

Security

Digital certificates

(Public) Key Management

- **Q.** When you receive a public key, how can you be sure that it is authentic?
- **A.** If the received public key is **digitally signed** by someone whose own public key you have and are sure is correct **and** you trust them to sign keys responsibly.

Digital Certificate

- Electronic document that binds an entity to a public key
- Using standard file format, usually X.509
- Signed by a third party called a **Certificate Authority (CA)**
- Certificate user (e.g. web browser) trusts CA to issue valid certificates.
- CA's public key may be authenticated by another (e.g. higher-level) CA



Digital Certificate – components

- Most important components of a digital certificate:
 - Subject (owner)
 - The name on the certificate – i.e. to whom it was issued
 - Subject's public key
 - The purpose of a certificate is to validate the public key of the subject
 - Issuer (Certificate Authority)
 - The identity of entity that signed the certificate
 - Issuer's digital signature
 - Serial number
 - Unique identifier for checking against revocation lists
 - Validity period
 - Start date; expiry date

Digital Certificate – example

The screenshot shows a digital certificate chain of trust. At the top, a browser window displays the URL <https://www.amazon.co.uk>. Below the URL, a certificate chain tree is shown with three levels:

- Root: DigiCert Global Root G2
- Intermediate: DigiCert Global CA G2
- Leaf: www.amazon.co.uk

The leaf node is highlighted with a red box. To the right, the text "Chain of trust" is displayed.

Below the certificate tree, the "Details" section is expanded, showing the following subject information:

Subject Name	
Country	US
State/Province	Washington
Locality	Seattle
Organization	Amazon.com, Inc.
Common Name	www.amazon.co.uk

This subject information is highlighted with a red box. To the right, the text "Subject (public key owner)" is displayed.

Further down, the issuer information is shown:

Issuer Name	
Country	US
Organization	DigiCert Inc
Common Name	DigiCert Global CA G2

This issuer information is highlighted with a red box. To the right, the text "Issuer (certificate authority)" is displayed.

Other details listed include:

- Serial Number: 0C 78 07 75 C7 85 6F 80 E8 D8 87 46 5E 60 E9 4B
- Version: 3
- Signature Algorithm: SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)
- Parameters: None
- Not Valid Before: Friday 4 May 2018 at 01:00:00 Irish Standard Time
- Not Valid After: Sunday 5 May 2019 at 13:00:00 Irish Standard Time

Each of these details is highlighted with a red box. To the right, the corresponding text labels are displayed: "Unique serial no.", "Signature algorithm", and "Validity period".

Chain of trust

Subject Name
Country US
State/Province Washington
Locality Seattle
Organization Amazon.com, Inc.
Common Name www.amazon.co.uk

Subject (public key owner)

Issuer Name
Country US
Organization DigiCert Inc
Common Name DigiCert Global CA G2

Issuer (certificate authority)

Serial Number 0C 78 07 75 C7 85 6F 80 E8 D8 87 46 5E 60 E9 4B

Unique serial no.

Version 3

Signature algorithm

Signature Algorithm SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)

Parameters None

Not Valid Before Friday 4 May 2018 at 01:00:00 Irish Standard Time

Validity period

Not Valid After Sunday 5 May 2019 at 13:00:00 Irish Standard Time

Digital Certificate – example (cont.)

Cert Global Root G2
DigiCert Global CA G2
 www.amazon.co.uk
Not Valid After Thursday 12 December 2019 at 12:00:00 Greenwich Mean Time
Public Key Info
Algorithm RSA Encryption (1.2.840.113549.1.1.1)
Parameters None
Public Key 256 bytes : CA E2 F2 03 C8 F8 60 94 46 8F 99 3C 95 93 C6 7F 68 79 C3 E2 48 D8 3C 75 AF F5 FA F9 0E 5B 62 E5 55 8B A7 D2 80 53 09 BA 41 47 7B 71 45 34 99 BE 13 21 3D EA 10 9E 87 14 CA BC F7 37 44 16 BC E1 2A CB CB 30 42 B4 B2 BC A8 13 CC C6 BC BA 22 AE 30 15 E3 B0 6B 1A 24 33 C7 B4 9C 20 46 6A 0E 82 F0 23 1E 09 38 29 20 A5 3B 91 37 24 D1 89 38 66 6B 7F 40 29 A6 C4 80 0C 4A E4 28 CB CE AE B3 6C 15 9D 9B 39 B0 3D 6C F7 BD 60 DE 30 06 ED BC 1E E8 2C 48 72 46 9F 8B 58 30 16 5E B9 03 C9 CB 34 94 0C 06 6C 91 D0 43 51 FB 31 9C 6E C7 B5 99 97 2C D8 9D CC F5 4F 06 C9 8B 79 11 00 56 95 BD 49 08 83 5B 9C 0D 3C 6D 6E F3 4B C0 E3 04 DB C1 C0 7F AD 50 F8 83 E1 85 DA 95 B7 A7 58 AA B9 19 2B 9F 6C 9F 59 D0 70 B5 DE 9A E5 F7 18 6C 3E 01 DA EA 2A 27 A4 34 53 E6 9F 07 A9 5A 25 9D 51 17 F7
Exponent 65537
Key Size 2,048 bits
Key Usage Encrypt, Verify, Wrap, Derive
Signature 256 bytes : 5A 65 E7 8A D2 7E E8 5B BD 6C A9 FA 20 D6 0C 87 EA 4B 26 5E 92 54 90 23 A5 53 5A 15 DB B0 FE A4 7E 69 5E 2E 9C 0B D4 1F A8 DD 89 E0 64 A9 EF 8D D6 7E 64 BD D1 9B 6F 67 CC D3 16 CA 6A 44 F9 9F D9 57 3E FB 68 09 1C 86 35 4D 08 C1 5E 9B AF 5A 15 51 98 C5 92 C4 B1 36 FC 2F B7 B8 90 9C 8C C8 2E 05 7B B3 10 D9 67 69 77 09 30 C2 60 D4 18 F5 A0 06 17 DE F4 35 36 8D 35 9C AF C3 3D AA 4B A8 AB BE 93 B3 B5 5D EB 19 14 84 72 E6 98 B2 63 15 34 EA 2F EC 34 65 5B 61 CE 01 F6 F0 40 47 A1 55 46 39 38 9E 6B DE 95 95 44 E4 50 2D 3E 18 4F 5E 27 87 4C 1E DC 09 AD D7 B1 95 38 67 62 22 97 B1 B6 56 52 35 4D B3 67 0B 55 61 AD 4D 66 9E 06 8D B7 E7 B8 6F B9 9F 69 3B 5C 0E 66 9F 55 77 E0 F6 F5 27 CE 7A 74 23 FF AD 7D A1 C4 99 4F 21 F6 2C 57 ED 23 37 70 E4 65 9A 1A 4D B3 D5 A9 3E C4 BD
Extension Key Usage (2.5.29.15)

Public key algorithm (RSA)

Public key
(RSA modulus)

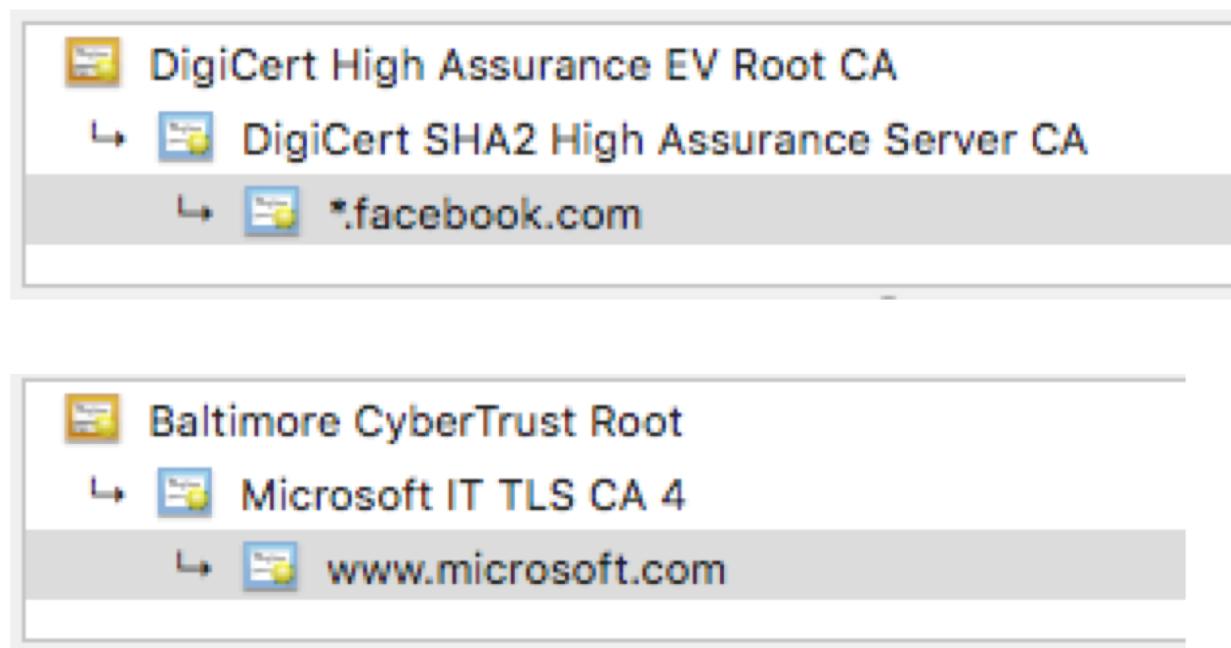
Exponent
(part of RSA public key)

Key size (2048 bits)

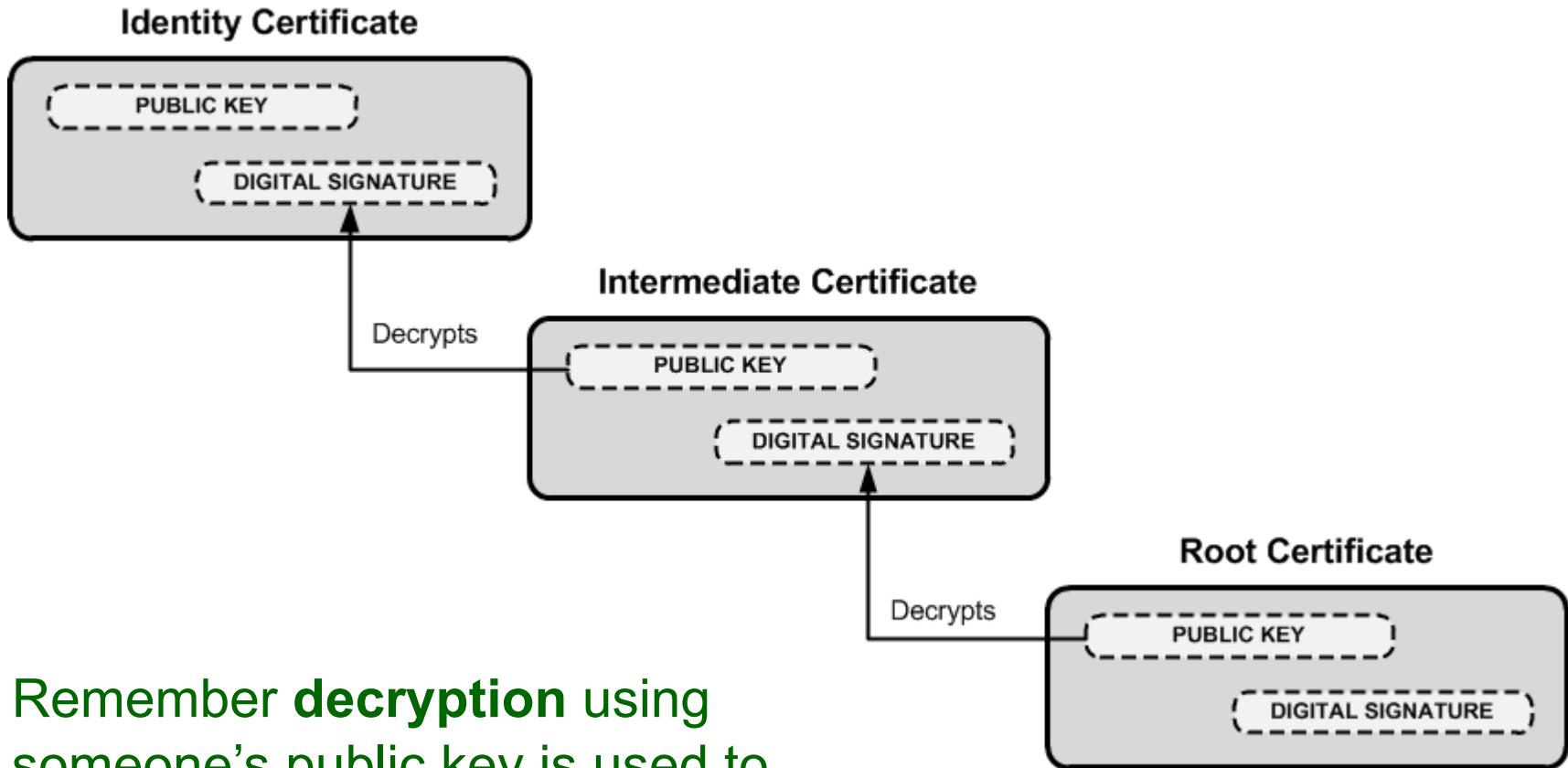
Signature
(signed hash)

Chain of trust

- Can build up a chain of trusts with linked digital certificates
- This is the basis of what are known as Public Key Infrastructures (PKIs)



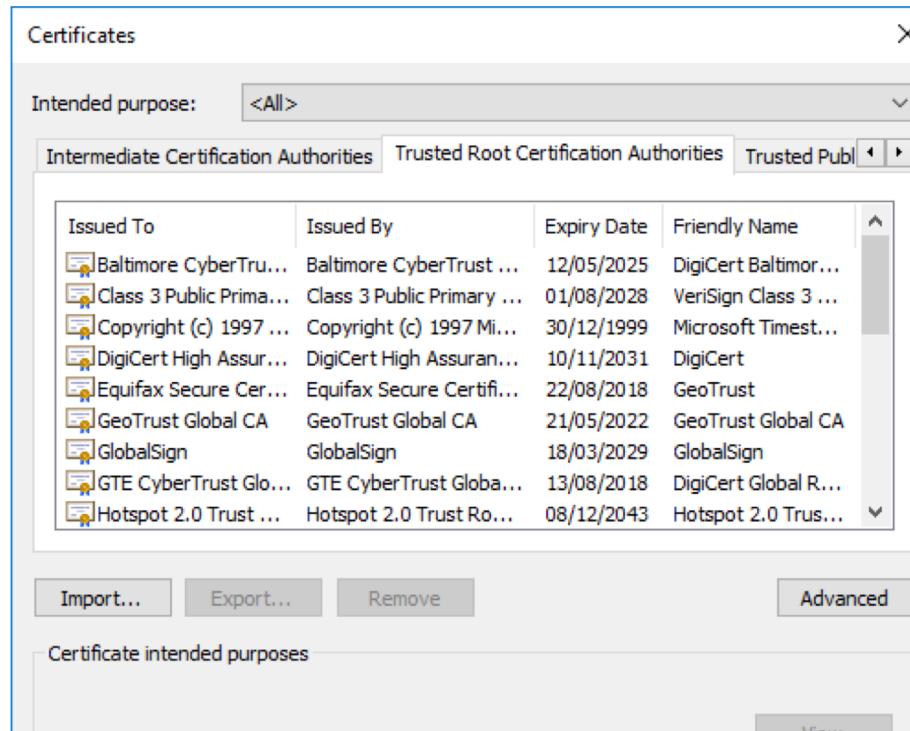
Verification using chain of trusts



Remember **decryption** using someone's public key is used to **verify** their signature

Chain of trust

- The buck must stop somewhere. Ultimately, at the end of the chain, you must trust a public key that is not signed (usually belonging to some recognised “authority”).
 - In your browser, this is one of the trusted root certificate authorities



Certificate Expiry & Revocation

- A Digital Certificate doesn't last for ever
- It normally **expires** after a certain time and must be renewed
- It may be **revoked**:
 - If the subject's private key is compromised
 - If there is a change in status of the subject
 - If the CA's private key is compromised
- Revoked certificates are placed on a Certificate Revocation List (CRL)

Certificate Revocation

- An issue is where to find CRL to check if cert has been revoked
 - One solution is to provide as part of certificate URL pointing to CRL
 - Another solution is OCSP (online certificate status protocol) which allows real time queries.
 - Another is to just rely on local list which is refreshed by browser updates (Chrome does this)

