X.509 标准简介

服务器 SSL 数字证书和客户端单位数字证书的格式遵循 X.509 标准。X.509 是由国际电信联盟（ITU-T）制定的数字证书标准。为了提供公用网络用户目录信息服务，ITU 于 1988 年制定了 X.500 系列标准。其中 X.500 和 X.509 是安全认证系统的核心， X.500 定义了一种区别命名规则，以命名树来确保用户名称的唯一性； X.509 则为 X.500 用户名称提供了通信实体鉴别机制，并规定了实体鉴别过程中广泛适用的证书语法和数据接口，X.509 称之为证书。

X.509 给出的鉴别框架是一种基于公开密钥体制的鉴别业务密钥管理。一个用户有两把密钥：一把是用户的专用密钥(简称为：私钥)，另一把是其他用户都可得到和利用的公共密钥(简称为：公钥)。用户可用常规加密算法（如 DES）为信息加密，然后再用接收者的公共密钥对 DES 进行加密并将之附于信息之上，这样接收者可用对应的专用密钥打开 DES 密锁，并对信息解密。该鉴别框架允许用户将其公开密钥存放在 CA 的目录项中。一个用户如果想与另一个用户交换秘密信息，就可以直接从对方的目录项中获得相应的公开密钥，用于各种安全服务。

最初的 X.509 版本公布于 1988 年 ,版本 3 的建议稿 1994 年公布 ,在 1995 年获得批准。本质上，X.509 证书由用户公共密钥与用户标识符组成，此外还包括版本号、证书序列号、CA 标识符、签名算法标识、签发者名称、证书有效期等。用户可通过安全可靠的方式向 CA 提供其公共密钥以获得证书，这样用户就可公开其证书，而任何需要此用户的公共密钥者都能得到此证书，并通过 CA 检验密钥是否正确。这一标准的最新版本 -- X.509 版本 3 是针对包含扩

展信息的数字证书，提供一个扩展字段，以提供更多的灵活性及特殊环境下所需的信息传送。

为了进行身份认证， X.509 标准及公共密钥加密系统提供了一个称作数字签名的方案。用户可生成一段信息及其摘要（亦称作信息“指纹”）。用户用专用密钥对摘要加密以形成签名，接收者用发送者的公共密钥对签名解密，并将之与收到的信息“指纹”进行比较，以确定其真实性。

目前，X.509 标准已在编排公共密钥格式方面被广泛接受，已用于许多网络安全应用程序，其中包括 IP 安全（Ipsec）、安全套接层（SSL）、安全电子交易（SET）、安全多媒体 INTERNET 邮件扩展（S/MIME）等。