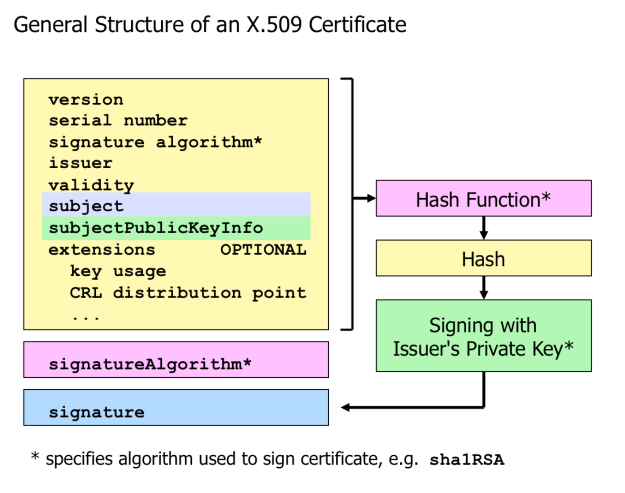
**IS ZA Digital Certificates**

Digital Certificates bind a **public key** to an identity

* Digital document that confirms that a public key belongs to a particular identity
* Dominating standard: X.509



Software components that process certificates are preconfigured to contain several root CA certifictes => Browsers, email-clients, PDF readers etc.

Certificate Revocation =>

* If certificate is no longer needed OR private key was compromised or stolen
  + Owner contacts the CA that issued the certificate
  + CA puts certificate serial number on a CRL

When application **validates** a certificate, it should therefore not only check certificate itself, but also **whether the certificate is still valid**

* Either download the **CRL** from the CA
* Or perform an online check at the CA using the **OCSP**

OCSP uses the HTTP protocol, the serial number is sent with the request

**The only way to revoke a root certificate is by removing it from the applications and systems where it is installed as trusted.**

Extended Validation Certificate:

* Most browsers user interfaces did not clearly differtiate between low-validation certificates and those that have undergone more rigourous vetting.
* By establishing stricter issuing criteria and requiring consistent application of those criteria by all participating Cas, EV SSL certificates are intended to restore confidence among users that a website operator is a legally established business or organization with a verifiable identity.
* Cas issuing EV certificates must follow certain guidelines about how to check the identity of the applicant

EV certificates therefore are a standard that link a certificate not only to a domain name, but also to an organization

Difference between normal and EV certificate:

* Special entry (object identifier, OID) => in the Certificate Policies extension