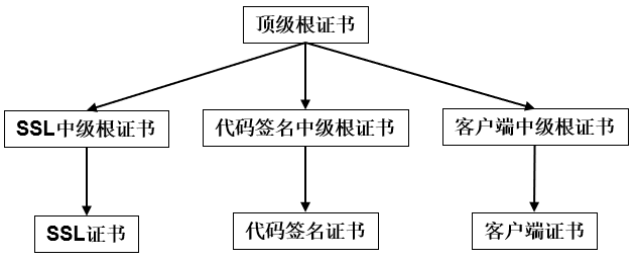
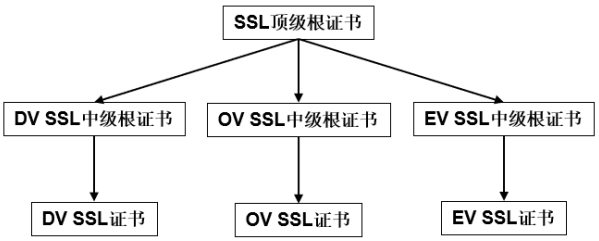
第 5 讲 什么是根证书？什么是可信根认证计划？

上一讲讲了多个非 CA 领域从业者可能不太懂的名词：根证书、顶级根证书、中级根证书、证书链、信任链等等，本讲就重点讲这些。我在第 3 讲讲 PKI 时讲过用 PKI 系统数字签名公钥后就是数字证书，数字证书含有 PKI 系统认证过的身份信息，用于证明拥有私钥的个体的可信身份。这里，并没有讲 PKI 系统用谁的私钥签名的？为何 PKI 系统签名后的数字证书是可信的？本讲详细讲解这个全球互联网的信任体系。

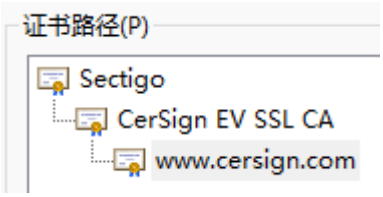
PKI 系统要对个体公钥实现数字签名一定要有一个私钥用于数字签名这个个体公钥，这个用于数字签名个体公钥的证书就是用于签发用户证书的根证书(Issuing CA)。而为了保障这个重要的根证书的安全，就增加了顶级根证书(Root CA)来负责签发这个用于签发用户证书的根证书，这个用于签发用户证书的根证书(Issuing CA)就称之为中级根证书(Intermediate CA)，或子根证书/从根证书(Sub CA)。顶级根证书仅用于离线签发中级根证书，而中级根证书就可以用于在线签发用户证书了。为了保障顶级根证书的安全，必须离线保存在安全房间的保险柜里，只有在需要签发中级根证书或签发中级根证书的吊销列表时才会拿出来用一下，一般情况下一年用一次，其余时间都是在保险柜里睡大觉的。顶级根证书有效期不能超过 25 年，中级根证书有效期不能超过 10 年。

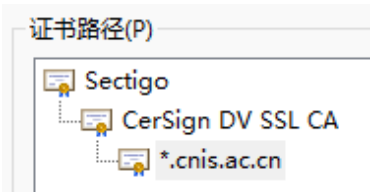
如下左图所示就是目前典型的证书链结构，顶级根证书签发用于签发 SSL 证书的中级根证书，称之为 SSL 中级根证书，可以有多个用于签发不同类型的 SSL 证书。用于签发代码签名证书的中级根证书称之为代码签名中级根证书，用于签发客户端证书的中级根证书称之为客户端中级根证书。不同类型用途的证书必须从不同的中级根证书签发，设置不同增强密钥用法，不能混用。但是，鉴于各种不同类型的数字证书的签发规则不同，各大浏览器和操作系统现在要求用于签发不同用途的数字证书必须独立设立顶级根证书，如下右图所示，SSL 顶级根证书专门用于签发 SSL 证书，该顶级根下面再签发三个不同类型的 SSL 证书专用中级根证书，如 DV SSL 中级根证书、OV SSL 中级根证书和 EV SSL 中级根证书，分别用于签发 DV SSL 证书、OV SSL 证书和 EV SSL 证书。至于这几种 SSL 证书有什么不同，将在下期详细讲解。





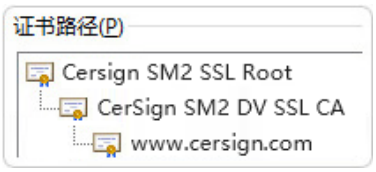
我们来看一看实际证书链(也叫证书路径)，如下图所示，Sectigo 就是顶级根证书，CerSign EV SSL CA 用于签发 EV SSL 证书，CerSign OV SSL CA 用于签发 OV SSL 证书，CerSign DV SSL CA 用于签发 DV SSL 证书。

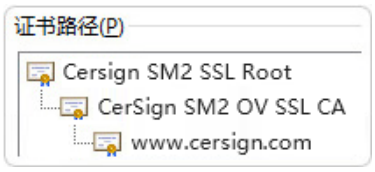


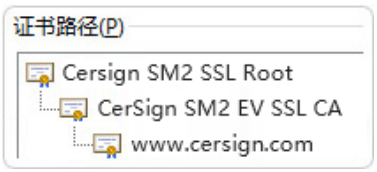


Sectigo 这个顶级根证书还用于签发代码签名证书和客户端证书，如下图所示：

我们再看一组采用国密算法的国密 SSL 证书专用顶级根证书的证书链，如下图所示，CerSign SM2 SSL Root 是一个专门用于签发 SSL 证书的国密算法顶级根证书，已经签发了三个 SSL 中级根证书，分别用于签发国密 DV SSL 证书、国密 OV SSL 证书和国密 EV SSL 证书，不能用于签发其他类型的数字证书。

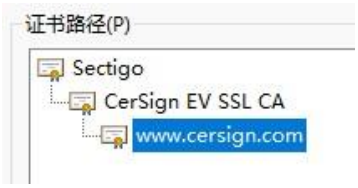






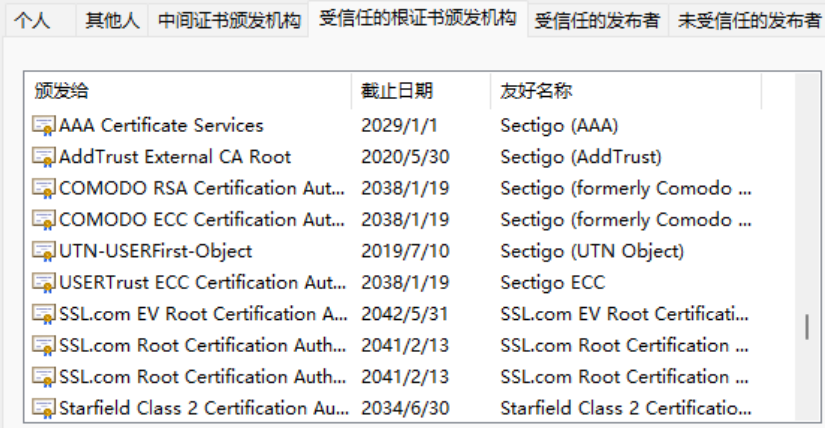
讲证书链，当然不能不讲交叉签名。交叉签名就是用一个顶级根证书给另外一个顶级根签名，签名后另外一个顶级根成为了第一个顶级根证书的中级根证书，原先的 3 级证书链就变成

了 4 级证书链。为什么要做交叉签名呢？当然是因为被交叉签名的根一般是新根，浏览器和操作系统还未信任和没有全部信任，需要用老根来带新根，就像出道的明星带新人一样的道理。如下左图所示，Sectigo AAA (AAA Certificate Services)是一个 2004 年的老根证书，而 Sectigo (USERTrust RSA Certification Authority)是 2010 年的根证书，老根 AAA Certificate Services 已经给这个新根做了交叉签名，这就是为何许多读者看到证书链为 4 级的情况。而如果删除这个 Sectigo AAA 根证书或禁用交叉签名证书，则证书链会显示为如下中图的 3 级证书链。也就是说，这张 SSL 证书可以走两条信任链，一个是走 Sectigo AAA 顶级根的信任链，一个是走 Sectigo 顶级根的信任链，Windows 的证书验证机制是优先走签发日期较新的信任链，由于交叉根证书是 2019 年签名的，这就是为何不少用户反映为何 CerSign 签发给用户的 SSL 证书总是显示为 4 级证书链。如果 Sectigo 在签发交叉根证书是使用比新的根证书还要早一分钟的时间，则 Windows 会优先显示 Sectigo (USERTrust)这个 3 级证书链。



零信浏览器在验证国密根证书时改进了 Windows 的信任链验证方式，如果有两个顶级根证书都是预置信任的，则验证到某个根证书是信任的，即使不是自签证书，也不再往上验证。这样就不会再走交叉根这条证书链了。这个验证方式的改进减少了证书链验证次数，加快了证书验证速度，能更快速地显示加密锁标识，也有利于新根直接显示为顶级根证书。

最后简单讲一讲浏览器或操作系统的可信根证书认证计划，目前各大浏览器都有自己的可信根证书认证计划，CA 机构需要按照浏览器厂商的要求提交相关的材料申请预置信任其顶级根证书。也就是说，各个浏览器维护了一个自己的信任源列表，只有浏览器信任的顶级根证书签发的 SSL 证书，浏览器才会信任并显示加密锁标识，否则会提示“不安全”或“根证书不受信任”。上面截图显示的完整证书链是因为 Windows 已经信任了 Sectigo 的顶级根证书，大家才会看到正常的 3 级或 4 级证书链。零信浏览器也有自己的可信根证书认证计划，所以，大家看到的完整的国密 SSL 证书证书链是因为此国密根证书在零信浏览器中已预置信任，大家如果下载这张证书在 Windows 中查看，则是无法正常显示的，因为 Windows 无法正常识别 SM2 算法 SSL 证书和证书链。



笔者认为：目前国际上的根证书信任机制是各个浏览器自己各搞一套，严重加重了各个 CA 机构的根预置工作负担，给新的 CA 机构造成了不公平的市场壁垒。很遗憾的是，目前我国的国密 SSL 证书根认证计划也是走的这条路，各个支持国密算法的国产浏览器也都是各自搞一套自己的根认证计划。所幸的是，多个国产浏览器都默认信任国家根证书，这就给各个 CA 机构省去了向各个浏览器申请根预置的时间和精力，也为各个浏览器省去了处理根预置的事情。所以，建议各个 CA 机构自签自己的国密根证书，生成自己的国密顶级根证书，在自己的顶级根证书下面签发一个或多个专门用于签发 SSL 证书的中级根证书，并向各个国密浏览器申请国密顶级根证书预置信任，这样就实现了用户证书可以走两条信任链，确保自己签发的国密 SSL 证书有更好的通用性，支持更多的国密浏览器。

-----下一讲内容预告-----

第 6 讲 SSL 证书有哪几种？如何正确选择 SSL 证书？

第 5 讲讲到了 SSL 证书有三种，那每一种 SSL 证书到底有什么不同？本讲详细讲解，并给出了笔者的 SSL 证书选用指南。

王高华

2023 年 3 月 6 日于深圳

请关注公司公众号，实时推送公司 CEO 精彩博文。