# java生成数字证书(1)

原文链接：<https://blog.csdn.net/happylee6688/article/details/42235613>

## 概要

## 这篇文章，我主要是想谈一下 CA 证书的工作原理，数字签名，证书格式等几个比较重要的概念。因为在后续的文章中，都会用到这几个概念，而且，想要自己做证书，这几个概念是必须要弄懂的。

## 什么是数字证书

数字证书就是互联网通讯中标志通讯各方身份信息的一串数字，提供了一种在 Internet 上验证通信实体身份的方式，其作用类似于司机的驾驶执照或日常生活中的身份证。它是由一个由权威机构 —— CA 机构，又称为证书授权（Certificate Authority）中心发行的，人们可以在网上用它来识别对方的身份。数字证书是一个经证书授权中心数字签名的包含公开密钥拥有者信息以及公开密钥的文件。最简单的证书包含一个公开密钥、名称以及证书授权中心的数字签名。数字证书还有一个重要的特征就是只在特定的时间段内有效。

## 原理

数字证书里存有很多数字和英文，当使用数字证书进行身份认证时，它将随机生成128位的身份码，每份数字证书都能生成相应但每次都不可能相同的数码，从而保证数据传输的保密性，即相当于生成一个复杂的密码。

数字证书绑定了公钥及其持有者的真实身份，它类似于现实生活中的居民身份证，所不同的是数字证书不再是纸质的证照，而是一段含有证书持有者身份信息并经过认证中心审核签发的电子数据，可以更加方便灵活地运用在电子商务和电子政务中。

## 颁发

数字证书颁发过程一般为：用户首先产生自己的密钥对，并将公共密钥及部分个人身份信息传送给认证中心。认证中心在核实身份后，将执行一些必要的步骤，以确信请求确实由用户发送而来，然后，认证中心将发给用户一个数字证书，该证书内包含用户的个人信息和他的公钥信息，同时还附有认证中心的签名信息。

用户就可以使用自己的数字证书进行相关的各种活动。数字证书由独立的证书发行机构发布。数字证书各不相同，每种证书可提供不同级别的可信度。可以从证书发行机构获得您自己的数字证书。

## 工作原理

数字证书采用公钥体制，即利用一对互相匹配的密钥进行加密、解密。每个用户自己设定一把特定的仅为本人所知的私有密钥（私钥），用它进行解密和签名；同时设定一把公共密钥（公钥）并由本人公开，为一组用户所共享，用于加密和验证签名。

当发送一份保密文件时，发送方使用接收方的公钥对数据加密，而接收方则使用自己的私钥解密，这样信息就可以安全无误地到达目的地了。通过数字的手段保证加密过程是一个不可逆过程，即只有用私有密钥才能解密。

在公开密钥密码体制中，常用的一种是RSA体制。其数学原理是将一个大数分解成两个质数的乘积，加密和解密用的是两个不同的密钥。即使已知明文、密文和加密密钥（公开密钥），想要推导出解密密钥（私密密钥），在计算上是不可能的。

按现在的计算机技术水平，要破解目前采用的1024位RSA密钥，需要上千年的计算时间。公开密钥技术解决了密钥发布的管理问题，商户可以公开其公开密钥，而保留其私有密钥。购物者可以用人人皆知的公开密钥对发送的信息进行加密，安全地传送给商户，然后由商户用自己的私有密钥进行解密。

## 数字签名

用户也可以采用自己的私钥对信息加以处理，由于密钥仅为本人所有，这样就产生了别人无法生成的文件，也就形成了数字签名。采用数字签名，能够确认以下两点：

* 保证信息是由签名者自己签名发送的，签名者不能否认或难以否认。
* 保证信息自签发后到收到为止未曾作过任何修改，签发的文件是真实文件。

将报文按双方约定的HASH算法计算得到一个固定位数的报文摘要。在数学上保证：只要改动报文中任何一位，重新计算出的报文摘要值就会与原先的值不相符。这样就保证了报文的不可更改性。

将该报文摘要值用发送者的私人密钥加密（对明文进行解密完全没问题，会得出一个不可读的“明文”），然后连同原报文一起发送给接收者，而“加密”后的报文即称数字签名。

接收方收到数字签名后，用同样的HASH算法对原报文计算出报文摘要值，然后与用发送者的公开密钥对数字签名进行解密（原先已经把签名加密了，现在再解密就能还原）得到的报文摘要值相比较。如相等则说明报文确实来自所称的发送者。

由于只有拥有私钥的签名者能通过“解密”摘要生成签名，因此具有安全和不可抵赖性。

那为什么是对报文摘要进行加密，而不是对原报文进行加密呢？这是因为RSA加解密非常耗时，被加密的报文越大，耗得时间越多，因此聪明的人类对其摘要进行加密，（因为报文摘要是要比原报文小得多），仍然能够起到同样的作用。这是为什么多了个报文摘要。

## 证书格式

目前数字证书的格式普遍采用的是X.509V3国际标准，一个标准的X.509数字证书包含以下一些内容：

* 证书的版本信息；
* 证书的序列号，每个证书都有一个唯一的证书序列号；
* 证书所使用的签名算法；
* 证书的发行机构名称，命名规则一般采用X.500格式；
* 证书的有效期，现在通用的证书一般采用UTC时间格式，它的计时范围为1950-2049；
* 证书所有人的名称，命名规则一般采用X.500格式；
* 证书所有人的公开密钥；
* 证书发行者对证书的签名。



作为文件形式存在的证书一般有这几种格式：

* 带有私钥的证书由Public Key Cryptography Standards #12，PKCS#12标准定义，包含了公钥和私钥的二进制格式的证书形式，以pfx作为证书文件后缀名。
* 二进制编码的证书 证书中没有私钥，DER 编码二进制格式的证书文件，以cer作为证书文件后缀名。
* Base64编码的证书证书中没有私钥，BASE64 编码格式的证书文件，也是以cer作为证书文件后缀名。

由此可看出，只有 pfx 格式的数字证书是包含有私钥的，cer 格式的数字证书里面只有公钥没有私钥。当然，我们经常使用的数字证书就是 cer 格式的，比如，12306 颁发的数字证书，就是这种格式的，购票之前，需要在自己的电脑上安装证书，以确保我们的客户端可以与正确的服务器进行通信。

当然，正如上面所说，CA 证书还是可以自己生成的，只不过自己生成的证书对于操作系统来说，是识别不了的，因为操作系统中并没有存在生成证书的发行机构。不过，这并不妨碍我们正常的使用证书。