

Certificates

A certificate binds a public key to a certain individual/entity. This is usually done using digital signatures: if a certificate bearing a public key and an individual's name is signed with a key pair which you already trust, then you can rest assure that the public key in the certificate really does belong to the individual named in the certificate.