

Certificate Recipient  
(Subject)

**Certificate Signing  
Request (CSR)**

Domain  
Identity

...

Subject's Public Key

Certificate Authority (Issuer)

Sign(Hash(

**TBSCertificate**

Subject's info

Issuer's info

...

Subject's Public Key

))

**Certificate**  
TBSCertificate

...  
Signature