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.

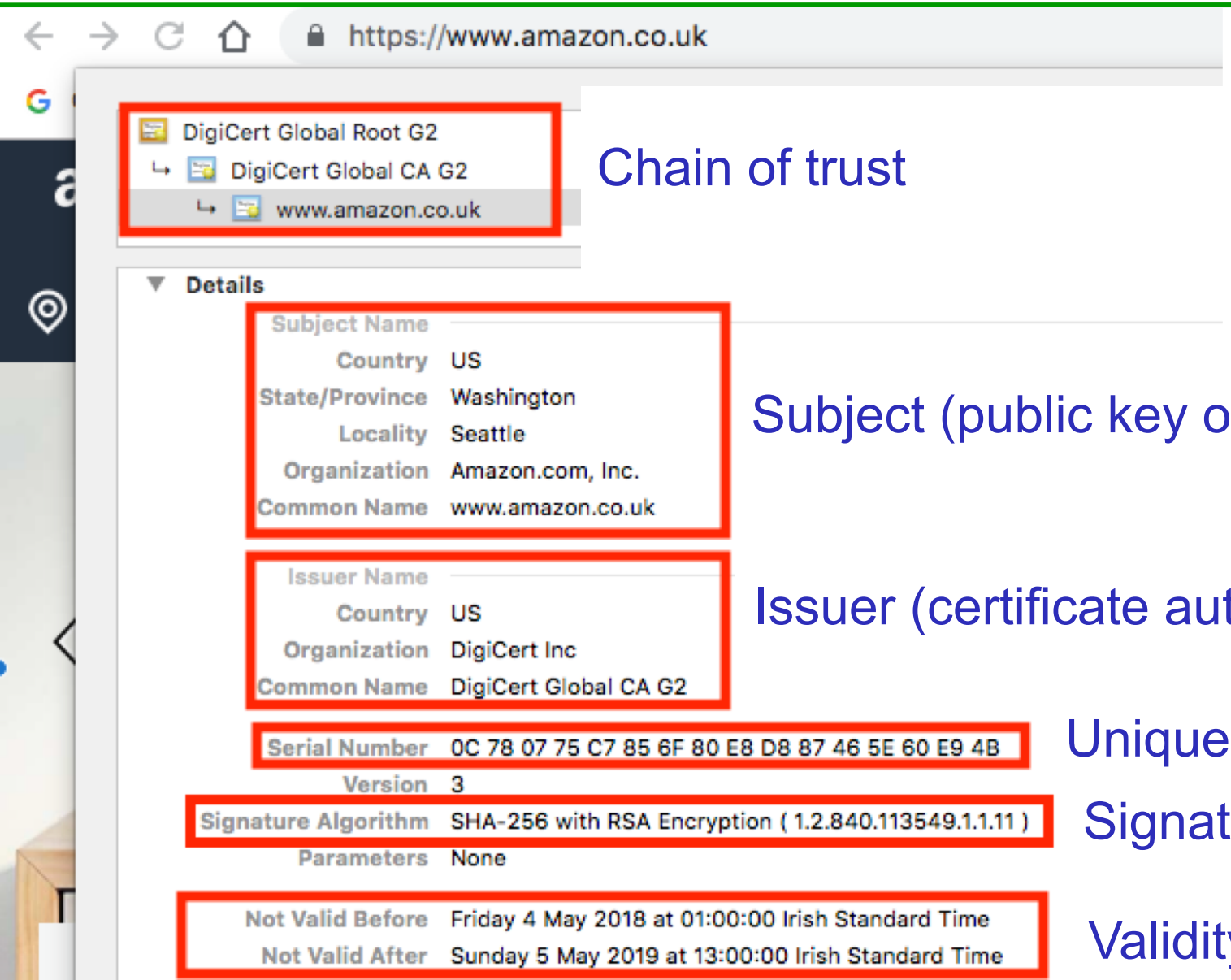
Digital Certificate

- 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



Chain of trust

Subject (public key owner)

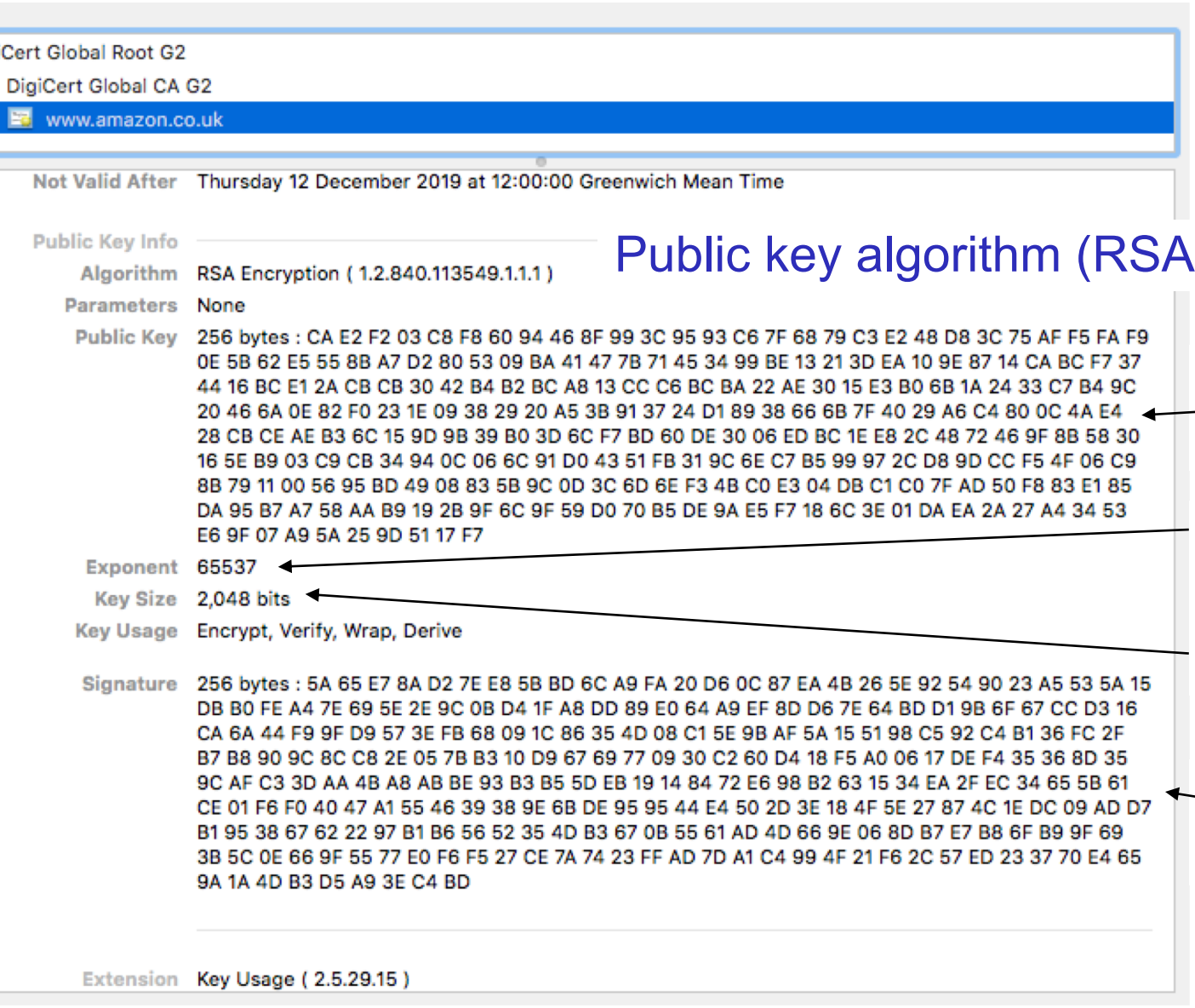
Issuer (certificate authority

Unique serial no.

Signature algorithm

Validity period

Digital Certificate – example (cont.)



Public key algorithm (RSA)

Public key (RSA modulus)

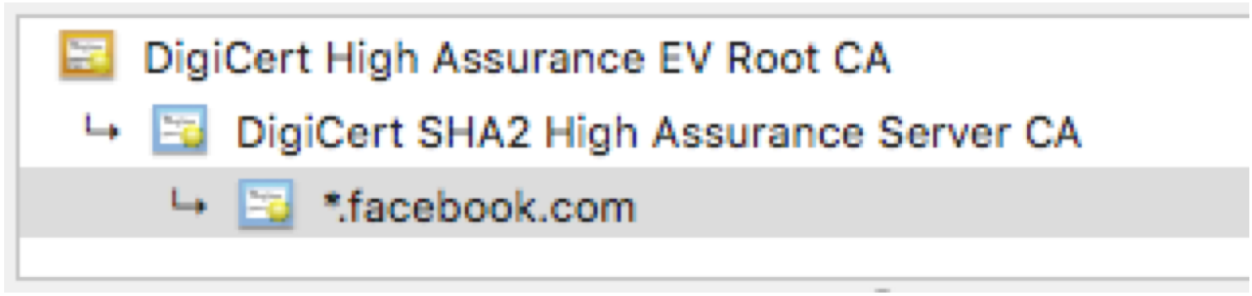
Exponent (part of RSA public key)

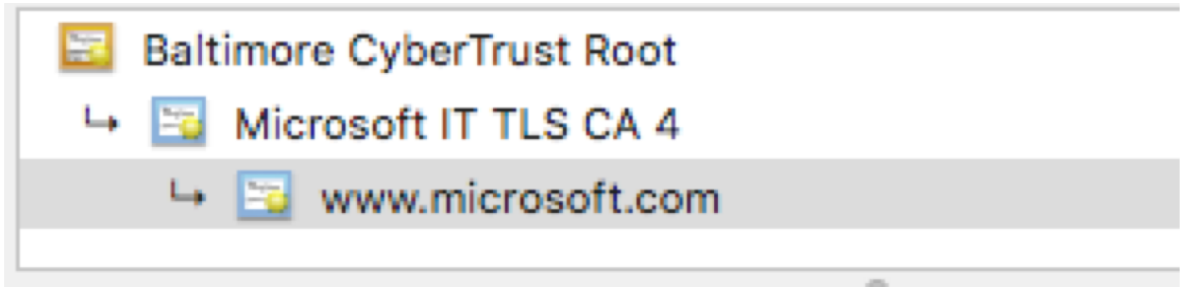
Key size (2048 bits)

Signature (signed hash)

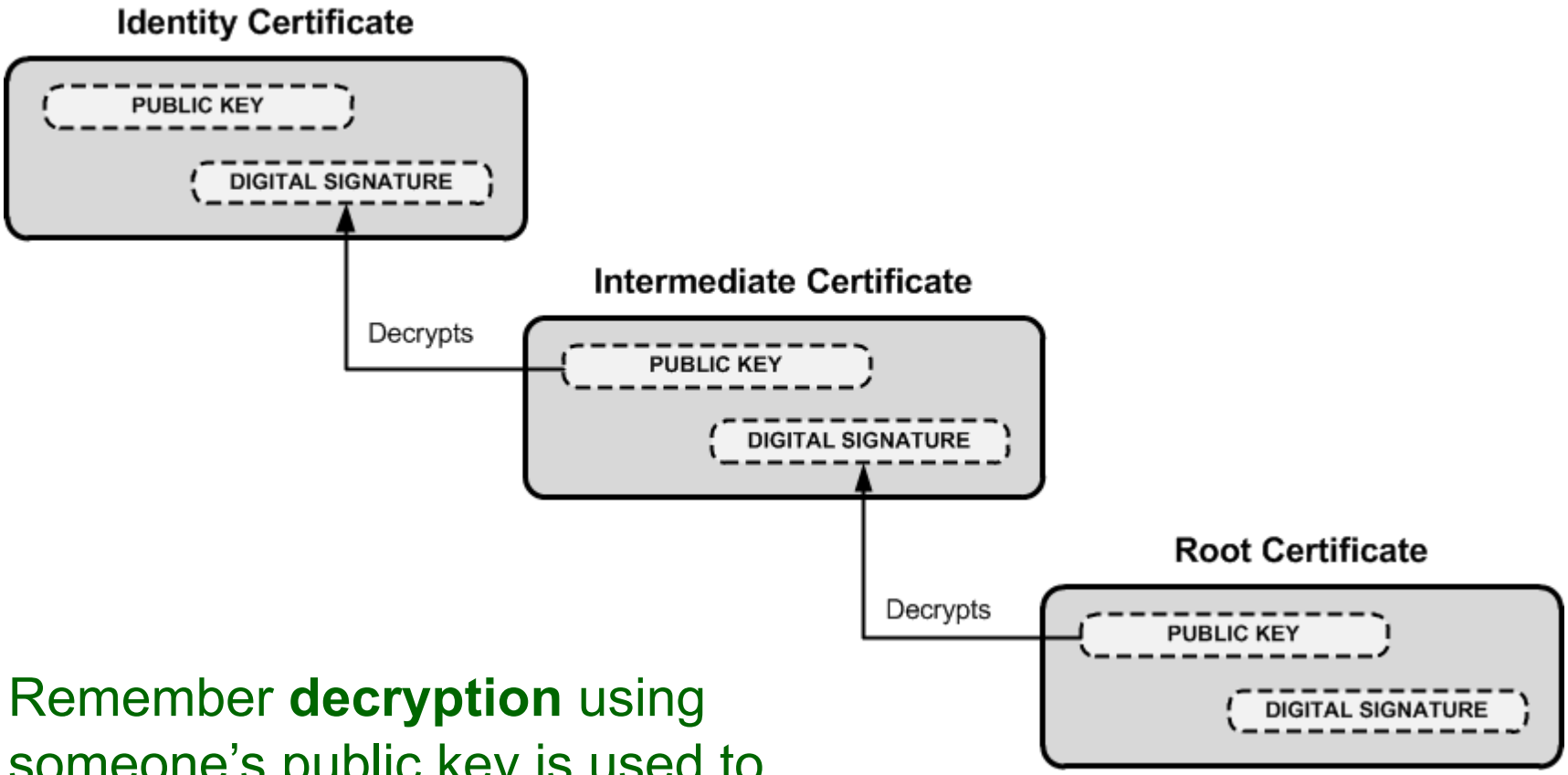
Chain of trust

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





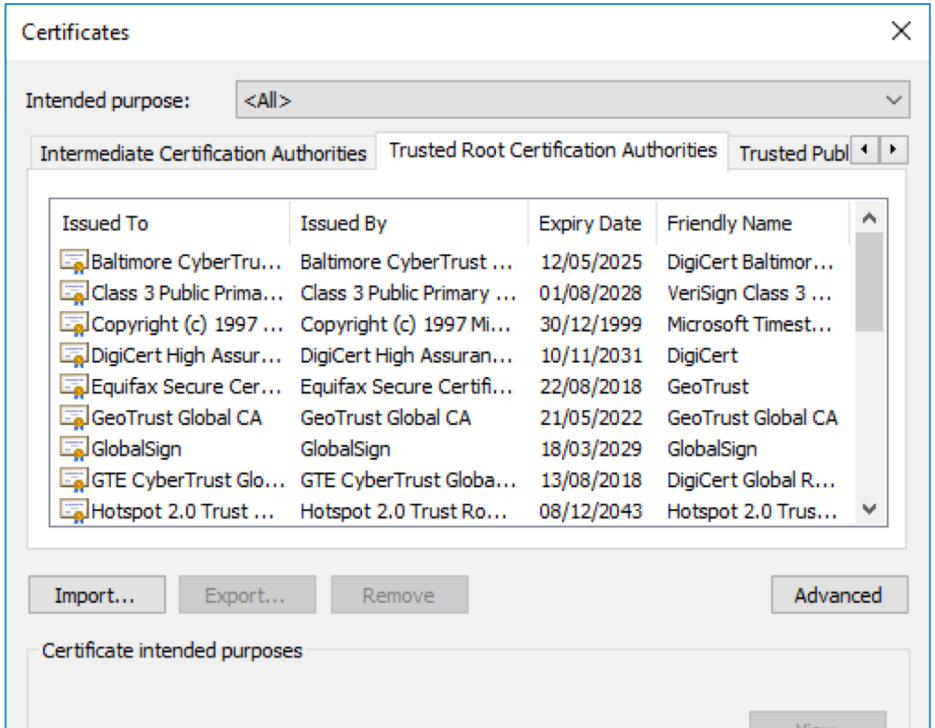
Verification using chain of trusts



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)