

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

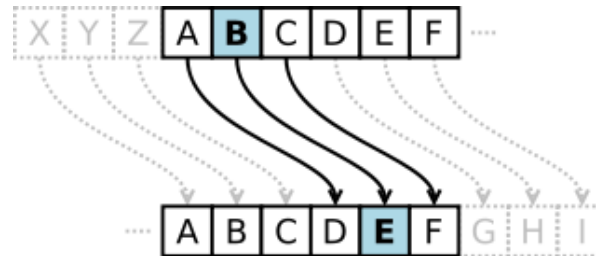


Fig. 2 Caesar cipher Source: Wikipedia

Cryptographic Algorithms

Symmetric Encryption

- 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**)

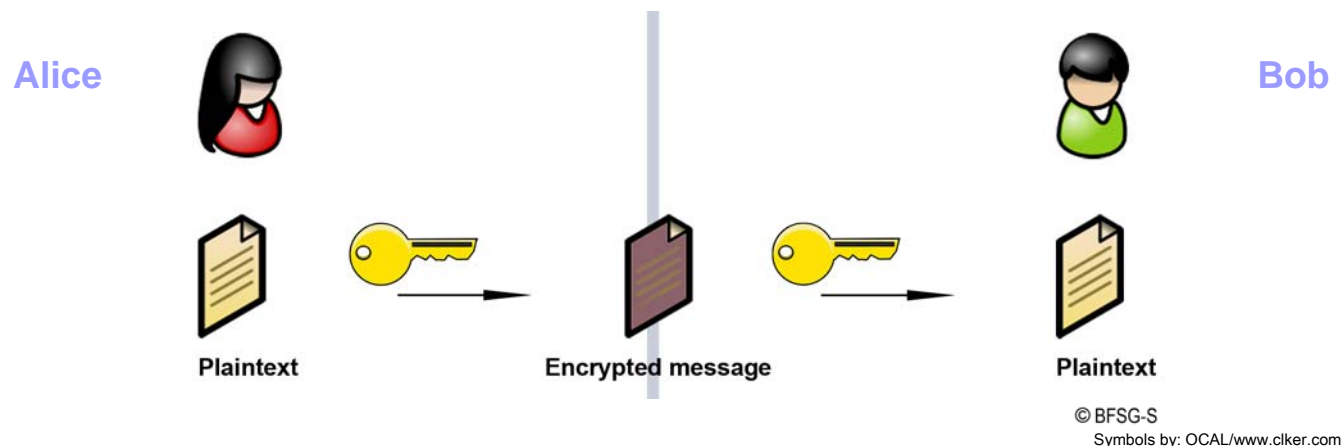


Fig. 3 Symmetric encryption model

Cryptographic Algorithms

Asymmetric Encryption

- 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.

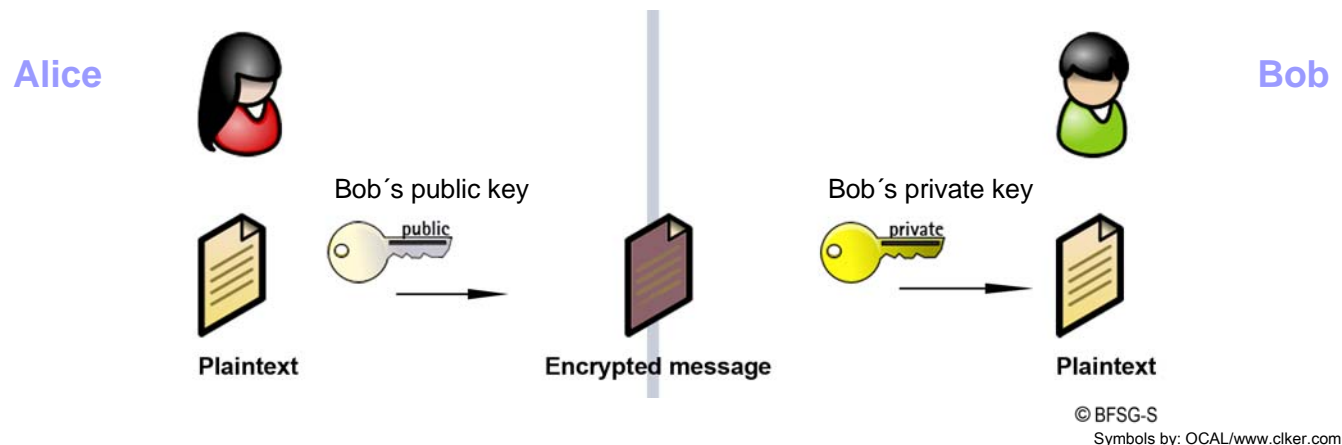


Fig. 4 Asymmetric encryption model

Cryptographic Algorithms

Asymmetric Encryption Algorithms

- 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)

Cryptographic Algorithms

Asymmetric Encryption Algorithms – RSA

- 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

Cryptographic Algorithms

Hashing Algorithm

- 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

Cryptography Usage within the context of information technology

Digital Signature

- 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].

Cryptography Usage within the context of information technology

Digital Signature

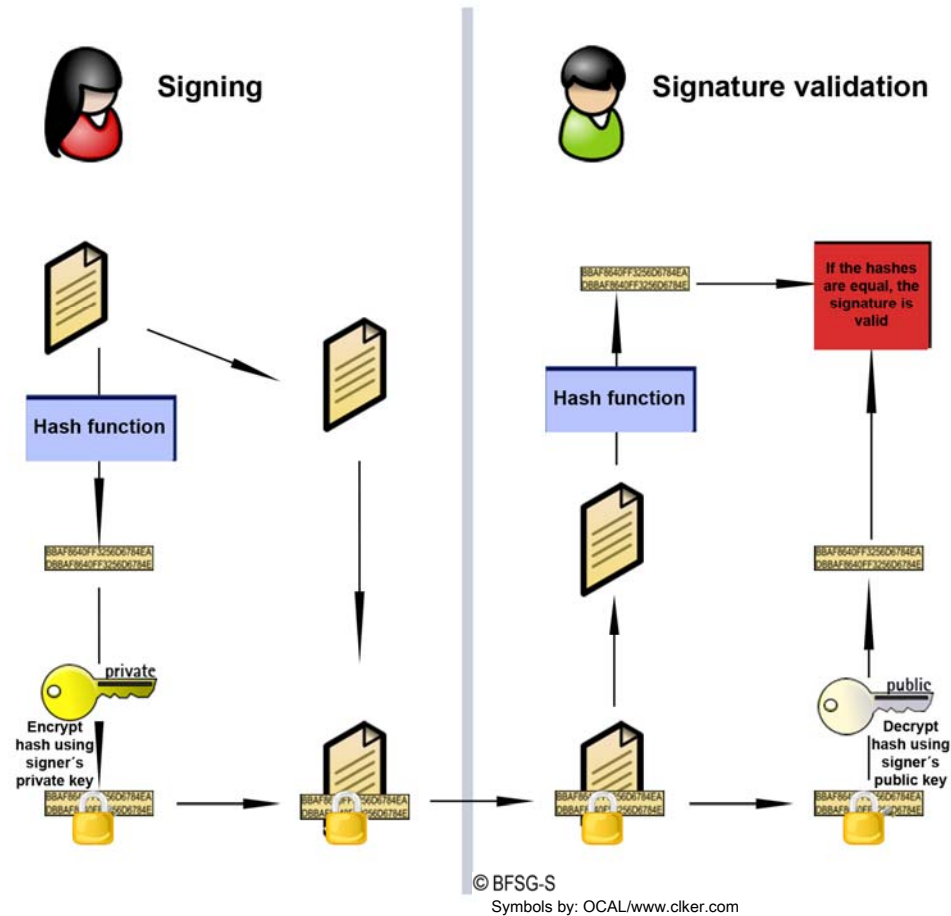


Fig. 6 Digital signature using public key cryptography

Cryptography Usage within the context of information technology

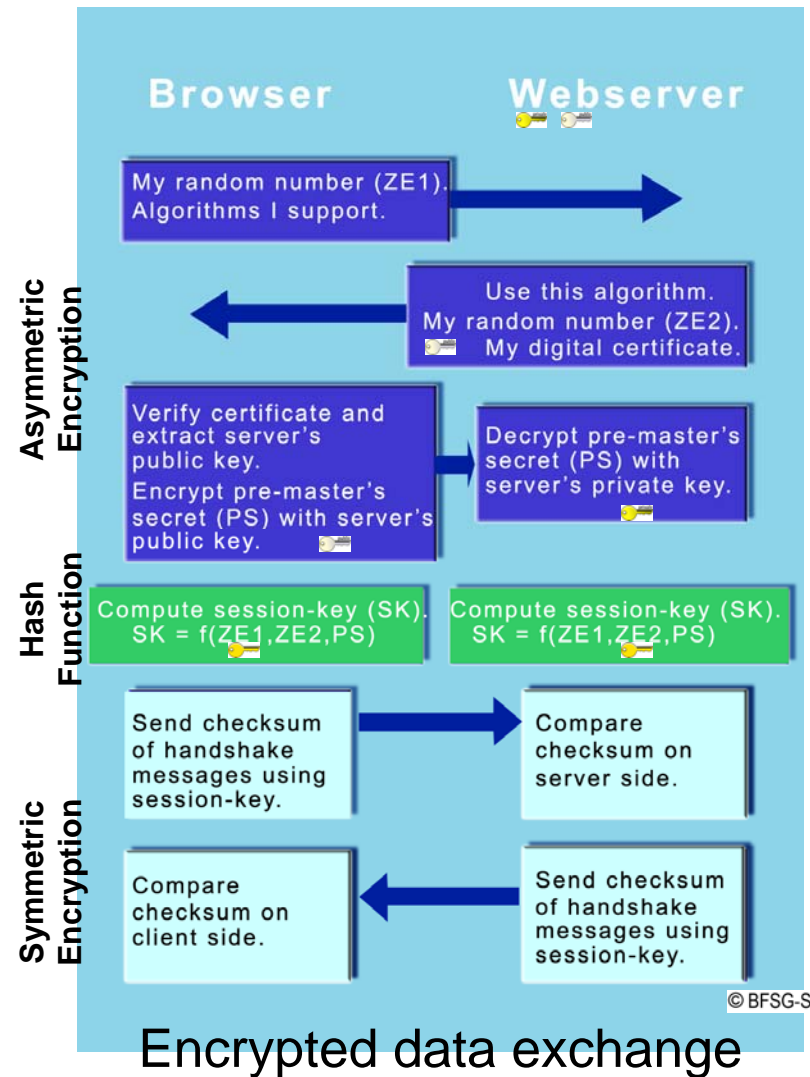
SSL (TLS)

- 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.].

Cryptography Usage within the context of information technology

SSL (TLS)

Fig. 7 SSL/TSL handshake scheme



Cryptography Usage within the context of information technology

Public Key Infrastructure (PKI) – Trust in Public Keys

- 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.**

Cryptography Usage within the context of information technology

Public Key Infrastructure (PKI) – Trust in Public Keys – Digital Certificate Structure

- 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.

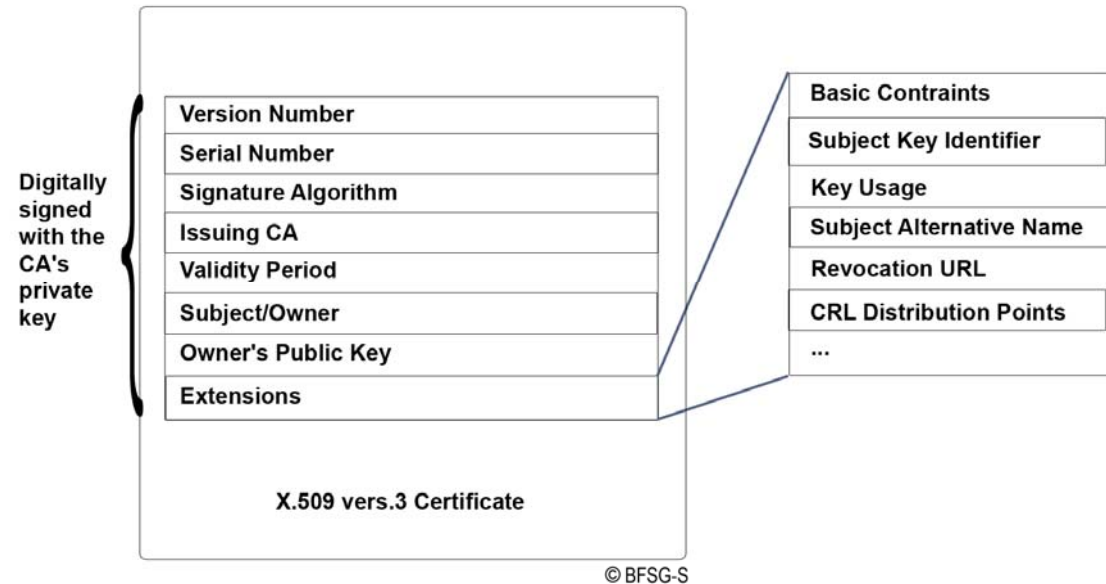


Fig. 8 Public Key Certificate (PKC) Structure

Cryptography Usage within the context of information technology

Public Key Infrastructure (PKI) – Trust in Public Keys – Digital Certificate Structure – Example

```

Certificate:
Data:
  Version: 3 (0x2)
  Serial Number: 3 (0x3)
  Signature Algorithm: sha1WithRSAEncryption
  Issuer: C=DE, O=Universitaet Hannover, OU=RRZN_CA, CN=CA der Universitaet Hannover (UH-CA)/serialNumber=2
  Validity
    Not Before: May 26 15:42:55 2004 GMT
    Not After : May 26 15:42:55 2005 GMT
  Subject: C=DE, O=Universitaet Hannover, OU=RRZN, CN=Birgit Gersbeck-Schierholz/serialNumber=3
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (2048 bit)
      Modulus (2048 bit):
00:ab:77:e0:53:4a:4a:6b:42:8b:e0:4b:91:14:6f:
df:e7:28:4f:58:e5:43:b5:01:71:fa:24:2f:6c:4e:
95:c1:03:f2:65:70:79:5b:8b:c fff:56:fe:0c:ad:
8c:53:fc:b5:28:56:33:e5:59:5a:2d:a3:c6:11:01:
2a:1a:56:a5:f0:0a:b9:5e:28:db:8f:e2:eb:6b:c3:
72:d3:35:83:e9:99:04:e3:38:18:41:25:e0:fd:02:
a0:59:d0:3c:b7:7a:d3:c3:3d:0e:1b:10:a8:d8:ce:
16:c9:e4:8e:46:1c:70:73:a9:1f:c7:f5:45:51:a6:
c4:80:12:af:78:28:1e:69:d9:9b:4a:b0:84:95:48:
5d:f8:00:df:12:a9:4f:2c:7e:82:ba:c4:bc:61:55:
5c:c8:48:e8:43:e9:6d:e2:c3:76:e9:1a:64:58:37:
d0:e2:08:08:d8:e4:5b:88:3f:89:8d:18:a4:d2:ae:
04:88:83:92:a9:4c:5e:70:2e:3e:d4:c1:b9:a8:17:
11:00:7a:76:2e:66:44:3c:5d:d7:fc:2d:d7:e4:6d:
e6:20:9c:2f:c3:63:44:78:11:e0:12:66:27:4d:22:
2e:e9:12:7f:94:b0:3e:3a:d0:16:5a:35:a4:a4:3e:
2b:9f:d0:8d:39:04:62:2f:fd:20:4a:a3:d0:00:78:
c8:e7
  Exponent: 65537 (0x10001)

  Signature Algorithm: sha1WithRSAEncryption
b6:38:e4:e0:d9:53:d5:b4:37:0a:9b:9b:e9:58:77:6e:6b:db:
31:0e:32:6d:87:a4:42:66:b8:1f:bd:e2:68:b8:23:5b:38:07:
a8:7f:a7:33:8d:97:a1:3a:e8:42:c0:49:48:e8:a2:6f:55:2f:
...
93:39:7d:62:aa:34:d0:b8:a7:eb:ab:eb:16:88:a3:2a:74:4c:
76:28:8e:be:0a:8f:50:68:c7:b4:f7:0e:a7:73:64:bf:29:88:
b3:b4:bad:feb:97:0e:82:45:4b:b9:7d:9e:c0:38:a0:e7:81:
30:17:c2:8a:64:05:ff:a1:43:9e:ca:fb:85:ed:ba:72:c0:d4:
35:6f:f7:2f:ad:c4:a6:2a:33:c6:e6:a1:ff:d8:f3:a0:b2:3e:
fd:0d:f6:0e
  
```

19v3 extensions:
 X509v3 Basic Constraints:
 CA:FALSE
 Netscape Cert Type:
 SSL Client, S/MIME
 X509v3 Key Usage:
 Digital Signature, Non Repudiation, Key Encipherment
 Netscape Comment:
 User Certificate of Universitaet Hannover
 X509v3 Subject Key Identifier:
 32:EA:A9:64:1F:A7:99:E4:F4:64:92:A0:E2:55:F4:13:A7:C6:41:C4
 X509v3 Authority Key Identifier:
 keyid:3A:92:B8:B8:3A:29:47:08:3D:ED:53:F4:D3:F3:48:7A:60:05:CB:BC
 DirName:/C=DE/O=Universitaet Hannover/OU=RRZN_CA/CN=oberste CA der Universitaet Hannover
 (UHtopCA)/emailAddress=uhtopca@ca.uni-hannover.de
 serial:02
 X509v3 Subject Alternative Name:
 email:gersbeck@rrzn.uni-hannover.de
 X509v3 Issuer Alternative Name:
 email:uh-ca@ca.uni-hannover.de
 Netscape CA Revocation Url:
 https://www.ca.uni-hannover.de/public/cao.crl
 Netscape Revocation Url:
 https://www.ca.uni-hannover.de/public/cao.crl
 X509v3 CRL Distribution Points:
 URI:https://www.ca.uni-hannover.de/public/crl/ca.crl.crl

-----BEGIN CERTIFICATE-----
MIIF0zCCBLugAwIBAgIBAzaNBgkqhkiG9w0BAQUFADB6MQswCQYDVQQGEwJERTeE
MBwGA1UEChMlVWV5pdmlVyc2I0YVWV0IEhhbm5vdmVvMRAwDgYDVQQLFA dS UlpO X0NB
MS0wKwYDVQQDEyRDRQ SBkZkIglWV5pdmlVyc2I0YVWV0IEhhbm5vdmVvYChV SC1DQ Sxk
CjAIBGNVBAUTA TlwHcNM DQw NtI2MTU0MjU1WWhcNM DUw NtI2MTU0MjU1WjBMBQsw
CQYDVQQGEwJERTeE MBwGA1UEChMlVWV5pdmlVyc2I0YVWV0IEhhbm5vdmVvMjQwCwYD
VQQLERRSUlpOM SMwIQY DVQQDExpCaXJ naXQgR2Vyc2JiY2stU2NoaWVvYyG9sejEK
...
aS1oYW5ub3ZlcisKZS9wdWlvY3J sL2NhY3JsLmNybDA/BglghkgBhvhCAQMEMhYw
aHR0cHM6Ly93d3cuY2EudW5pLWVhbM5vdmVvLmRIL3B1Yi9jcmwvY2FjcmmwY3Js
MEEGA1UdHwQ6MDgwN0a0DKGMGH0dHBzOi8vd3d3LmNhLnVuaS1oYW5ub3ZlcisK
ZS9wdWlvY3JsL2NhY3JsLmNybDA NBgkqhkiG9w0BAQUFAOQA QEA QEA tjik4Nt1bQ3
Cpub6Vh3bmvbMQwybYe kQma4H73iaLgJWzghQh+ nM42XoTroQsBJ SOiib1UvEzsk
2bNnjyIdEZapCxALM7gZGuNV860XWXP RO orZ8WCYP SA c4T8PrdTJ ItvMFEzqjWj
2twKT9Va wErDA KpGH40XWRcm7STb8yB SVA W4rTwasJ iU1pO mgEFez2GbhB7AB8
DtvplYg kwfQyk zBY qo0L in66vrfOijKnRM diM vqgPUGjHTpCMp3NkvymIs7S6
38uXDIJF S7I9nOA 4oOe BM BFCm QF/6FJsr7he26csDUINW/3L63Epiozxuah9jz
oLH+IQ32Dg==
-----END CERTIFICATE-----

Digital Signature, i.e. certificate components' digest encrypted with the CA's private key

Fig. 9 Public Key Certificate (PKC) specifications

Cryptography Usage within the context of information technology

Public Key Infrastructure (PKI) – Trust in Public Keys – Browser and mailclient specifications

Subject/Owner

Issuer (CA)

Validity

Fingerprint, Hash digest

Zertifikat-Ansicht: "Universitaet Hannover ID von Birgit Gersbeck-Schierholz ...

Allgemein Details

Dieses Zertifikat wurde für die folgenden Verwendungen verifiziert:

- SSL-Client-Zertifikat
- E-Mail-Unterzeichner-Zertifikat
- E-Mail-Empfänger-Zertifikat

Herausgegeben für

Allgemeiner Name (CN)	Birgit Gersbeck-Schierholz
Organisation (O)	Universitaet Hannover
Organisationseinheit (OU)	RRZN
Seriennummer	09:28:CB:58

Herausgegeben von

Allgemeiner Name (CN)	CA der Universitaet Hannover (UH-CA), G02
Organisation (O)	Universitaet Hannover
Organisationseinheit (OU)	RRZN_CA

Validität

Herausgegeben am	14.09.06
Läuft ab am	14.09.07

Fingerabdrücke

SHA1-Fingerprint	0B:1F:B0:3A:C6:2E:16:53:4B:9F:D3:99:90:71:B3:C5:0B:F1:2E:93
MD5-Fingerprint	13:FC:02:A3:C7:FA:76:1A:7B:60:3C:FE:24:C1:BA:DA

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

Cryptography Usage within the context of information technology

Public Key Infrastructure (PKI) – Trust in Public Keys – Chain of Trust

- 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.].

Cryptography Usage within the context of information technology

Public Key Infrastructure (PKI) – Trust in Public Keys – Chain of Trust

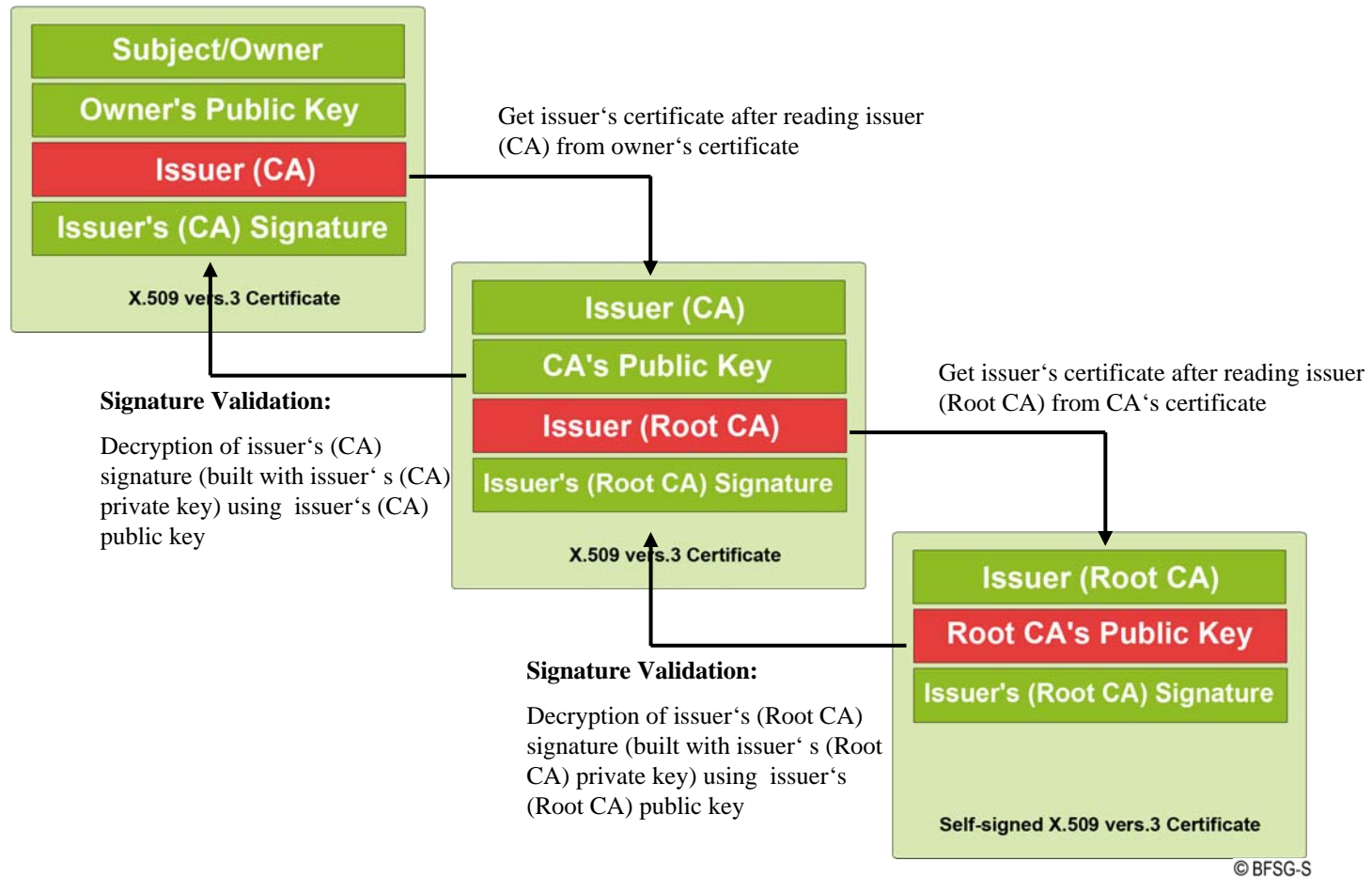


Fig. 11 Certification path from the certificate owner to the root CA, where the chain of trust begins - each certificate in the chain is signed by the entity identified by the next certificate in the chain

Cryptography Usage within the context of information technology

Public Key Infrastructure (PKI) – Trust in Public Keys – Chain of Trust

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

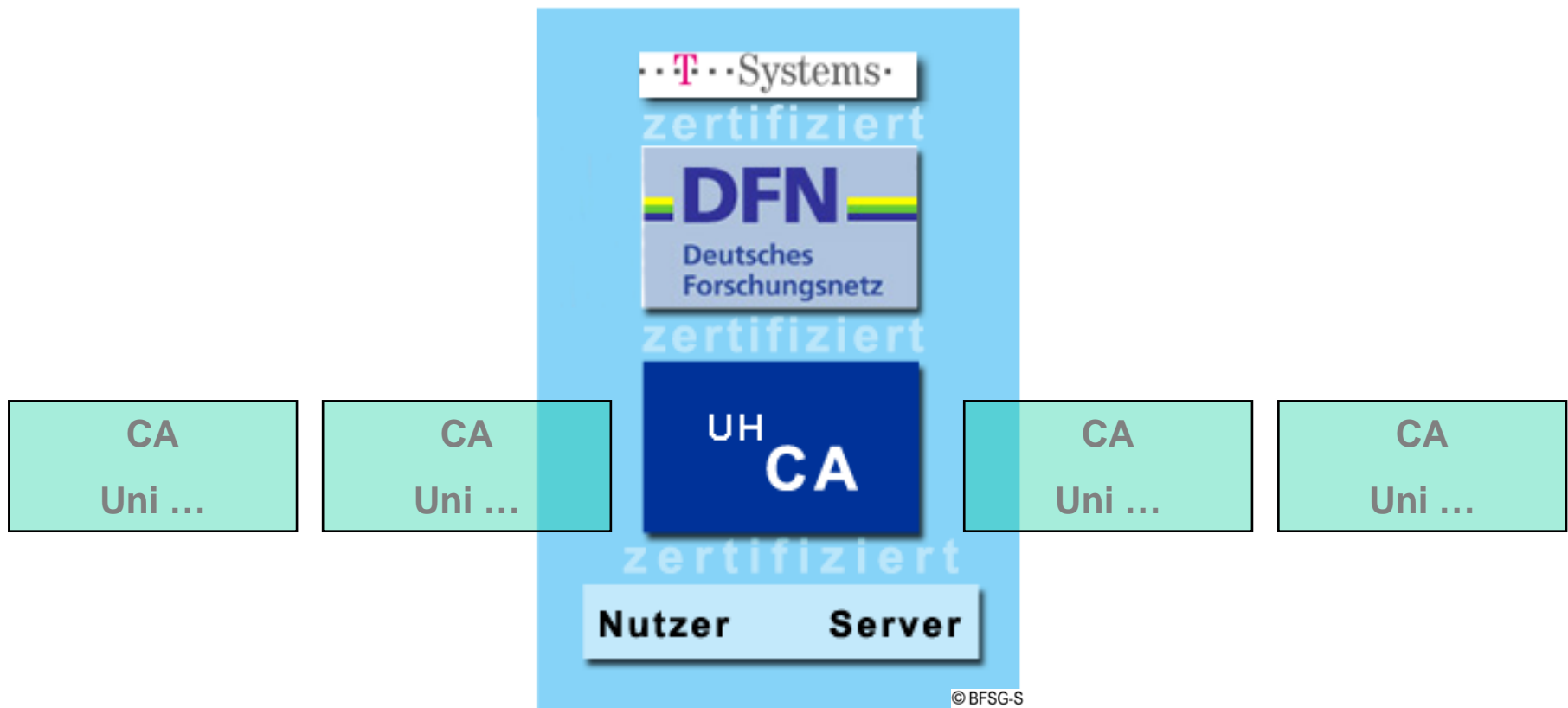


Fig. 12 PKI using the example of Deutsches Forschungsnetz (DFN)

Cryptography Usage within the context of information technology

Public Key Infrastructure (PKI) – Object Signing and Signature Validation

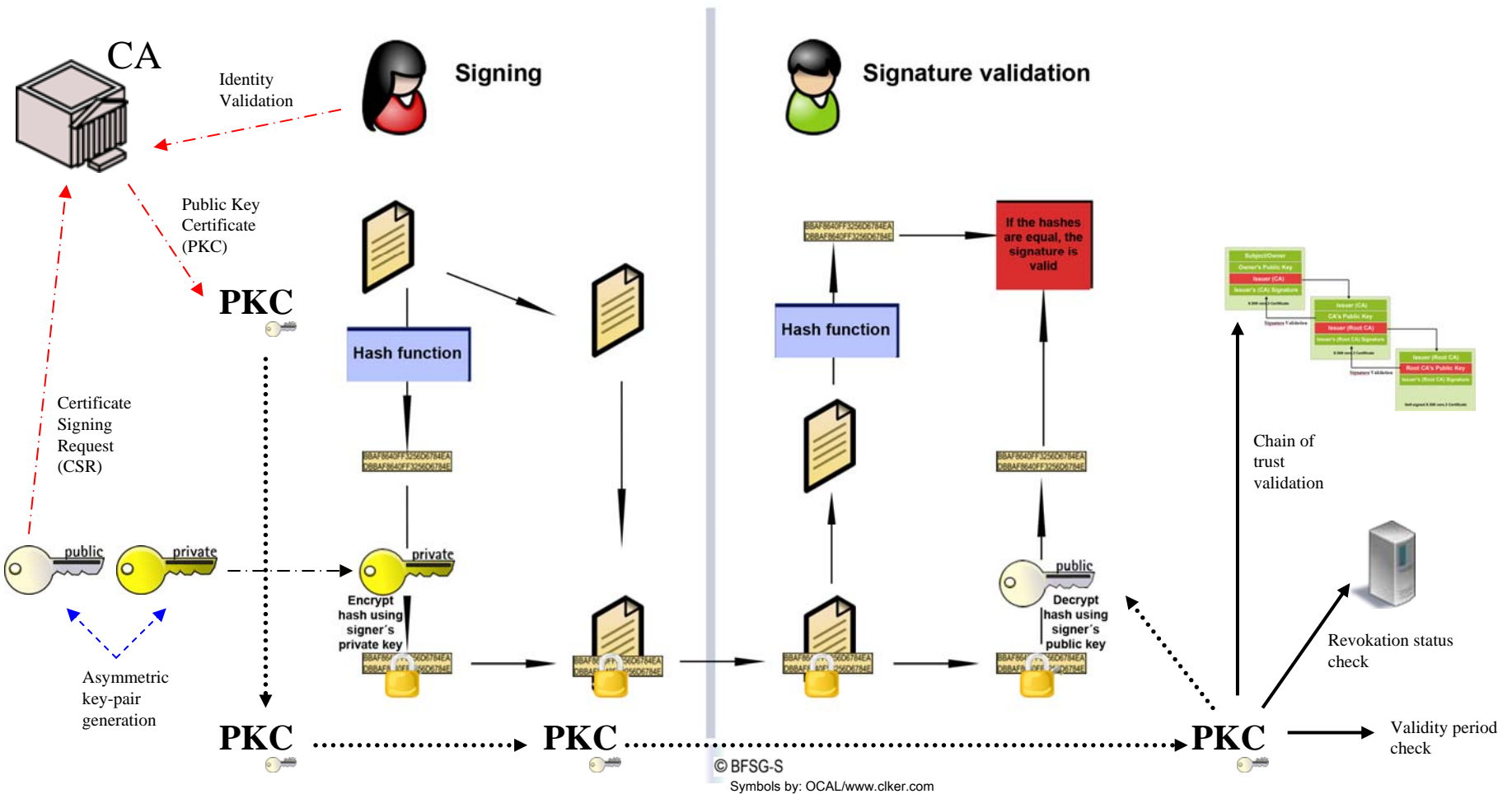


Fig. 13 Digital signature scheme using Public Key Certificates (PKC)

Trustworthy Communication by Means of Public Key Cryptography Epilogue



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