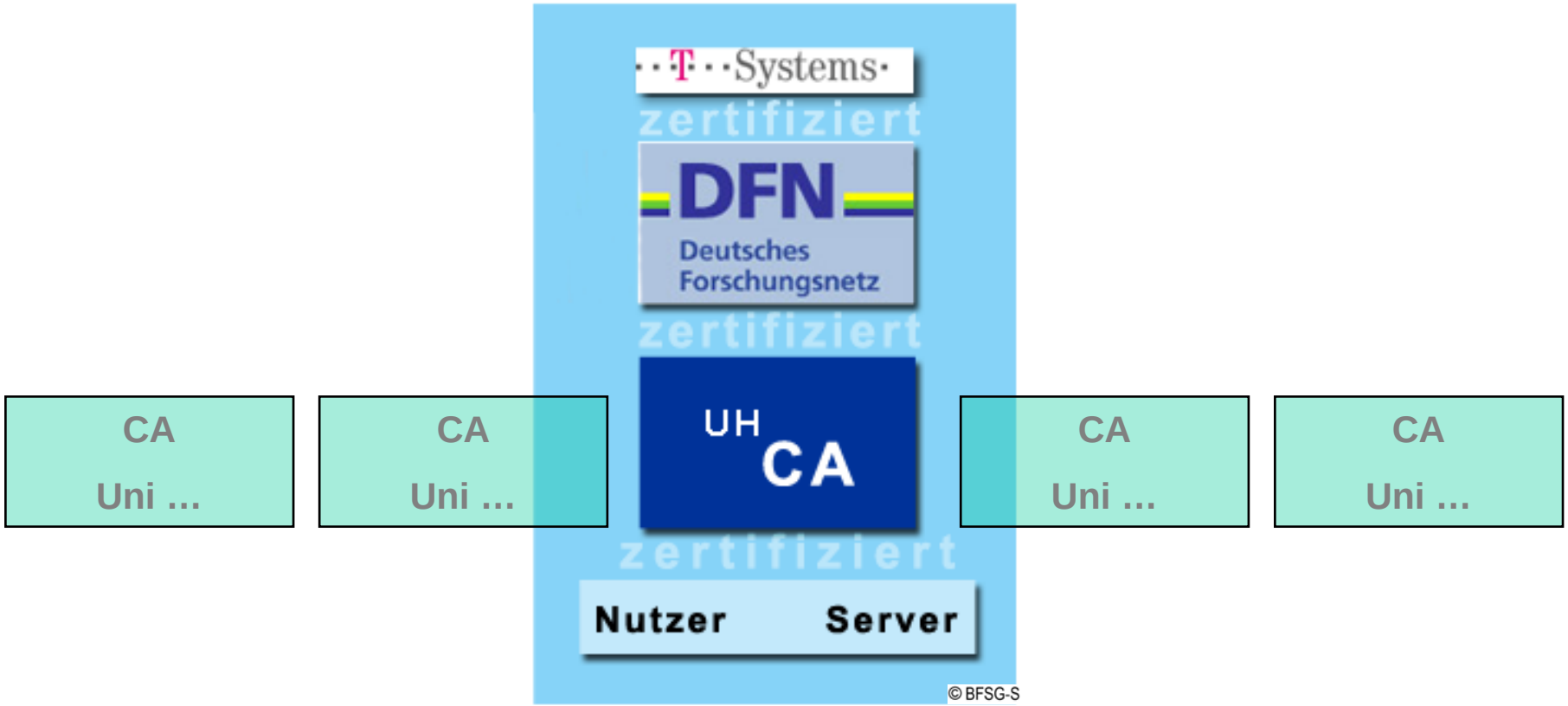

Fig. 12 PKI using the example of Deutsches Forschungsnetz (DFN)

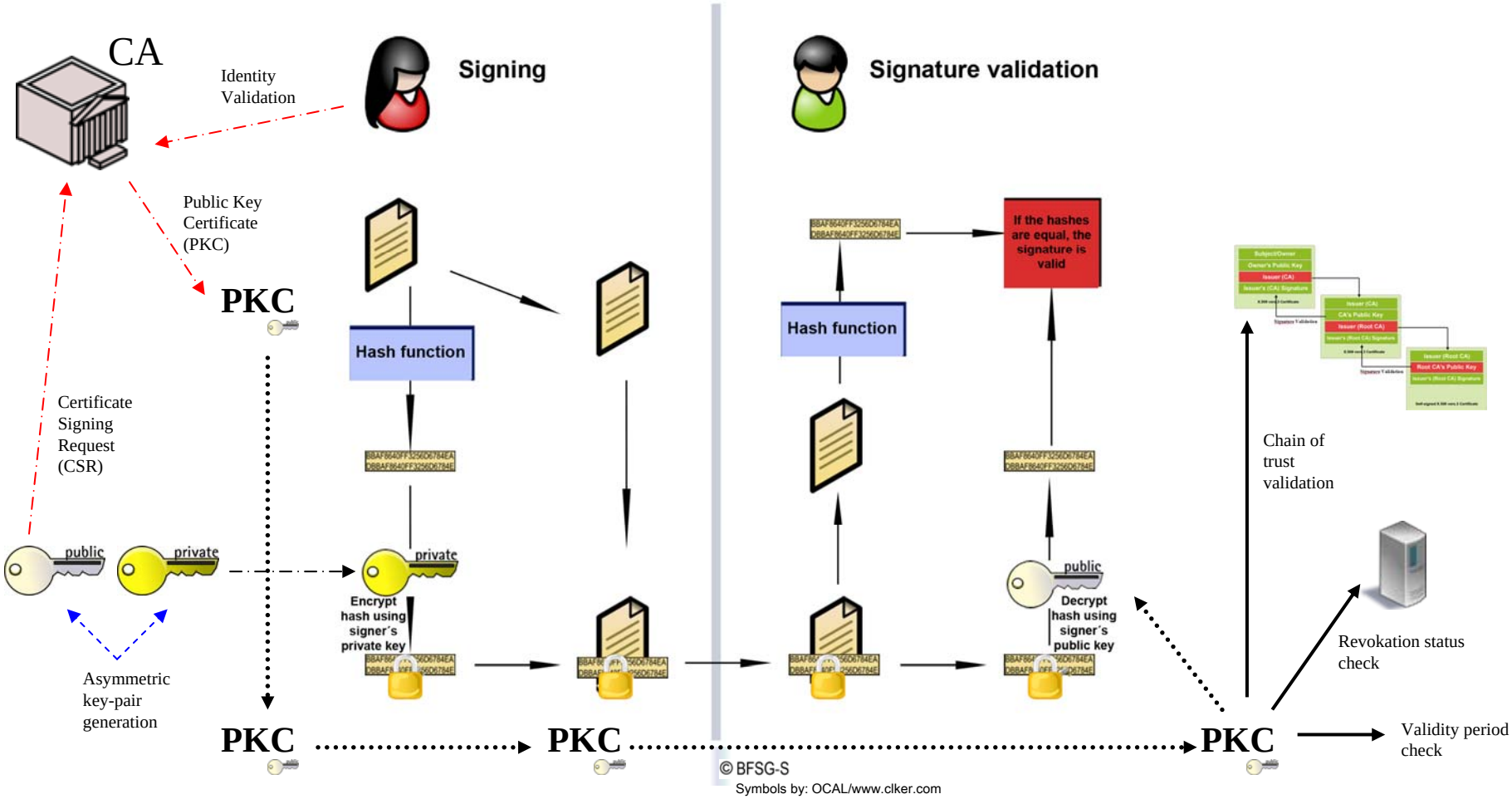

Fig. 13 Digital signature scheme using Public Key Certificates (PKC)

Epilogue

Source: CryptMail User's Guide, Copyright © 1994 Utimaco Belgium