**X.509**

**Q: Give me an example of X.509 certificate and tell me how it works.**

1. X.509简介

X.509是被广泛使用的数字证书标准，是由国际电联电信委员会（ITU-T）为单点登录（SSO-Single Sing-on）和授权管理基础设施（PMI-Privilege Management Infrastructure）制定的PKI标准。X.509定义了（但不仅限于）公钥证书、证书吊销清单、属性证书和证书路径验证算法等证书标准。

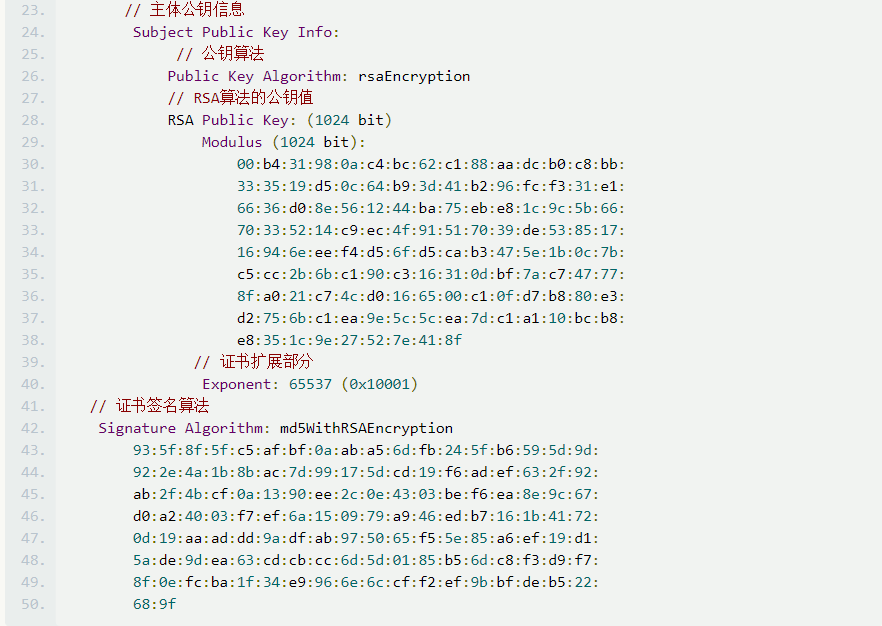
1. X.509基本结构



1. X.509实例

以下是一个典型的X.509证书实例

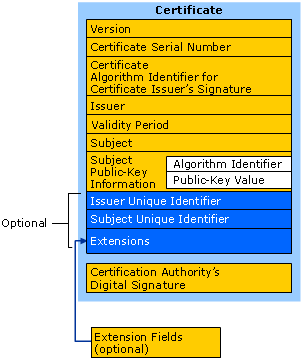




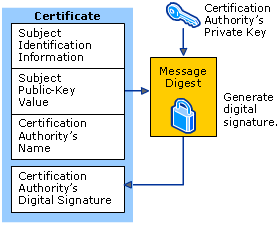
1. X.509工作描述
2. 基本原理

数字证书是用来确认网络上个人电脑和其他实体的在线身份的电子凭证。数字证书的作用类似于身份证，如护照和驾驶证，由认证机构(certificate authority,CA)颁发。 CA用自己的私钥对用户的身份信息(主要是用户名和该用户的公钥)进行签名，该签名和用户的身份信息一起就形成了证书。除用户信息外，数字证书中还包括证书机构名称,证书有效期,证书的序列号,签名使用的哈希算法,公钥使用的加密算法等相关信息。

1. 证书结构

右图为X.509第三版证书的内容，详细描述可见上页（2.X.509基本结构）

1. 工作过程
2. 使用用户的身份信息生成数字签名

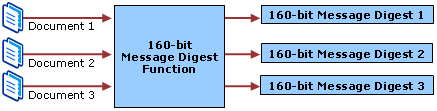
一个CA使用其私有密钥对每次发出的证书进行数字签名。为了创建数字签名，从该证书生成摘要，加密该摘要用其私钥，并且把数字签名作为证书的一部分。任何人都可以使用的消息摘要函数和CA的公钥来验证证书的完整性。如果证书已损坏或者与它人篡改，被改变的证书的信息摘要将和数字签名不匹配。下图显示了由CA生成数字签名的方式。

1. 签名验证

用户A把自己的证书发送给用户B。用户B使用CA的公钥对证书的签名进行验证，由于只有CA才能生成该证书，因此只要证书验证正确，即说明证书是由CA发布的，证书中用户A的公钥是值得信赖的。用户B以后就可以使用该公钥验证用户A的签名或者和A进行加密通信。

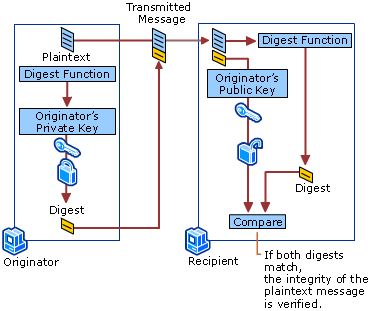
1. 消息摘要函数

消息摘要函数，也称为散列函数，常用结合非对称密钥，以进一步加强公共密钥加密。消息摘要是通常为128位至160位的长度，并为每个数字文件或文档的唯一数字标识符。文档的两个副本都会有相同的消息摘要，即使修改文件中的一个比特，都会导致消息摘要的变化。下图显示了基本的消息摘要过程。



消息摘要是结合常用的与公开密钥技术来创建数字签名或用于认证，完整性和不可抵赖性的“数字指纹”。消息摘要还与数字签名技术常用于电子文件和文档提供数据完整性。

1. 基本的完整性检查过程



如果消息摘要和证书中包含的数字签名不匹配，认为其被更改或损坏。

1. 如何验证证书机构的公钥-证书的证书

用户B使用证书机构的公钥来验证用户A的数字证书，但如何又能够知道用户B拿到的证书机构的公钥不是伪造的呢？解决办法是再找一个证书机构对该证书机构的公钥颁发一个证书，这样形成了一个公钥证书的嵌套循环，该循环的终点就是根证书机构。根证书机构较少，其公钥可以通过安全的方式发布，如通过USB拷贝、书面文件当面移交。

