

User
(Owner)

Certificate Authority
(Issuer)

Public Key
Private Key

Certificate request

User Identity
Public Key

User Identity
Public Key
Issuer Identity
Algorithm names

Public Key
Private Key

Hash of request

Encryption

Certificate
User Identity
Public Key
Issuer Identity
Algorithm names
Signature

User Identity
Public Key
Issuer Identity
Algorithm names
Signature