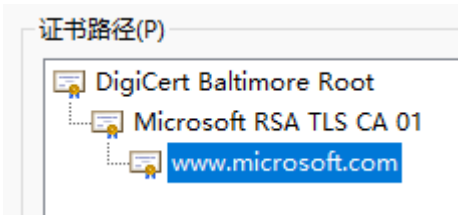
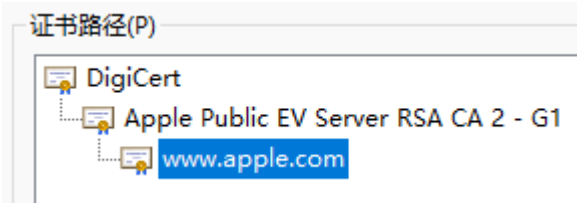
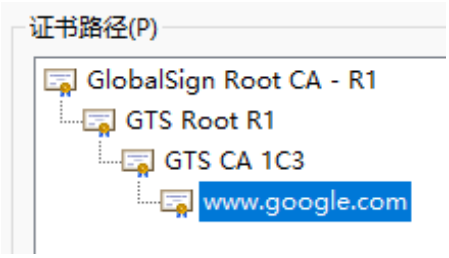
独家披露有关中级根证书的 N 个技术秘密

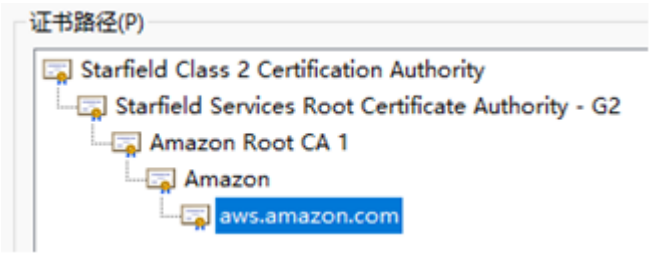
笔者从 2004 年底进入了国际 CA 领域，从此以后就与根证书结下了无解之缘，有些缘分可能现在还不宜披露，今天我就把可以披露的给有兴趣的读者讲一些。

先看看几个互联网巨头的官网部署的 SSL 证书的证书链(证书路径)是什么样的。微软官网的 SSL 证书是由顶级根证书 DigiCert 签发给微软的中级根证书 Microsoft RSA TLS CA 签发，而苹果官网的 SSL 证书是由顶级根证书 DigiCert 签发给苹果的中级根证书 Apple Public EV Server RSA CA 签发，证书链都是 3 级。而谷歌官网的证书链是 4 级的，这是因为谷歌自己有根证书 GTS Root R1，但是由于笔者的电脑中没有这个根证书，所以显示其上一级根证书 GlobalSign Root CA – R1，这是 GlobalSign 根证书给谷歌根证书做了交叉签名。更有意思的是，亚马逊云 AWS 官网的证书链显示为 5 级，而实际上第 1 级、第 2 级和第 3 级证书都是顶级根证书，只是第 1 级根证书给第 2 级根证书做了交叉签名，第 2 级根证书给第 3 级根证书做了交叉签名。所有显示的证书链中用户 SSL 证书的上一级一定是中级根证书，也叫签发根证书(Issuing CA)，专用于签发用户证书。







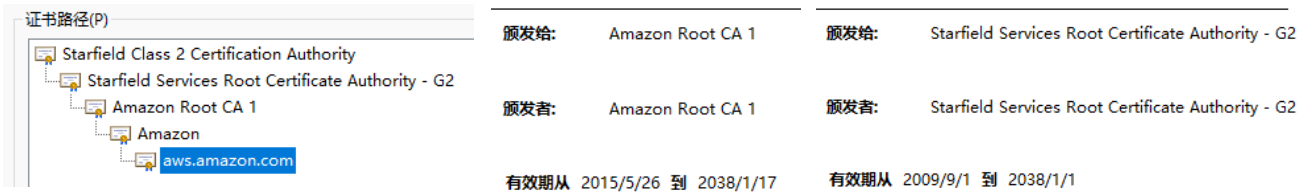


大家再看看证签官网的证书链是 4 级的，如下左图所示，同样道理，Sectigo (AAA) 和 USERTrust RSA CA 都是顶级根证书，但是前者给后者做了交叉签名，就使得用户证书显示为 4 级证书链。而如果大家打开 MMC 的证书管理模块，找到这个交叉签名证书，有时也称之为交叉根证书，把这个交叉根证书禁用，如下中图所示，则证签官网显示的 SSL 证书的证书链就是 3 级了，顶级根证书是 Sectigo，CerSign EV SSL CA 是中级根证书，用于为用户签发 EV SSL

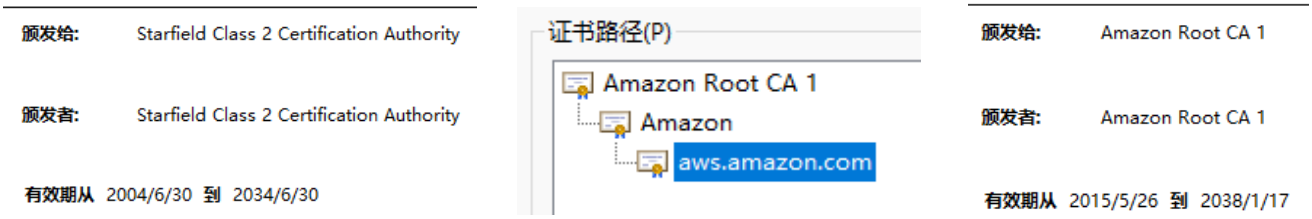
证书。

估计有读者就开始迷惑了，开始有问题要问了。为什么要搞这么复杂？为什么要做中级根证书？为什么又有交叉根证书？不急，笔者一一披露这些技术秘密。

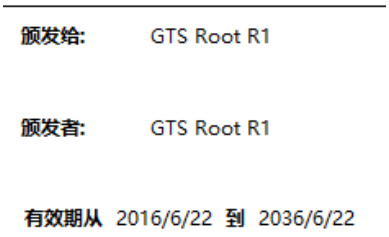
我们可以拿最复杂的亚马逊的 5 级证书链作为案例来解释这些问题。第 1 级顶级根证书 Starfield Class 2 CA 属于 GoDaddy, 从名称就能看出来这个根证书是 GoDaddy 买的。第 2 级根证书 Starfield Services Root CA -G2 则属于亚马逊的，当然也是买的。第 3 级根证书从名字上看就知道是亚马逊自己的，这是一个亚马逊成立自己的 CA 公司 Amazon Trust Services 时生成的自己名称的根证书，这个根证书是 2015 年生成的，如下中图所示，这是一个新的根证书，所以才需要第 2 级的根证书给这个根证书做交叉签名，而第 2 级根证书则是 2009 年生成的。按理说，这个根已经 12 年了，如下右图所示，可以不用再做交叉根证书签名了。

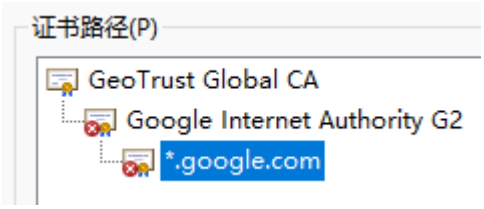


但是，实际上，这个根又被第 1 级根证书交叉签名了，因为第 1 级根证书是 2004 年生成的，如下左图所示，这个根到现在已经有 17 年历史了，应该都已经普遍预置了，估计 17 年前的老设备还在使用也很少了。有意思的是，笔者正准备去 MMC 禁用这些交叉根证书时，发现亚马逊官网的证书链已经变成了如下中图所示的 3 级证书链，这说明 Windows 有自动启用最新的根证书功能。也就是说，既然 Amazon Root CA 1 已经信任(如下右图所示)，就无需再往上验证其他交叉签名根证书了，以加快证书验证速度。也许有些读者的电脑就是直接显示 3 级证书链的。



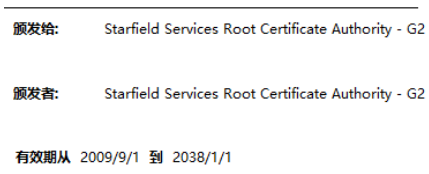
同理，谷歌的根证书是 2016 年 6 月生成的，仍然属于比较新的根证书，如下左图所示，而给谷歌根证书交叉签名的 GlobalSign 根证书是 1998 年的老根证书，如下中图所示。其实谷歌在 2016 年 10 月购买了 GlobalSign 的两个根证书 GlobalSign R2 和 R4，但是由于这两个根都是 2006 年生成的，所以，谷歌仍然选择用 GlobalSign 的 1998 年老根做交叉签名。在此之前，谷歌也是中级根证书模式，由 GeoTrust 根证书签发，这些中级根证书现在都已经过期。





最后再给大家展示一个更有意思的交叉签名解决方案，如下左图所示为第 2 级根证书，这个根证书的签发日期是 2009 年 9 月 1 日。如下中图所示，第 1 级根证书在 2009 年 9 月 2 日给这个当时新生成的根证书做了交叉签名。但是，我们再看如下右图所示，第 1 级根证书给第 2 级根证书签发了一个起始日期为 2009 年 8 月 30 日的交叉根证书。12 年后到今天，我们无法考证第 2 个根密钥生成后到底是 9 月 1 日自签名生成根证书，还是 8 月 30 日先由第 1 个根证书给第 2 个根密钥做了数字签名，生成了右图的交叉签名证书，反正，我们现在看到的是有两个时间的交叉签名证书。

这里有值得我们学习的技术诀窍：如果我们希望优先使用新根证书，则交叉签名证书的签名时间一定要比新根证书签名时间早一点；而如果我们希望优先使用交叉根证书，则交叉签名证书的签名时间一定要比新根证书签名时间要晚一点。这是因为 Windows 的验证机制是优先使用最新日期的根证书作为证书链来验证，而交叉签名一般情况下是先有新根再有老根交叉签名，所以，绝大多数的交叉签名都是交叉签名证书时间会晚些，结果是新根证书在交叉签名证书过期之前一直没有机会使用，这不利于新根的品牌展示和广泛应用。这是今天我要披露的一个最重要的技术秘密，特分享给有需要的读者。



也许有些读者看到这里就更加迷糊了，不要紧，如果作为 SSL 证书用户，这些都可以不用

理解。如果是希望定制中级根证书，这些也可以不懂，因为我们会搞定这些技术问题，本文仅供有兴趣了解一些中级根证书秘密的读者参考。

王高华

2021 年 12 月 9 日于深圳

请关注公司公众号，实时推送公司 CEO 精彩博文。