Certificates

Chapter 1

Cryptography Engineering

Gildas Avoine

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES RENNES

IUF

SUMMARY OF CHAPTER 1

- Fundamentals
- Certificates X.509
- Certificate Examples
- Obtaining a Certificate
- Verifying a Certificate
- Conclusion and Further Reading

FUNDAMENTALS

- Fundamentals
- Certificates X.509
- Certificate Examples
- Obtaining a Certificate
- Verifying a Certificate
- Conclusion and Further Reading

Basics

- The goal of a certificate is to link a public-key with its owner.
- The pair (public key, owner) is signed by a trusted party.

Basics

- The goal of a certificate is to link a public-key with its owner.
- The pair (public key, owner) is signed by a trusted party.
- The trusted party is named Certification Authority (CA).

Basics

- The goal of a certificate is to link a public-key with its owner.
- The pair (public key, owner) is signed by a trusted party.
- The trusted party is named Certification Authority (CA).
- To check the signature, the CA public-key is needed:
  - Snake biting its tail!

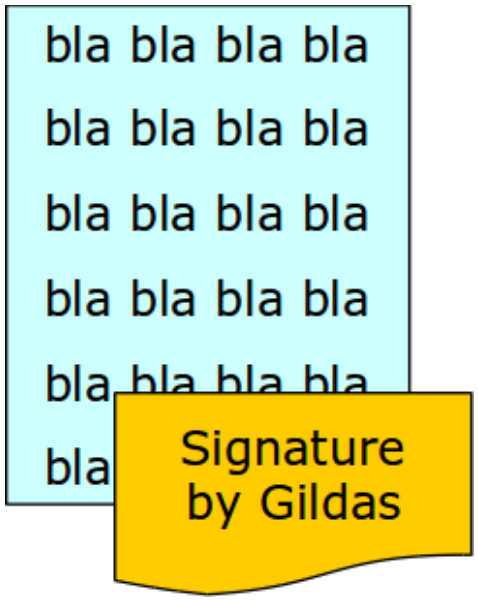
Basics

- The goal of a certificate is to link a public-key with its owner.
- The pair (public key, owner) is signed by a trusted party.
- The trusted party is named Certification Authority (CA).
- To check the signature, the CA public-key is needed:
  - Snake biting its tail!
- The pair (CA's public-key, CA) is self-signed: root certificate.

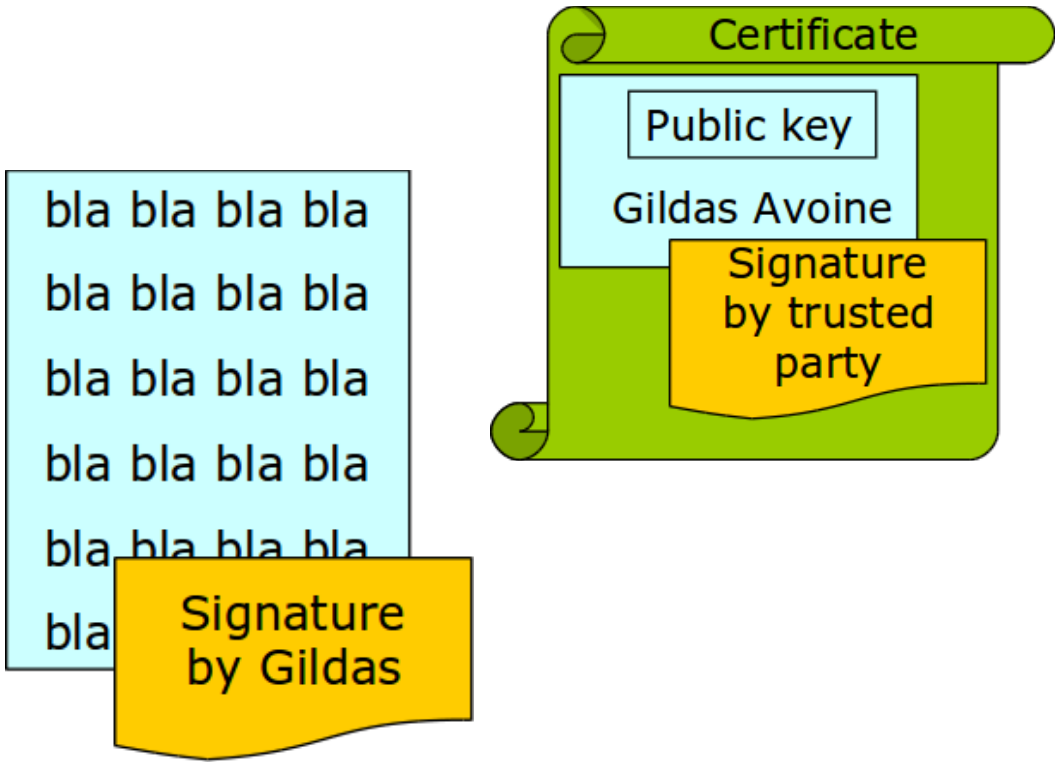
Basics

- The goal of a certificate is to link a public-key with its owner.
- The pair (public key, owner) is signed by a trusted party.
- The trusted party is named Certification Authority (CA).
- To check the signature, the CA public-key is needed:
  - Snake biting its tail!
- The pair (CA's public-key, CA) is self-signed: root certificate.
- The authenticity of the the root certificate is fundamental.

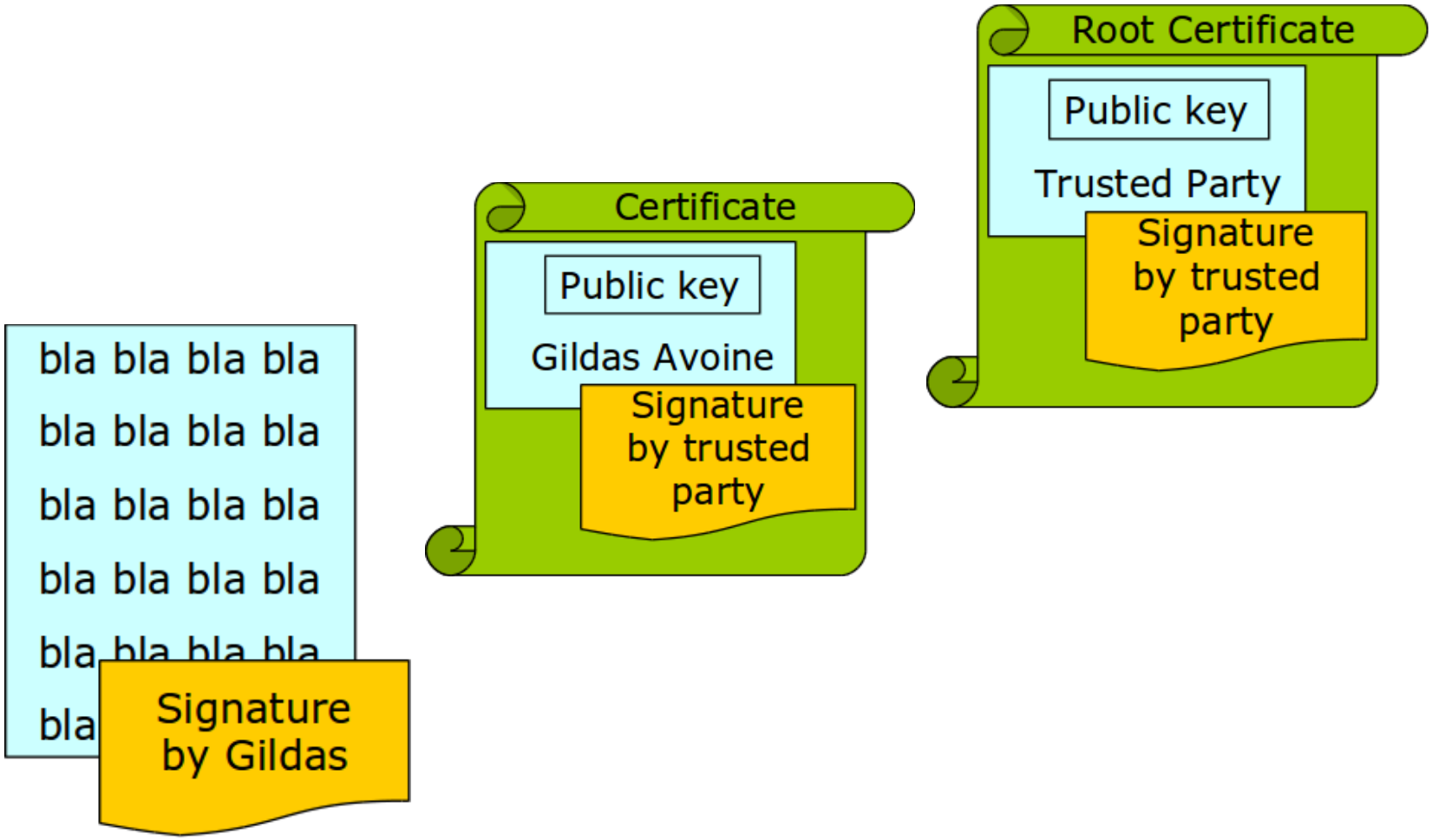
Basics Illustrated



Basics Illustrated



Basics Illustrated



Fundamental Information

- Public-key.
- Identity of the public-key owner.
- Signature of the certification authority.

CERTIFICATES X.509

- Fundamentals
- Certificates X.509
- Certificate Examples
- Obtaining a Certificate
- Verifying a Certificate
- Conclusion and Further Reading

X.509 Certificates

- X.509: Standard from International Telecommunication Union (ITU), released in 1988. Also IETF RFC-2459 (and updates).

X.509 Certificates

- X.509: Standard from International Telecommunication Union (ITU), released in 1988. Also IETF RFC-2459 (and updates).

- An X.509 certificate must contain three fields.
  - TBS Certificate (TBS = "To Be Signed")
    - → The useful payload of the certificate (see next slide).
  - CA signature algorithm.
    - → Identifier for the cryptographic algorithm used by the CA to sign this certificate.
  - CA signature value.
    - → Signature of the certificate by the CA.

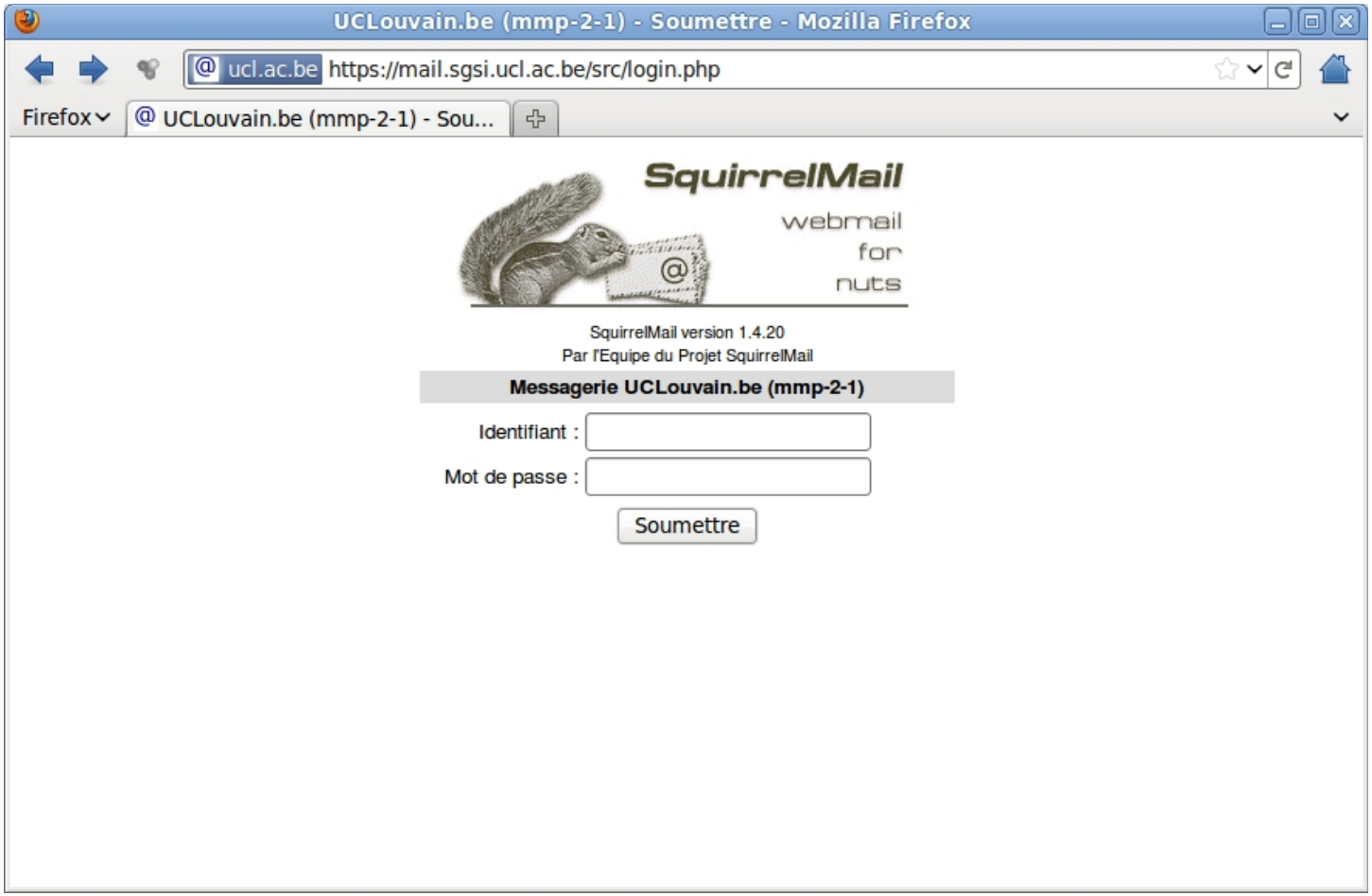
X.509: TBS Certificate

- Serial number.
  - Unique number assigned by the CA to the certificate.
- Issuer field
  - Identifies the entity who has signed and issued the certificate.
- Subject.
  - Identifies the entity associated with the public key (O:organization, C: country, OU: Organization Unit, CN: common name eg. DNS, ST: state, L: city, etc. no IP address).
- Validity.
  - Not before, not after.
- Subject Public Key Info.
  - Public key and identify the algorithm with which the key is used (e.g., RSA, DSA, or DH).
- Etc.

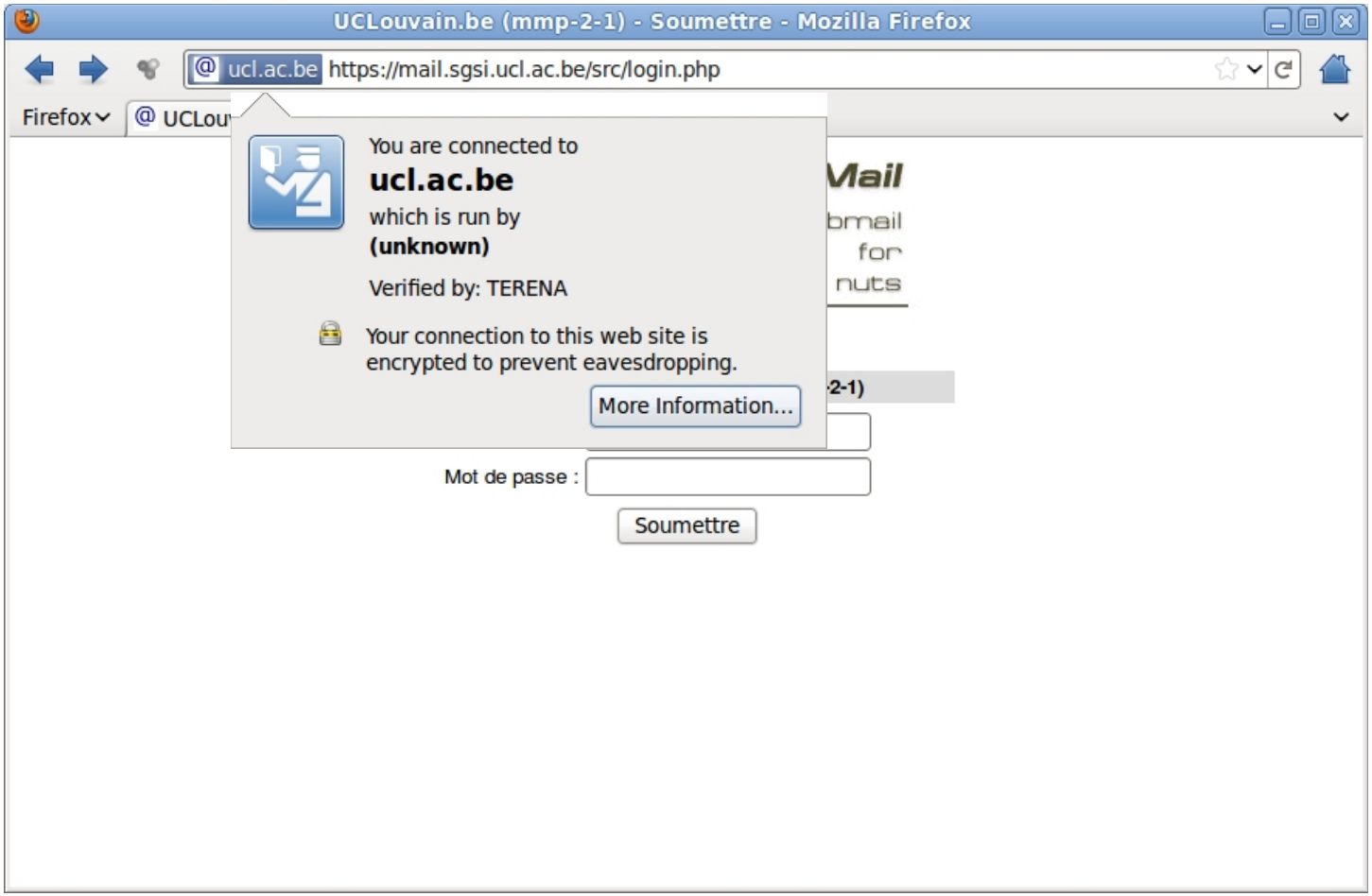
CERTIFICATE EXAMPLES

- Fundamentals
- Certificates X.509
- Certificate Examples
- Obtaining a Certificate
- Verifying a Certificate
- Conclusion and Further Reading

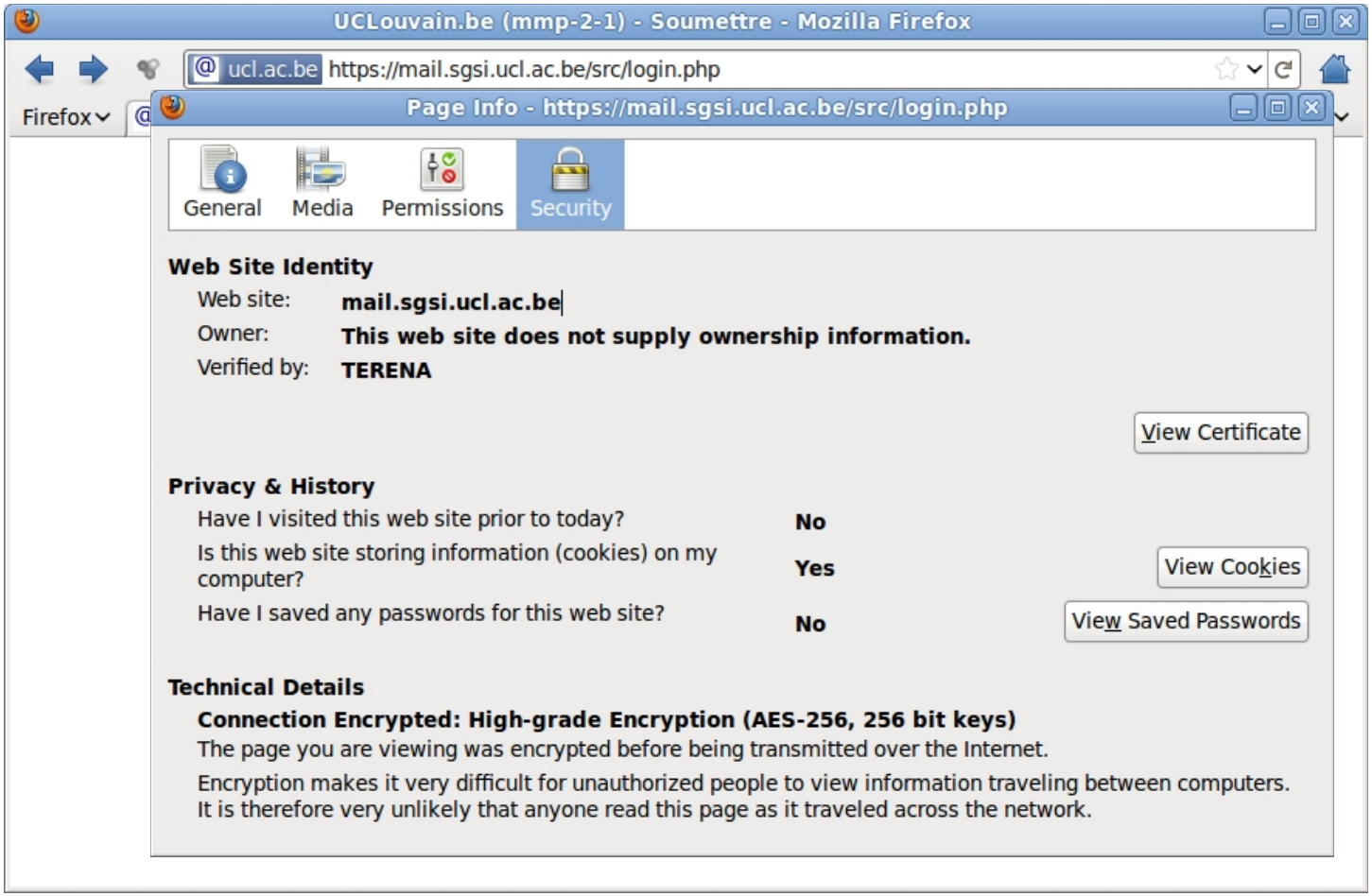
Example: UCL Webmail Certificate



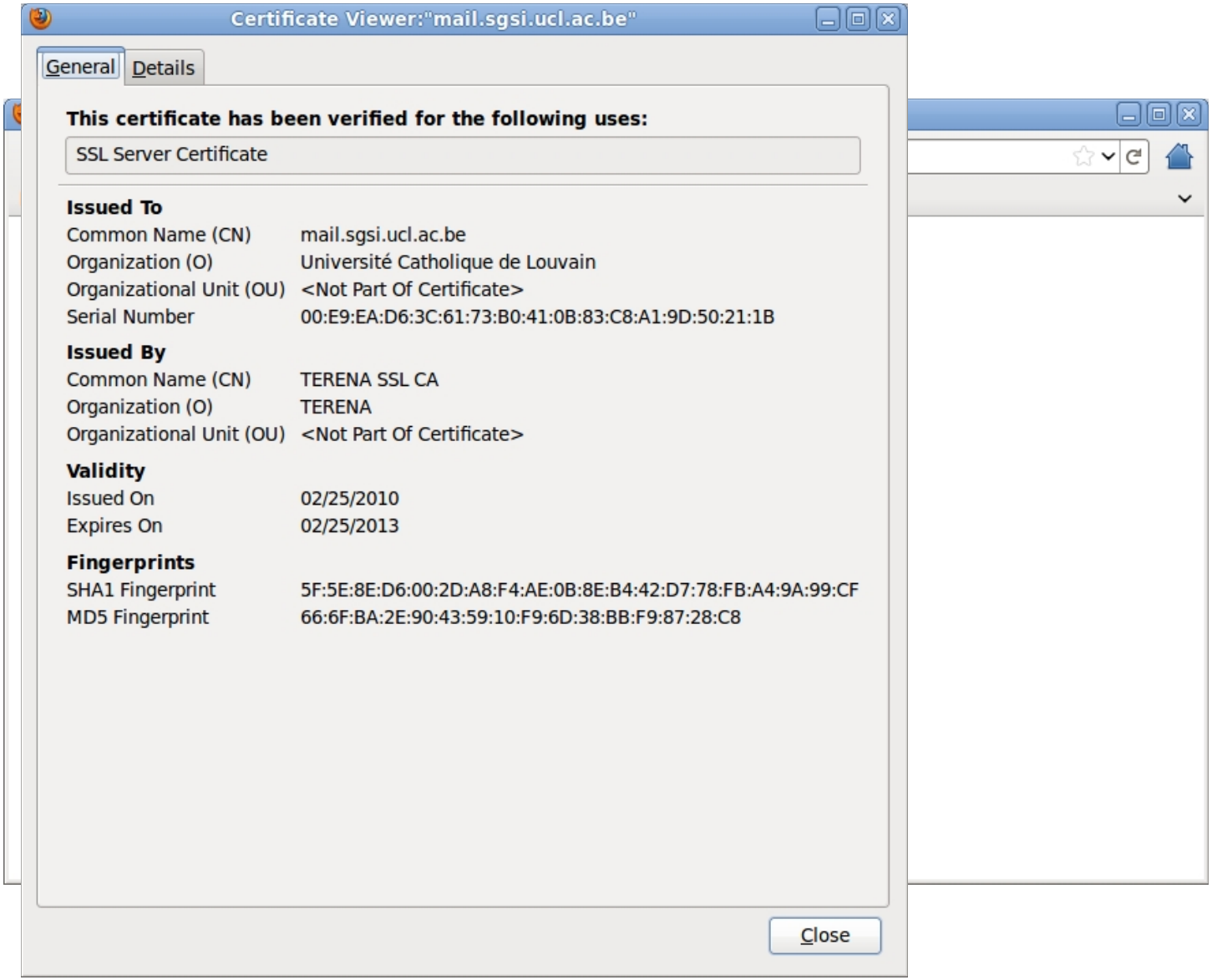
Example: UCL Webmail Certificate



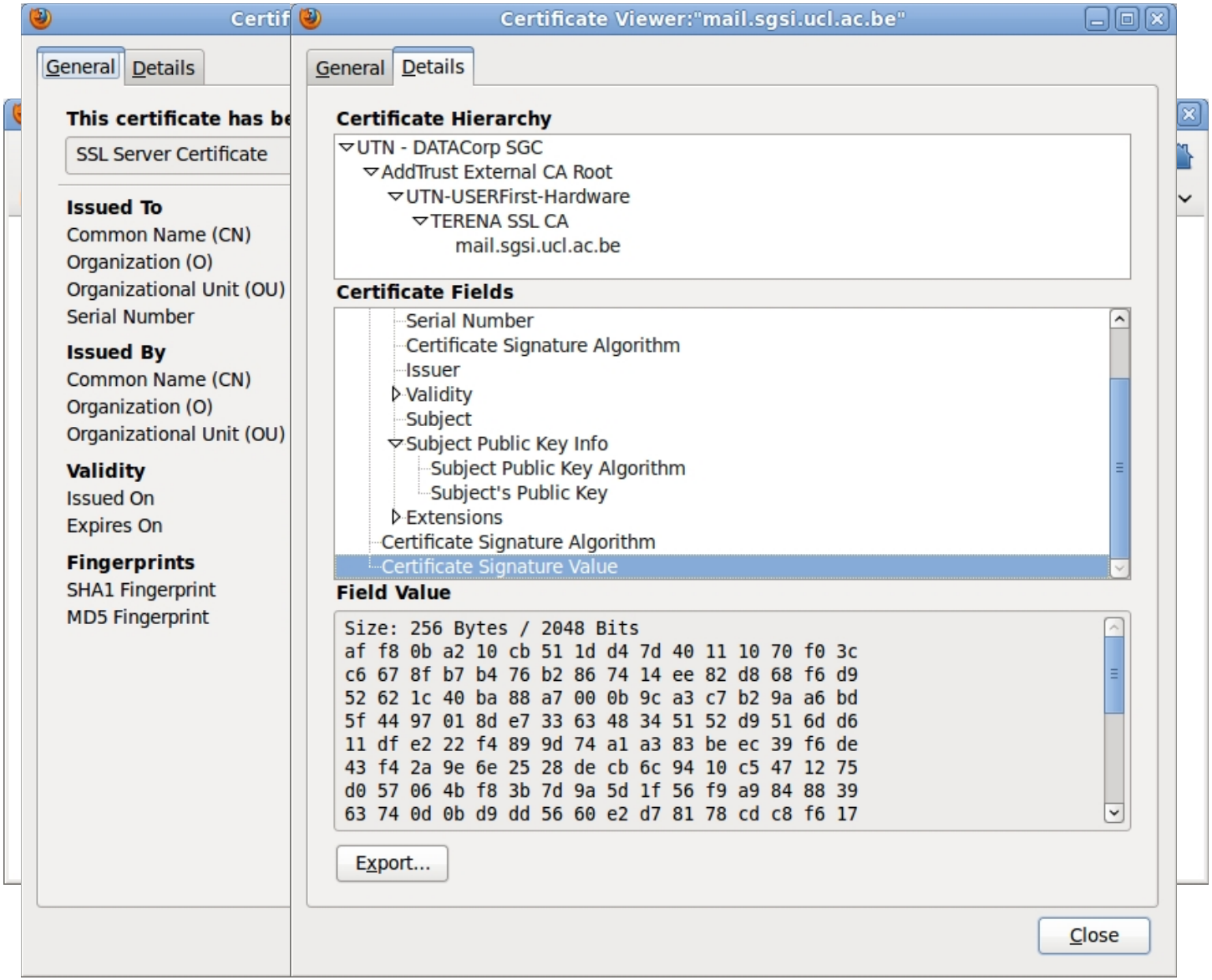
Example: UCL Webmail Certificate



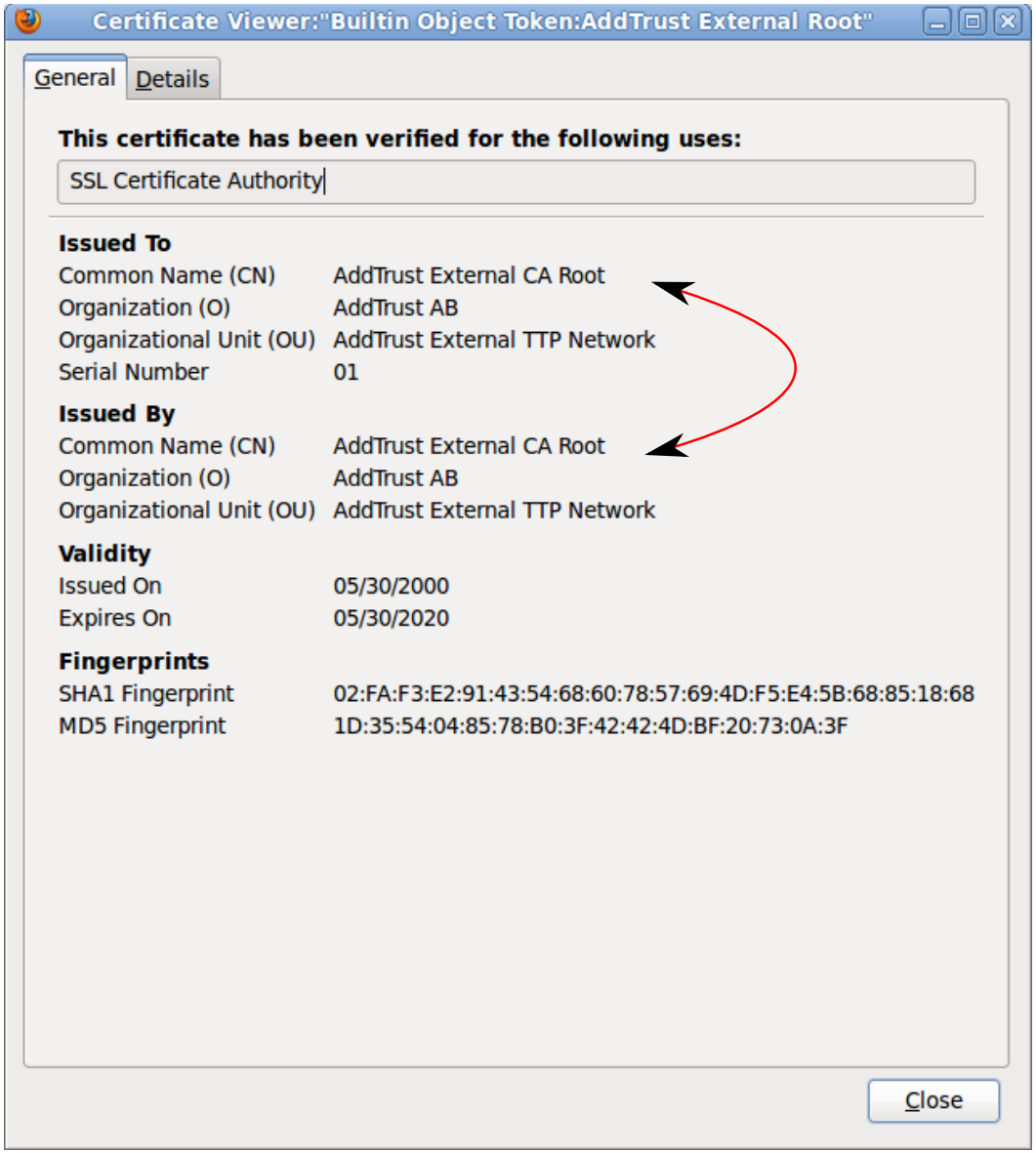
Example: UCL Webmail Certificate



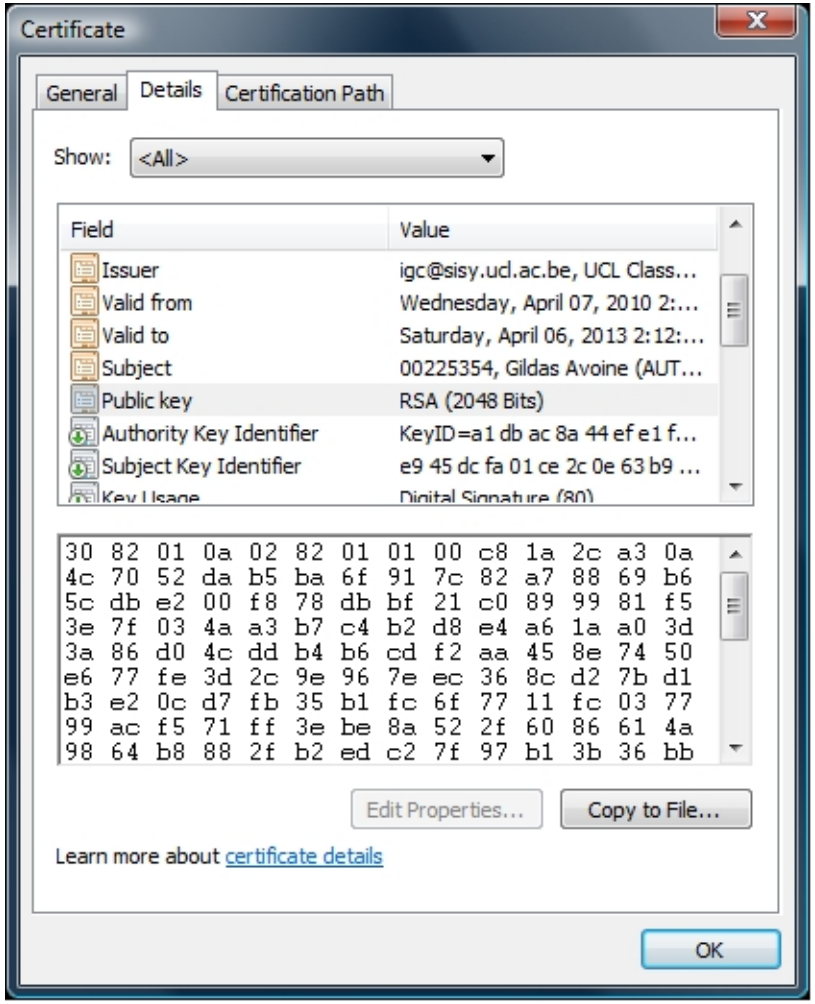
Example: UCL Webmail Certificate



Example: Root Certificate



Example: UCL Member Card



Example: Belgian ePassport
Page 1/2

```
Data:
    Version: 3 (0x2)
    Signature Algorithm: sha1WithRSAEncryption
    Issuer: C=BE, O=Kingdom of Belgium, OU=Federal Public Service Foreign Affairs Belgium, CN=CSCAPKI_BE
    Validity
        Not Before: Apr 10 00:00:00 2006 GMT
        Not After : Jul 15 23:59:59 2011 GMT
    Subject: C=BE, O=Kingdom of Belgium, OU=Federal Public Service Foreign Affairs Belgium, CN=DSPKI_BE
    Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
        RSA Public Key: (2048 bit)
            Modulus (2048 bit):
                00:8f:9c:2c:f8:05:b5:bd:ed:51:1a:9f:b0:57:6e:
                86:53:07:46:ac:ab:b6:05:e7:d6:e8:a6:6a:7b:ba:
                9b:27:aa:8a:9f:80:ec:87:b3:9d:68:b7:29:cb:b1:
                df:de:5e:48:9e:34:21:9f:97:ea:98:7a:f7:f6:88:
                1c:ca:a3:b1:3f:b2:d8:36:9a:06:0b:b3:f0:02:20:
                ce:ff:a9:e2:12:00:b2:1d:71:df:3e:cc:64:83:e2:
                f9:e8:30:15:a5:62:95:ab:8e:8c:ee:dc:73:9a:9f:
                58:78:c9:38:fd:ae:7c:71:17:73:c8:64:23:d2:34:
                99:58:ef:bc:ca:dc:e3:38:39:d4:30:16:c1:8e:52:
                a9:b0:eb:7f:5f:06:65:02:bc:72:1e:eb:14:40:af:
                39:20:25:48:cf:2f:8e:1b:4f:2e:d6:fb:49:b7:ab:
                a3:e5:56:2e:31:a1:30:56:69:dc:4f:b4:d8:49:a4:
                af:e6:0c:e8:65:df:58:d5:ee:7f:80:02:d5:35:63:
                2a:14:81:0a:eb:7d:5e:17:f8:63:9a:67:28:b0:b8:
                f4:39:0b:cb:91:63:4b:e3:14:e0:69:dd:dd:92:26:
                b2:8b:a4:0c:4d:de:10:b8:96:2b:e7:f1:ac:2e:2f:
                11:15:bd:13:1d:61:c4:bf:69:24:28:9f:67:dd:b6:
                49:b5
            Exponent: 65537 (0x10001)
```

Example: Belgian ePassport
Page 2/2

```
    X509v3 extensions:
        X509v3 Authority Key Identifier:
            keyid:00:84:19:14:B2:CE:7E:0A:DE:3A:26:F9:FD:DD:1F:F4:01:42:A8:0E

        X509v3 Key Usage: critical
            Digital Signature
Signature Algorithm: sha1WithRSAEncryption
      5d:ed:53:da:14:3d:e2:ab:2d:41:3c:ea:bc:55:3b:78:2a:2c:8e:0b:54:74:af:bd:a9:e1:c5:
      92:a4:f0:db:a9:0b:7d:0c:96:fb:1b:38:92:e2:48:3a:a2:49:a0:f6:9f:41:97:43:85:68:99:
      08:cd:fd:8a:2d:36:ec:86:92:53:46:dd:07:ee:30:64:37:6c:7a:c5:5e:3a:21:95:e3:bb:02:
      c4:fa:51:8d:12:e2:4c:ca:c1:07:0c:e7:52:89:6f:4a:8f:83:c5:a0:26:3e:3c:a2:38:1b:27:
      6b:32:10:ef:61:73:c8:03:97:39:75:8e:4b:81:3e:c8:c4:96:92:6a:f4:94:81:a5:83:38:a5:
      3d:cd:ff:1d:53:6b:36:6b:5d:82:fd:f5:fe:85:e0:e9:62:b8:77:0d:cf:05:1d:9b:75:f1:ec:
      05:9c:9e:e7:2f:10:76:af:6b:34:56:ff:d3:9a:2a:61:ec:8e:8e:02:bd:85:21:2c:ba:c4:1b:
      58:90:51:de:25:d7:48:db:67:0a:3e:46:e6:80:52:d6:ed:bc:ec:cb:48:b4:45:bf:cd:55:f3:
      25:f0:68:ff:c1:3b:8a:28:9e:95:9b:c9:da:2a:80:4d:1a:14:9a:f9:4f:37:d1:cc:c3:a8:c4:
      e7:5c:de:87:60:ac:11:b5:04:73:f0:3d:95:b5:26:31:bd:65:f8:87:8c:92:93:9b:36:73:ad:
      36:77:f3:d3:f7:e8:82:ce:6a:ee:4b:a2:a4:38:8f:95:a5:dc:49:6a:ba:7b:aa:7a:b8:42:63:
      ba:30:3f:2c:fa:07:87:85:29:81:88:19:2e:07:34:fb:f1:5d:e0:ea:c4:f0:15:6d:1c:93:33:
      21:72:4f:a3:10:30:26:e6:62:7d:ef:36:8e:34:60:c8:b6:76:b5:f6:22:7c:93:61:15:ea:fa:
      55:b1:8a:fc:ae:e9:14:df:8f:19:a2:1d:5b:fe:b3:b3:23:bb:20:0e:81:0a:74:f6:a9:f2:2b:
      cd:77:9b:c1:20:78:38:1f:4b:75:62:bc:41:44:83:a6:5b:c2:59:31:04:bc:49:91:c1:b2:48:
      93:61:e6:f5:58:1d:c9:28:48:d5:82:de:2f:77:ce:db:7b:a9:9d:10:c9:f8:28:7b:79:85:a7:
      79:95:12:00:81:85:b7:44:69:7d:35:bf:5d:84:bd:ea:cf:c0:f6:26:5d:bd:25:43:fa:68:89:
      8d:12:e6:8c:ab:97:00:a0:85:1f:df:7a:3d:91:e0:ed:87:79:bb:8f:cd:58:6f:e9:0b:7e:81:
      78:a7:10:36:60:d9:de:c3:90:56:fc:b7:6d:d3:82:3d:56:36:92:7e:ac:28:4c:43:43:c4
```

OBTAINING A CERTIFICATE

- Fundamentals
- Certificates X.509
- Certificate Examples
- Obtaining a Certificate
- Verifying a Certificate
- Conclusion and Further Reading

Certificate Authorities

- Issuers of certificates found on web servers.
- GeoTrust, Verisign, and Thawte: same group.

CA	Count %
GoDaddy.com	20.12
GeoTrust	10.68
Verisign	9.62
Equifax	6.41
Thawte	5.26
DigiCert	4.09
Comodo Limited	4.05

Source (Jan. 2012): https://secure1.securityspace.com/es/s_survey/data/man.201002/casurvey.html

How to Obtain a Certificate

- The applicant must present himself to the CA.
- The CA (physically) authenticates the applicant.
- The CA asks the participant to generate public/private keys.
- The CA creates a certificate with the applicant's identity, public key, expiration date, etc. and the CA's signature.
- The CA provides a copy of its own public key to the applicant.
- The applicant can spread his certificate to who shares a common "trusted ancestor".

Registration Authority

- The CA can delegate the registration of an applicant to the registration authority (RA).
- The RA does not have CA's private key.
- The CA trusts the RA to authenticate the applicants.
- After having authenticated the applicant, the RA lets the applicant generate a pair of keys and sends the public key to the CA to create the certificate.
- Technically the RA sends a signed Certificate Signing Request (CSR) to the CA.

Certificate without CA

- Everyone can generate himself a certificate.
- Distribute the certificate through an authenticated channel.
- Examples:
  - Internal HTTPS server in a company.
  - PGP certificates.

CSR in Practice with OpenSSL

- Generate a 1024-RSA key-pair.

  openssl genrsa 1024 > mykey.key

- Generate a CSR.

  openssl req -config my.cnf -new -key mykey.key -out myreq.csr

- Verify a CSR.

  openssl req [-text] [-noout] -verify -in myreq.csr

- Online checkers.
  - http://support.ecenica.com/ssl-certificates/csr-checker/
  - https://ssl-tools.verisign.com/checker/

Certificates in Practice with OpenSSL

- Generate a certificate.

  openssl x509 -req -in myreq.csr -signkey mykey.key -out mycert.crt

- View a certificate.

  openssl x509 -text -in mycert.crt

- Verify a certificate.

  openssl verify mycert.crt

VERIFYING A CERTIFICATE

- Fundamentals
- Certificates X.509
- Certificate Examples
- Obtaining a Certificate
- Verifying a Certificate
- Conclusion and Further Reading

Verifying a Certificate

- Verify the certification path.
  - Performed locally.
  - Delegated to a server: SCVP.
    - → Server-based Certificate Validation Protocol.
- Verify the validity period.
- Verify that the certificate is not revoked.
  - Performed locally: CRL (certificate revocation lists).
  - Delegated to a server: OCSP.
    - → Online Certificate Status Protocol.

OCSP in Firefox 4.0

CONCLUSION AND FURTHER READING

- Fundamentals
- Certificates X.509
- Certificate Examples
- Obtaining a Certificate
- Verifying a Certificate
- Conclusion and Further Reading

Key Concepts

- A certificate aims to link a public-key with an identity.
- A trusted authority (CA) signs certify this link with a signature.
- A user should generate himself his private key and he should not provide it to the authority.

Key Escrowing

- A company can provide two key-pairs and certificates to each of its employees.
  - One to be used for signature.
  - The other to be used for encryption.
- CA puts aside (escrows) a copy of the private encryption key.
- In case of problems, the company can always decrypt its employees' mails and files.
- The employees remain the only ones to be able to sign with their signing key.

Further Reading

- ITU Recommendation X.509: `http://www.itu.int/rec/T-REC-X.509`
- OpenPGP certificates: `http://gnutls.org/manual/html_node/OpenPGP-certificates.html`