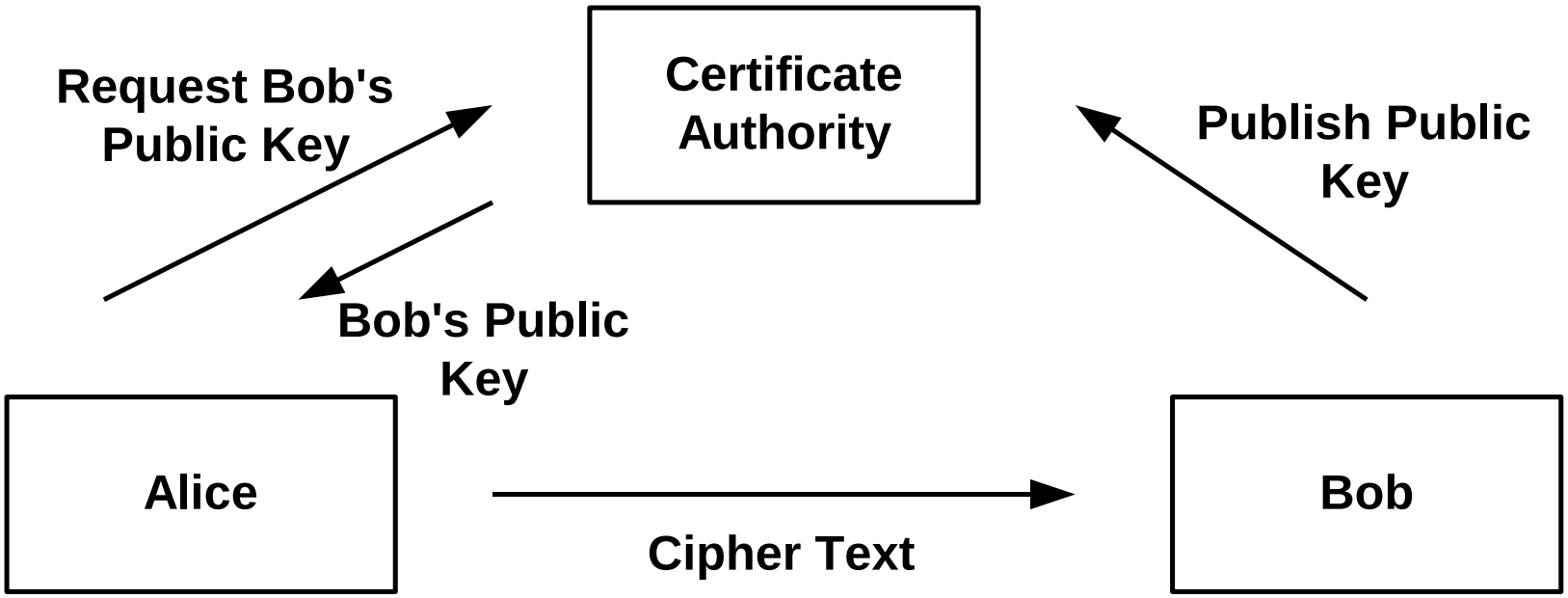
Digital certificate

-Digital certificate is a statement signed by a trusted person or party.

-An attachment to an electronic message used for security purposes. The most common use of a digital certificate is to verify that a user sending a message is who he or she claims to be, and to provide the receiver with the means to encode a reply.

-An individual wishing to send an encrypted message applies for a digital certificate from a *Certificate Authority (CA)*. The CA issues an encrypted digital certificate containing the applicant's public key and a variety of other identification information. The CA makes its own public key readily available through print publicity or on the Internet.

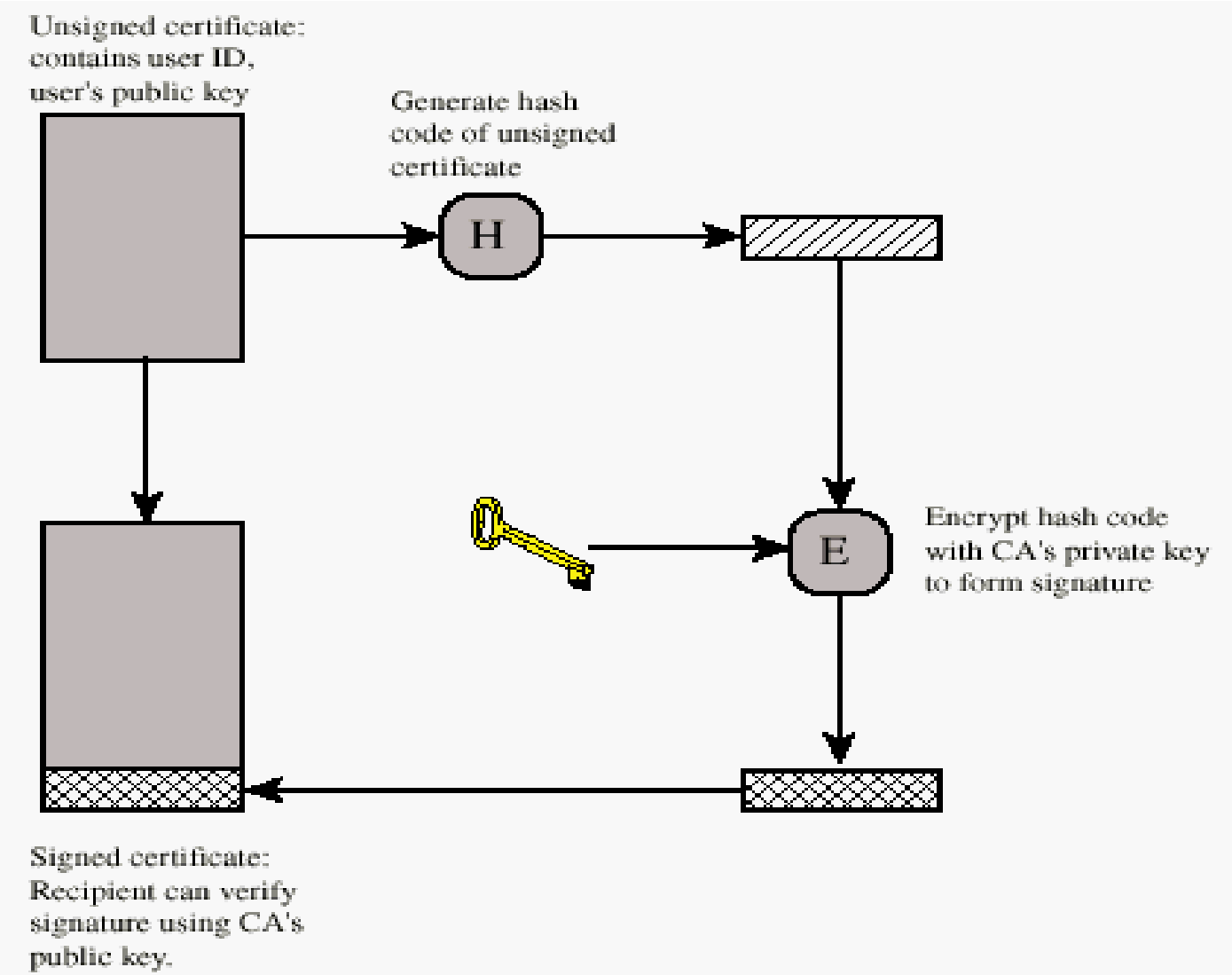
Certificate Authority



certification authority

- Abbreviated as *CA*, a trusted third-party organization or company that issues digital certificates used to create digital signatures and public-private key pairs. The role of the CA in this process is to guarantee that the individual granted the unique certificate is, in fact, who he or she claims to be.

Key Management
Public-Key Certificate Use



X.509

- A widely used standard for defining digital certificates. X.509 (Version 1) was first issued in 1988.
- When X.509 was revised in 1993, two more fields were added resulting in the Version 2 format. These two additional fields support directory access control.
- X.509 Version 3 defines the format for certificate extensions used to store additional information regarding the certificate holder and to define certificate usage. Collectively, the term X.509 refers to the latest published version.

Contents of a typical digital certificate

- **Serial Number**: Used to uniquely identify the certificate.
- **Subject**: The person, or entity identified.
- **Signature Algorithm**: The algorithm used to create the signature.
- **Issuer**: The entity that verified the information and issued the certificate.
- **Valid-From**: The date the certificate is first valid from.
- **Valid-To**: The expiration date.
- **Key-Usage**: Purpose of the public key (e.g. encipherment, signature, certificate signing...).
- **Public Key**: The public key to encrypt a message to the named subject or to verify a signature from the named subject.
- **Thumbprint Algorithm**: The algorithm used to hash the certificate.
- **Thumbprint**: The hash itself to ensure that the certificate has not been tampered with.

Certificates and web site security

- The most common use of certificates is for HTTPS-based web sites. A web browser validates that an SSL (Transport Layer Security) web server is authentic, so that the user can feel secure that their interaction with the web site has no eavesdroppers and that the web site is who it claims to be.

- **Structure of a certificate**
- The structure of an X.509 v3 digital certificate is as follows:
- Certificate
  - Version
  - Serial Number
  - Algorithm ID
  - Issuer
  - Validity
    - Not Before
    - Not After
  - Subject
  - Subject Public Key Info
    - Public Key Algorithm
    - Subject Public Key
  - Issuer Unique Identifier (Optional)
  - Subject Unique Identifier (Optional)
  - Extensions (Optional)
    - ...
- Certificate Signature Algorithm
- Certificate Signature

Sample X.509 certificates

- This is an example of a decoded X.509 certificate for www.freesoft.org,
- the actual certificate is about 1KB in size. It was issued by Thawte, as stated in the Issuer field.
- Its subject contains many personal details, but the most important part is usually the common name (CN), as this is the part that must match the host being authenticated.

- Certificate: Data: Version: 1 (0x0) Serial Number: 7829 (0x1e95) Signature Algorithm: md5WithRSAEncryption Issuer: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc, OU=Certification Services Division**, CN=**Thawte Server CA/emailAddress=server-certs@thawte.com Validity Not Before: Jul 9 16:04:02 1998 GMT Not After : Jul 9 16:04:02 1999 GMT Subject: C=US, ST=Maryland, L=Pasadena, O=Brent Baccala, OU=FreeSoft, CN=www.freesoft.org/emailAddress=baccala@freesoft.org Subject Public Key Info: Public Key Algorithm: rsaEncryption RSA Public Key: (1024 bit) Modulus (1024 bit):
  00:b4:31:98:0a:c4:bc:62:c1:88:aa:dc:b0:c8:bb:
  33:35:19:d5:0c:64:b9:3d:41:b2:96:fc:f3:31:e1:
  66:36:d0:8e:56:12:44:ba:75:eb:e8:1c:9c:5b:66:
  70:33:52:14:c9:ec:4f:91:51:70:39:de:53:85:17:
  16:94:6e:ee:f4:d5:6f:d5:ca:b3:47:5e:1b:0c:7b:
  c5:cc:2b:6b:c1:90:c3:16:31:0d:bf:7a:c7:47:77:
  8f:a0:21:c7:4c:d0:16:65:00:c1:0f:d7:b8:80:e3:
  d2:75:6b:c1:ea:9e:5c:5c:ea:7d:c1:a1:10:bc:b8: e8:35:1c:9e:27:52:7e:41:8f
  Exponent: 65537 (0x10001) Signature Algorithm: md5WithRSAEncryption
  93:5f:8f:5f:c5:af:bf:0a:ab:a5:6d:fb:24:5f:b6:59:5d:9d:
  92:2e:4a:1b:8b:ac:7d:99:17:5d:cd:19:f6:ad:ef:63:2f:92:
  ab:2f:4b:cf:0a:13:90:ee:2c:0e:43:03:be:f6:ea:8e:9c:67:
  d0:a2:40:03:f7:ef:6a:15:09:79:a9:46:ed:b7:16:1b:41:72:
  0d:19:aa:ad:dd:9a:df:ab:97:50:65:f5:5e:85:a6:ef:19:d1:
  5a:de:9d:ea:63:cd:cb:cc:6d:5d:01:85:b5:6d:c8:f3:d9:f7:
  8f:0e:fc:ba:1f:34:e9:96:6e:6c:cf:f2:ef:9b:bf:de:b5:22: 68:9f

- Certificate: Data: Version: 3 (0x2) Serial Number: 1 (0x1) Signature Algorithm: md5WithRSAEncryption Issuer: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc, OU=Certification Services Division, CN=Thawte Server CA/emailAddress=server-certs@thawte.com Validity Not Before: Aug 1 00:00:00 1996 GMT Not After : Dec 31 23:59:59 2020 GMT Subject: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc, OU=Certification Services Division, CN=Thawte Server CA/emailAddress=server-certs@thawte.com **Subject Public Key Info**: Public Key Algorithm: rsaEncryption RSA Public Key: (1024 bit) Modulus (1024 bit): 00:d3:a4:50:6e:c8:ff:56:6b:e6:cf:5d:b6:ea:0c: 68:75:47:a2:aa:c2:da:84:25:fc:a8:f4:47:51:da: 85:b5:20:74:94:86:1e:0f:75:c9:e9:08:61:f5:06: 6d:30:6e:15:19:02:e9:52:c0:62:db:4d:99:9e:e2: 6a:0c:44:38:cd:fe:be:e3:64:09:70:c5:fe:b1:6b: 29:b6:2f:49:c8:3b:d4:27:04:25:10:97:2f:e7:90: 6d:c0:28:42:99:d7:4c:43:de:c3:f5:21:6d:54:9f: 5d:c3:58:e1:c0:e4:d9:5b:b0:b8:dc:b4:7b:df:36: 3a:c2:b5:66:22:12:d6:87:0d Exponent: 65537 (0x10001) X509v3 extensions: X509v3 Basic Constraints: critical **CA:TRUE** Signature Algorithm: md5WithRSAEncryption 07:fa:4c:69:5c:fb:95:cc:46:ee:85:83:4d:21:30:8e:ca:d9: a8:6f:49:1a:e6:da:51:e3:60:70:6c:84:61:11:a1:1a:c8:48: 3e:59:43:7d:4f:95:3d:a1:8b:b7:0b:62:98:7a:75:8a:dd:88: 4e:4e:9e:40:db:a8:cc:32:74:b9:6f:0d:c6:e3:b3:44:0b:d9: 8a:6f:9a:29:9b:99:18:28:3b:d1:e3:40:28:9a:5a:3c:d5:b5: e7:20:1b:8b:ca:a4:ab:8d:e9:51:d9:e2:4c:2c:59:a9:da:b9: b2:75:1b:f6:42:f2:ef:c7:f2:18:f9:89:bc:a3:ff:8a:23:2e: 70:47

- This is an example of a self-signed certificate, as the issuer and subject are the same. There's no way to verify this certificate except by checking it against itself; instead, these top-level certificates are stored by web browsers.
- Thawte is one of the root certificate authorities recognized by both Microsoft and Netscape. This certificate comes with the web browser and is trusted by default.

X.509 Certificate Revocation List (CRL)

- Is to prevent fraud and misuse.
- A certificate may be revoked for one the following reason:
  - The user's private key is compromised
  - The user is no longer certified by this CA
  - Expiration of the certificate
  - The CA's private key a compromised
- Version 1 was published in 1988.
- Version 2 was published in 1997.

X.509 Certificate Revocation List (CRL)

- Is to prevent fraud and misuse.
- A certificate may be revoked for one the following reason:
  - The user's private is compromised
  - The user is no longer certified by this CA
  - The CA's private key a compromised
- Version 1 was published in 1988.
- Version 2 was published in 1997.

X.509 CRL (cont..)

- X09 CRL consists of the following fields:
  - Version
  - Serial Number
  - Revocation Date
  - Algorithm Identifier
  - Issuer name
  - Last update
  - Next update
  - Extensions (Version 2 only)
  - Signature