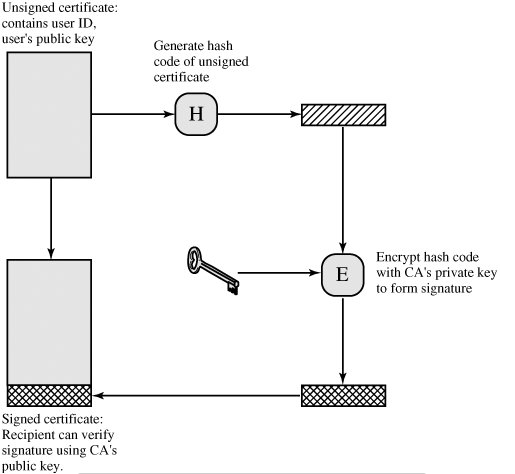
**X.509 Authentication Service**

X.509 defines a framework for the provision of authentication services by the X.500 directory to its users. The directory may serve as a repository of public key certificates. Each certificate contains the public key of a user and is signed with the private key of a trusted certification authority.X.509 defines alternatives authentication protocols based on the use of public-key certificates.

It was initially issued in 1988.The standard was subsequently revised to address some security concerns and hence a revised recommendation was issued in 1993.The third version was issued in 1995 and revised in 2000.

X.509 is based on the use of public-key cryptography and digital signatures. Digital signature is assumed to require use of a hash function but there is no dictation of a specific hash algorithm. The diagram illustrates the generation of a public key certificate.



CERTIFICATE

Heart of the x.509 scheme is the public key certificate associated with each user. These user certificates are assumed to be created by a certification authority and placed in the directory by the user. Directory is not responsible for the creation of public keys or for certification function.

Entire format of a certificate.

