# java生成数字证书(2)

原文链接：<https://blog.csdn.net/happylee6688/article/details/42238821>

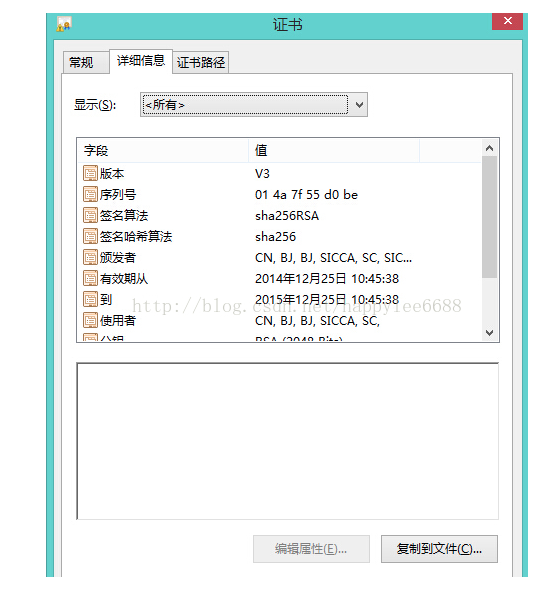
## 序

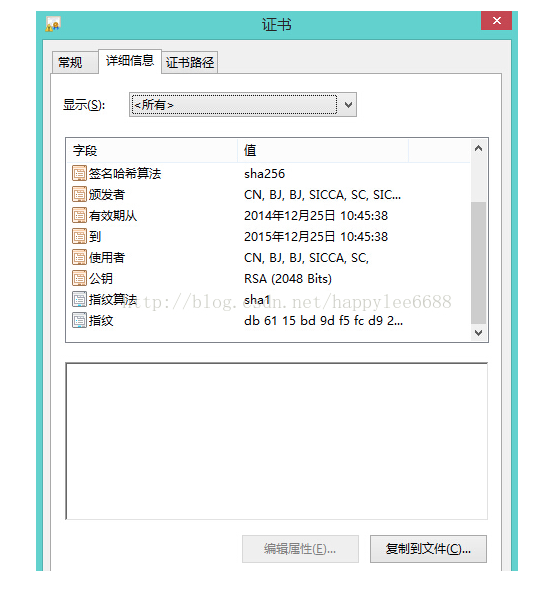
上一篇介绍了一下 CA 证书的几个相关概念，这几个概念还是很重要的，目的在于了解数字证书，以及其的工作原理。这篇文章主要是对 CA 证书进行剖析，讲一下证书的基本构成，这对于生成正确的、可以访问的证书是必不可少的。

## 构成

废话不多说，直接上内容。

先看一下证书到底是什么，在 Windows 下查看证书时（这里以 cer 为例），界面是这样的。





常规选项卡里，主要介绍了证书信息，颁发者，和有效日期等。

而 详细信息 选项卡中，包含的信息是比较多的，他们都是以一种 Key — Value 的形式存在的，其中字段包括：版本、序列号、签名算法、颁发者、有效期、公钥、指纹等等。在上一篇文章中也有提到。下面我们就详细的来看看这些字段到底是干什么用的。

## 详细信息

* 版本（Version）

很明显，这个是证书的版本号，不同版本的证书格式是不同的。这里，我用的是 V3 版本。

* 序列号（Serial Number）

证书序列号，同一身份验证机构签发的证书序列号是唯一的。

* 签名算法（Signature algorithm）

签名算法，指的是这个数字证书中的数字签名所使用的加密算法，可以通过根证书中的公钥对这个证书中的指纹进行解密。

* 颁发者（Issuer）

证书发布机构，指出这个证书是哪个公司创建的，这是哪个 CA 中心的证书。当然，如果是你自己公司生成的证书，那么颁发者就是你自己的公司了。

* 有效期（Valid from to）

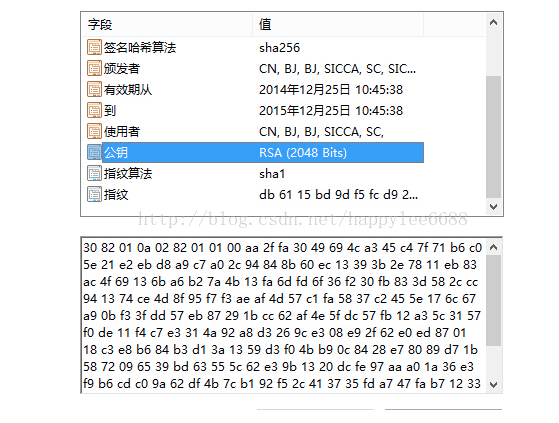
证书的生成日期，以及证书使用的截至日期。证书有效期失效之后，在认证服务器中会进行校验，校验失败后，重新生成新证书或者是其他的操作。这个依据证书的发布机构而定。

* 使用者（Subject）

这个证书是发布给谁的，或者说是证书的所有者，一般是某个人或者某个公司的名称、机构的名称、公司网站的网址等。当然，如果是根证书的话，那么，使用者就是自己的公司了。

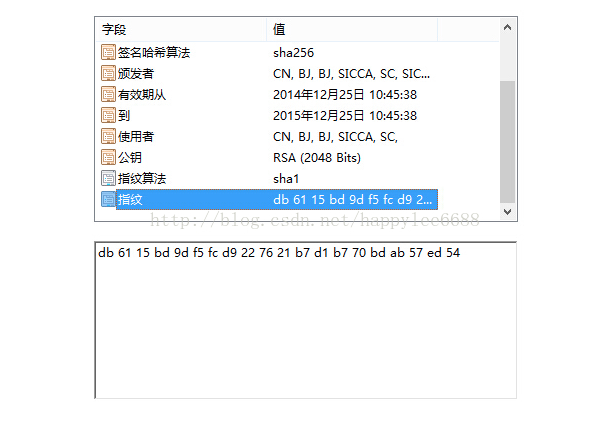
* 公钥（Public key）

证书的公钥，主要是用来对消息进行加密的，这个证书的公钥是 2048 位的，他的值可以在对话框中看到，是很长的一段十六进制数。



* 指纹及指纹算法（Thumbprint、Thumbprint algorithm）

指纹以及指纹算法，在证书发布的时候，发布机构会根据指纹算法先计算出整个证书的hash值，并使用证书发布机构的私钥对其进行签名构成一个指纹，并将指纹与该证书放在一起。



在生成证书的时候，需要自己设定颁发者、有效期、使用者等等。版本、签名算法、以及证书公钥等都是要设定的，否则生成的证书是无法正常使用的。