Certificates

# X.509 Authentication Service

ITU-T (International Telecommunication Union – Telecommunication Standardization Sector) recommendation X.509 is a part of the X.500 series of recommendations that define a directory service. The directory is a server or distributed set of servers that maintains a database of information about users. The information includes a mapping from user name to network address, as well as other attributes and information about the users.

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 alternative authentication protocols based on the use of public-key certificates.

X.509 is an important standard because the certificate structure and authentication protocols defined in X.509 are used in variety of contexts (SSL, SET, etc.).

A third version of X.509 was issued in 1995 and revised in 2000.

# Certificates

The heart of X.509 scheme is the public-key certificate associated with each user. These user certificates are assumed to be created by some trusted certificate authority (CA) and placed in the directory by the CA or by the user. The directory itself is not responsible for the creation of public keys or for the certification function; it merely provides an easily accessible location for users to obtain certificates.

Figure 14.3a shows the general format of a certificate, which includes the following elements ([www.dante.net/np/ds/osi/9594-8-X.509.A4.ps](http://www.dante.net/np/ds/osi/9594-8-X.509.A4.ps) ):



# Certificates (Cont 1)

1. Version: Differentiates among successive versions of the certificate format: the default version is 1. If the Issuer Unique Identifier or Subject Unique Identifier are present, the value must be version 2. If one or more extensions are present, the version must be version 3.
2. Serial number: An integer value, unique within the issuing CA, that is unambiguously associated with this certificate
3. Signature algorithm identifier: The algorithm used to sign the certificate, together with any associated parameters. Because this information is repeated in the Signature field at the end of the certificate, this field has little, if any, utility
4. Issuer name: X.500 name of the CA that created and signed this certificate (about X.500 names see, for example, http://java.sun.com/products/jndi/tutorial/ldap/models/x500.html )
5. Period of validity: Consists of two dates: the first and the last on which certificate is valid
6. Subject name: The name of the user to whom this certificate refers. That is, this certificate certifies the public key of the subject who holds the corresponding private key
7. Subject’s public key information: The public key of the subject, plus an identifier of the algorithm for which this key is to be used, together with any associated parameters
8. Issuer unique identifier: An optional bit string field used to identify uniquely the issuing CA in the event the X.500 name has been reused for different entities
9. Subject unique identifier: An optional bit string used to identify uniquely the subject in the event the X.500 name has been reused for different entities
10. Extensions: A set of one or more extension fields. Extensions were added in version 3 and are discussed later

Signature: Covers all of the other fields of the certificate; it contains the hash code of the other fields, encrypted with the CA’s private key. This field includes the signature algorithm identifier