SSL Made Easy

Created by Brent Denny

Crypto Stuff

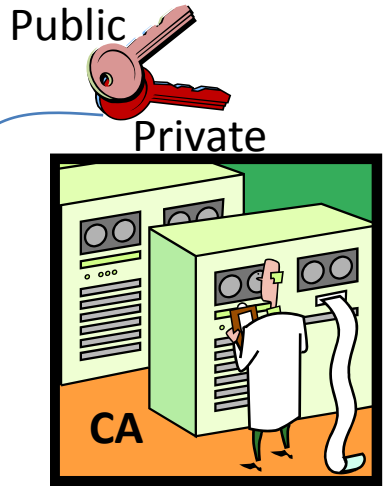
- Asymmetric Encryption
  - Public and Private Key Pair
  - Great security – One key encrypts the other decrypts
  - Not good for large data – Very slow, CPU taxing
- Symmetric Encryption
  - Single Key – same key used for encryption & decryption
  - Great for encryption speed
  - Not good for security, as the other party also needs the key

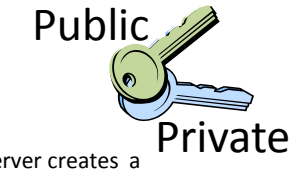
Crypto Stuff (Cont.)

- Hash (Message Digest)
  - Hash encryption creates a checksum type data
  - Same data hashed always results in same result
  - If the data is modified hash result will be different*
- SSL
  - Employs a hybrid system
  - Asymmetric keys help share the Symmetric keys
  - Hashing proves the data is authentic and unmodified

* Except in the very rare case of a hash collision

Certificate Request





1.WEB server creates a certificate request and sends it to the Certificate Authority

2. CA checks validity of request and builds a certificate for the web server

Contents of certificate include

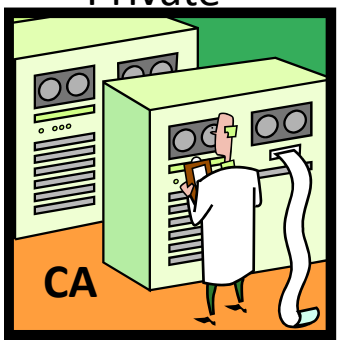
FQDN (that client uses to access WEB)
Dates the certificate is valid (from – to)
CA identification
PUBLIC key of WEB server
CRL (Revocation list pickup location)
Other info
Digital Signature (HASH signed by the PRIVATE key of the CA)

3. CA hashes the certificate and encrypts the hash with the PRIVATE key of the CA (Digital Signature)

4. Certificate is sent to the WEB server, the web server then adds the certificate to the bindings of the web site

In Case of a Security Breach

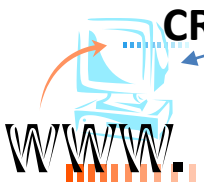
Private



Contents of certificate include

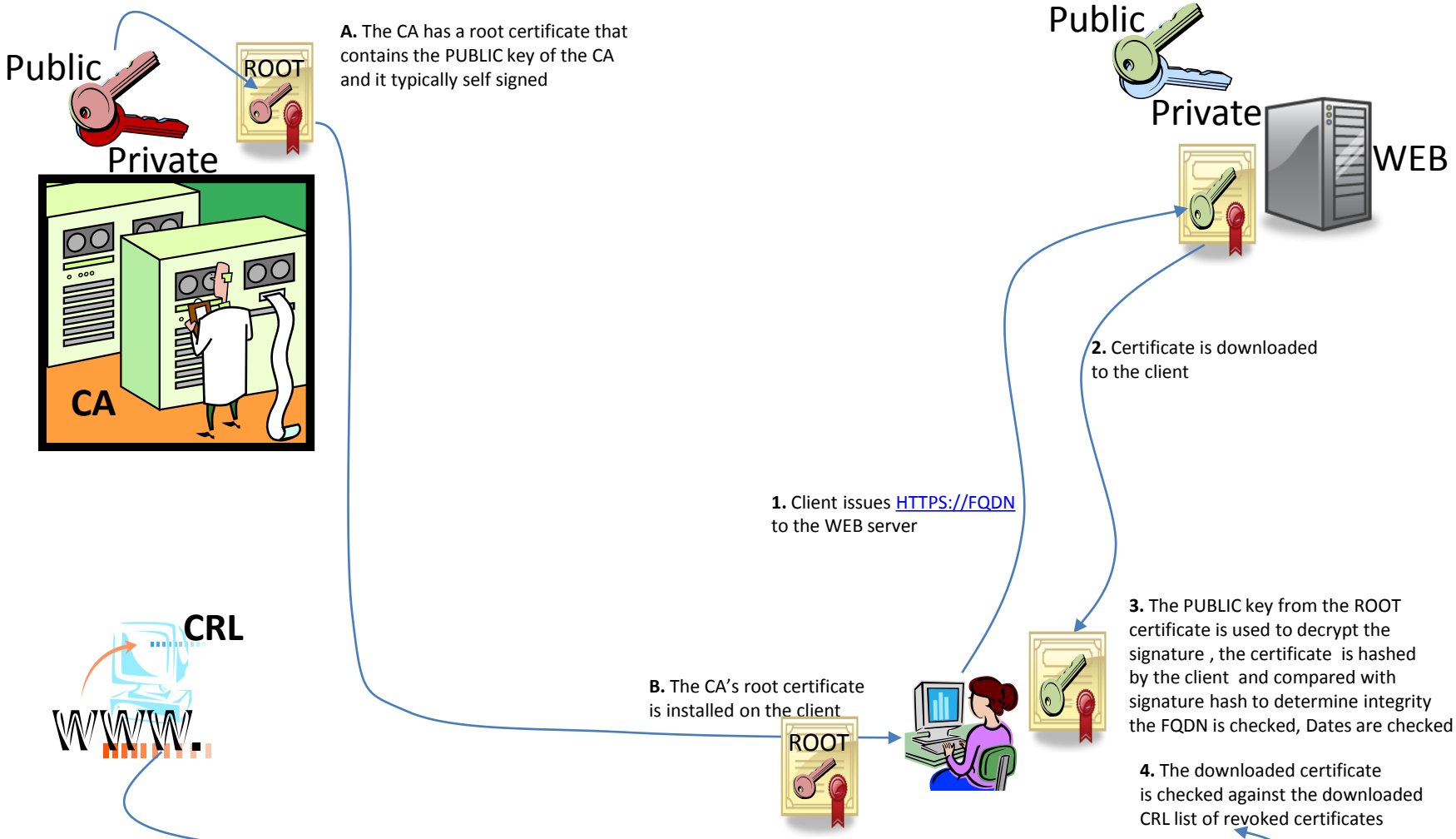
FQDN (that client uses to access WEB)
Dates the certificate is valid (from – to)
CA identification
PUBLIC key of WEB server
CRL (Revocation list pickup location)
Other info
Digital Signature (HASH signed by the PRIVATE key of the CA)

1. If there has been a security issue the CA revokes the certificate issued by this CA and adds the ID of the revoked certificate to a list called CRL (Certificate Revocation List)



2. The CA Publishes this CRL list in a web site or LDAP site setup for this purpose

Client using SSL (part 1)



Client using SSL (part 2)