SWINBURNE UNIVERSITY OF TECHNOLOGY

TNE30024

Deploying Secure Engineering Applications Online

Tutorial 2 (week 3)

Digital Certificates

Questions

1) What is a Digital Certificate?

A **Digital Certificate** is an electronic document used to prove the ownership of a public key. It is issued by a trusted third party called a Certificate Authority (CA) and contains information about the key owner, the key itself, and the digital signature of the CA. Digital certificates ensure that the public key belongs to the person or entity claiming to own it, and they are primarily used in secure communications such as SSL/TLS for website encryption.

2) What is a Root Certificate?

A **Root Certificate** is the top-level certificate in a Public Key Infrastructure (PKI) that is issued by a trusted Certificate Authority (CA). It is self-signed and is used to sign and issue other certificates, creating a chain of trust. The root certificate is trusted implicitly, meaning that it must be installed in the trusted certificate store of a browser or operating system.

3) Consider the following scenario:

Organisation A wishes to offer paid services via the Internet. They submit to Organisation B via a web interface an unsigned certificate, pay necessary fees and ask them to sign the certificate. Before signing the certificate Organisation B requests Organisation C to verify the certificate request. Organisation C verifies the request and informs Organisation B that the request is valid. Organisation B signs the certificate and issues it to Organisation A.

a) Which protocol does Organisation A (probably) need the certificate for?

Organisation A likely needs the certificate for the **SSL/TLS** protocol, which is used to secure communications over the Internet, particularly for paid services such as e-commerce.

b) Which organisation is the CA and which the RA?

- **Organisation B** is the **Certificate Authority (CA)** because it issues and signs the certificate.
- **Organisation C** is the **Registration Authority (RA)** because it verifies the request before the CA signs the certificate.

c) What sort of checks would Organisation C carry out?

Organisation C (the RA) would verify:

- The identity of Organisation A.
- That Organisation A controls the domain name or server.
- The authenticity of the certificate request.
- That Organisation A is a legitimate entity, possibly through documents or other forms of verification.

d) To get their certificate verified, does Organisation A include in the certificate request:

i) the public key? ii) the private key? iii) both? iv) Neither?

Organisation A includes i) the public key in the certificate request. The private key should never be shared or included in the request, as it is used to secure communications on the server.

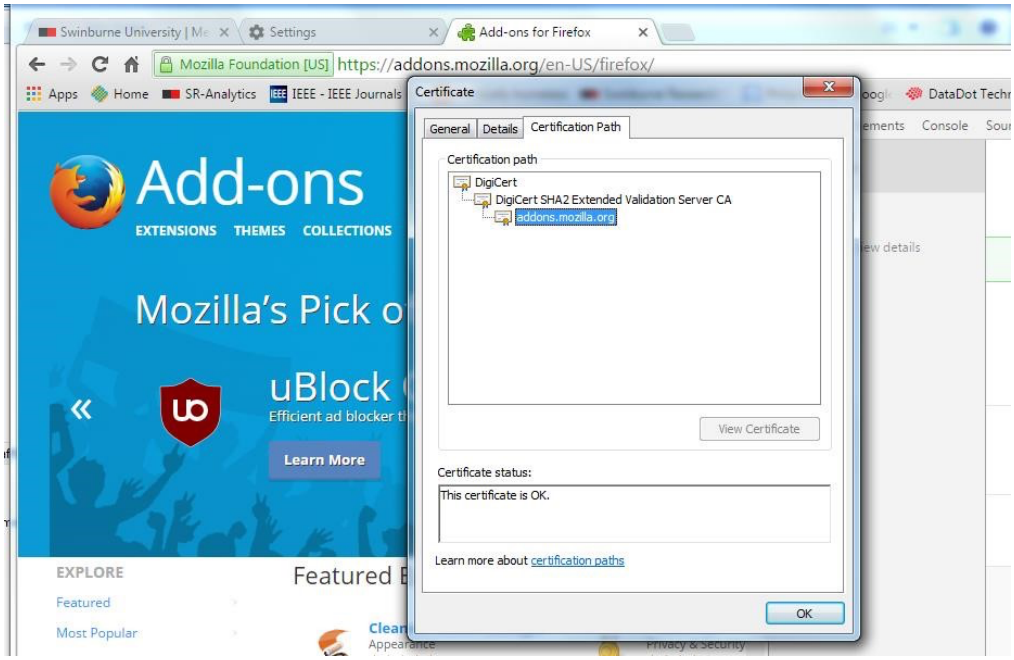
e) How would this process differ if the certificate is a private certificate?

If the certificate is a **private certificate** (e.g., for internal use within an organization), the certificate request may not need to go through an external CA or RA. Instead, it may be issued by an internal CA within the organization, and the verification process may be simpler or entirely skipped.

4) When purchasing goods via a website, why does the SSL/TLS protocol require the website to provide a digital certificate but not the person doing the purchasing?

The SSL/TLS protocol requires the **website** to provide a digital certificate because it ensures that the website is legitimate and that the user is communicating securely with the correct server. The person doing the purchasing (client) does not need to provide a certificate because SSL/TLS uses asymmetric encryption, where the client initiates a secure connection and can remain anonymous. Only the server needs to prove its identity to establish trust.

5) The following is a digital certificate for addons.mozilla.org. The certificate has been verified by clicking the lock icon. What steps will have taken place in verifying the certificate?



- **Certificate Chain Validation**: The browser checks that the certificate for `addons.mozilla.org` was issued by a trusted intermediate CA, which in turn was signed by a trusted root CA.

- **Digital Signature Verification**: The browser verifies the digital signature on the certificate to ensure it was indeed signed by the issuing CA.
- **Validity Check**: The browser checks the certificate's expiration date and validity period.
- **Revocation Status**: The browser checks if the certificate has been revoked by querying the CA's Certificate Revocation List (CRL) or using the Online Certificate Status Protocol (OCSP).
- **Domain Verification**: The browser confirms that the domain name in the certificate matches the website being accessed (`addons.mozilla.org`).
- **Trust Decision**: If all checks are successful, the browser displays the secure padlock icon to indicate the certificate is valid.

6) Alice wishes to send a message to Bob. In order to guarantee the validity of identity, who will require a digital certificate in the following situations?

   a) The message is to be encrypted.

Bob, the recipient, will require a digital certificate. Alice will use Bob's public key (from his certificate) to encrypt the message, ensuring only Bob (who holds the private key) can decrypt it.

   b) The message is to be signed.

Alice, the sender, will require a digital certificate. Alice will use her private key to sign the message, and Bob will verify the signature using Alice's public key from her certificate to ensure the message's authenticity.

7) What is the role of a Registration Authority (RA) in PKI? Is an RA needed for private certificates?

A **Registration Authority (RA)** in PKI is responsible for verifying the identity of entities (users, organizations, or devices) requesting digital certificates before the Certificate Authority (CA) issues the certificate. The RA acts as an intermediary between the certificate requester and the CA, ensuring that the request is legitimate and the certificate can be trusted.

For **private certificates**, an RA may not be necessary if the certificates are used internally within an organization. In such cases, the internal CA might perform both the RA and CA functions, or the identity checks could be handled in a simplified manner based on internal policies.