第 4 讲 什么是 SSL 证书？什么是国密 SSL 证书？

上一讲讲了 PKI 公钥基础设施所签发的最重要的数字证书是 SSL 证书，从本讲开始就重点讲 SSL 证书，分几期讲。本讲将先讲一讲 SSL 证书的用途和全球知名的 SSL 证书提供商有哪些。

大家使用电脑浏览器上网时一定能看到许多网站都会在地址栏显示一个加密锁标识，这表明这个网站部署了 SSL 证书，实现了从浏览器到服务器之间的自动化信息加密传输，这是用密码技术实现了信息的加密保护，同时实现服务器的身份认证。

大家点击加密锁标识能查看 SSL 证书是什么样的，如下左图所示，证书信息中显示“这个证书的目的如下：向远程计算机证明你的身份，保证远程计算机的身份” 第一个目的中的“远程计算机”是指用户端电脑，用户使用浏览器访问网站时，网站的身份由 SSL 证书来证明网站的真实身份。第二个目的中的“远程计算机”指服务器，意思是 SSL 证书能证明 Web 服务器的身份。这两句话有点拗口，其核心意思是 Web 服务器的可信身份由 SSL 证书来证明。大家注意到没有，没有写明加密的目的，可以理解为加密只是附带的功能，证明服务器身份是主要功能，这是数字证书的核心功能，在证明了服务器的可信身份后才用其公钥证书加密对称加密密钥实现信息加密。如右图所示，如果用记事本打开 SSL 证书，则显示的是一堆乱码，一般以-----BEGIN CERTIFICATE-----开始，并以-----END CERTIFICATE-----结束。

-----BEGIN CERTIFICATE-----
MIIEZzCCBA2gAwIBAgIRALmghu6WndRMwZDtrt7qo8owCgYIKoZIzj0EAwIwUDEL
MAkGA1UEBhMCQ04xIjAgBgNVBAoTGVpvVHJ1cyBUZWNobm9sb2d5IExpbW10ZWQx
HTAbBgNVBAMTFFpvVHJ1cyBFQOMgRFYgU1NMIENBMB4XDTIzMDExNjAwMDAwMFoX
DTI0MDExNjIzNTk1OVowGTEXMBUGA1UEAxMOd3d3LnpvdHJ1cy5jb20wWTATBgcq
hkjOPQIBBggqhkjOPQMBBwNCAATDQ7xL5XXELBpA8eqkR4yynpeZOpn9xwnj1u0E
MnzIRT9F4xIjdZ1KKhzy/OnwUQLMHkOwJB6Q4Uu0hZXFs0GLo4IC/TCCAvkwHwYD
VR0jBBgwFoAUesjDkz1jTaJdrGO7uJn/Ba8fH1IwHQYDVR0OBBYEFNh0ENCJBSwK
1beGZ25nNBZ0XkU3MA4GA1UdDwEB/wQEAwIHgDAMBgNVHRMBAf8EAjAAMB0GA1Ud
JQQWMBQGCCsGAQUFBwMBBggrBgEFBQcDAjBJBgNVHSAEQjBAMDQGCysGAQQBsjEB
AgJbMCUwIwYIKwYBBQUHAgEWF2h0dHBzOi8vc2VjdG1nby5jb20vQ1BTMAgGBmeB
DAECATB2BggrBgEFBQcBAQRqMGgwPAYIKwYBBQUHMAKGMGh0dHA6Ly9jcnQuc2Vj
dG1nb2NoaW5hLmNvbS9ab1RydXNFQ0NEV1NTTENBLmNydDAoBggrBgEFBQcwAYYc
aHR0cDovL29jc3Auc2VjdG1nb2NoaW5hLmNvbTCCAX8GCisGAQQB1nkCBAIEggFv
BIIBawFpAHcAdv+IPwq2+5VRwmHM9Ye6NLSkzbsp3GhCCp/mZ0xaOnQAAAGFuGvP
eQAABAMASDBGAiEAxAaqhR+CMNgQDKLFieTse6ZoZZG9p9d+L1gwjk1dAIkCIQDX
3uTkJUvT9h4UoabJ9T/ou/Li/JGoksBQ+ozV/QnDsAB1ANq2v2s/tbYin5vCu1xr
6HCRcWy7UYSFNL2kPTBI1/urAAABhbhrz1UAAAQDAEYwRAIgCf4bdGo1Dv0MXK2O
pRdy8pz8X4T8+hiR/wVdftORir0CIG1Qm6bkhohTKd6rO+q2LH057UTfAujdy8Nu
3pmCQ81vAHcA7s3QZNXbGs7FXLedtM0TojKHRny87N7DUUhZRnEftZsAAAGFuGvP
IgAABAMASDBGAiEAgTdzz9oN+0dnadXPvRUFmZw21Rc0mwrCy5Bx0LEKaxoCIQCO
kRv/WY+veZ3qnj+XPgSena4IORILWYMbEoNoyUT46TA0BgNVHREELTArgg53d3cu
em90cnVzLmNvbYINbXkuem90cnVzLmNvbYIKem90cnVzLmNvbTAKBggqhkjOPQQD
AgNIADBFAiAB7Oj1OB+4jF77GhsK1yLNYT1Mgnr+MkCI0SWD/XmehgIhAJEuH52o
Rmj9p1XTeBIUoKehivGnwIdR4Z1bQO5WFPUR
-----END CERTIFICATE-----

SSL 证书中最核心的部分当然是密码算法，所以用户会关心这张 SSL 证书采用的何种密码

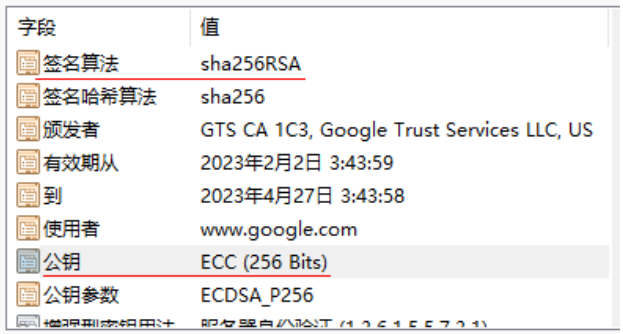
(C) 2023 零信技术（深圳）有限公司

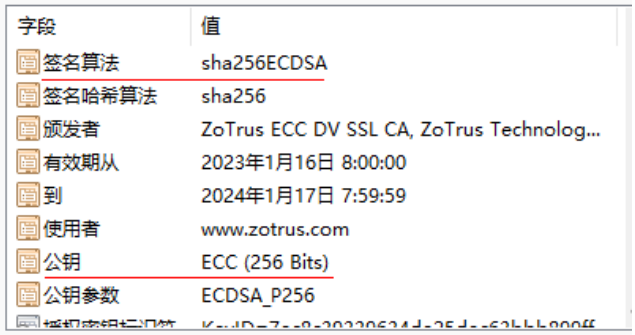
算法签发的，也就是说 PKI 系统是采用何种密码算法数字签名公钥的。目前，国际上认可的算法是 RSA 算法和 ECC 算法，用这两种算法签发的 SSL 证书称之为国际 SSL 证书，或 RSA SSL 证书，或 ECC SSL 证书。这种叫法的目的是为了区分采用国密算法 SM2 签发的 SSL 证书，我们称之为国密 SSL 证书，或 SM2 SSL 证书，又可称为商用密码 SSL 证书，或商密 SSL 证书。使用零信浏览器访问网站时点击加密锁标识会看到“连接已加密(RSA)”或(ECC)或(SM2)，这就是明确告诉用户目前正在使用何种密码算法实现 https 加密。

目前，国际标准要求 RSA 算法的 SSL 证书密钥长度必须至少 2048 位，而 ECC 算法的 SSL 证书至少是 256 位，国密标准要求的国密 SM2 算法 SSL 证书也是 256 位，大家从密钥位数的长度就应该能理解 ECC 算法和 SM2 算法密钥短，加解密速度更快，能节省算力、带宽和电力。所以，现在许多大流量网站都部署了 ECC 算法 SSL 证书，这也是国密算法 SM2 SSL 证书的技术优势，因为都是采用 256 位的椭圆曲线算法，只是国密 SM2 算法的曲线参数是我国自己计算出来的不同。根据证书透明日志数据统计，目前全球有效的 SSL 证书中采用 RSA 算法的 SSL 证书占比 90%，ECC 算法的 SSL 证书占比 10%，相信随着各大云服务商纷纷自动化为用户配置 ECC 算法 SSL 证书，其比例一定会不断上升。

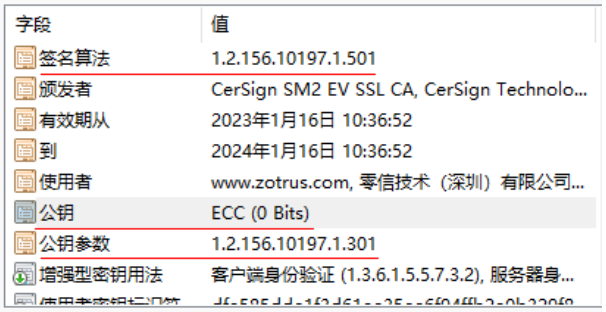
如下左图所示，谷歌搜索部署的就是 ECC SSL 证书，大家再看看此证书的签名算法是 RSA，这说明签发此张 SSL 证书中级根证书是 RSA 算法证书，这是一张顶级根证书和中级根证书都是 RSA 算法，只有用户证书是 ECC 算法，也就是说证书信任链采用 RSA 算法签名，而实际 https 加密采用 ECC 算法实现，这当然也是符合国际标准的，是因为谷歌没有 ECC 算法的顶级根证书的不得已的做法。我们再看看右下图，签名算法是 ECDSA，用户证书公钥是 ECC，这说明签发此张 SSL 证书的中级根证书是 ECC 算法证书，这是一张顶级根证书、中级根证书和用户证书都采用 ECC 算法的 SSL 证书，整个证书链文件更小，https 协议握手效率更高，更节省流量和带宽。

(C) 2023 零信技术（深圳）有限公司





当然，国密 SSL 证书的全证书链都是采用国密 SM2 算法，如下左图所示为零信浏览器查看国密 SSL 证书的证书信息，签名算法是国密 SM3_SM2。而用 Windows 证书查看器查看，则显示签名算法为 OID：1.2.156.10197.1.501，这是因为 Windows 目前还不能正常识别和显示 SM2 SSL 证书的签名算法，所以下面的公钥参数也是显示为 OID：1.2.156.10197.1.301，能识别出这张证书采用的是椭圆曲线算法，但是由于无法识别出是 SM2 算法的曲线，所以显示为 ECC(0 Bits)。大家在不支持 SM2 算法的系统中查看证书时只要看到这两个 OID，那就是 SM2 算法证书，只是系统没有正常翻译显示出来而已。



SSL 证书的第二个重要信息是这张证书是哪个 CA 签发的，顶级根证书是哪一家 CA 的，了解这些信息也很重要。在常规的下面就显示了这张 SSL 证书是颁发给哪个域名的，颁发者是谁，证书有效期等信息，如下左图所示，目前常见的证书有效期为一年或者 90 天。点击“证书路径”选项卡，则会显示此证书的完整证书链，第一行就是顶级根证书，表示这张证书的最终信任源来自哪家 CA 机构。第二行是中级根证书，一般代表这张证书的品牌，第三行是用户证书绑定的网站域名。同时，我们从下面这两张图就能看出这张 SSL 证书的顶级根证书、中级根证书和用户证书都是 ECC 算法证书。

(C) 2023 零信技术（深圳）有限公司

目前，市场上统计某个品牌的 SSL 证书提供商的市场份额或签发量，都是以中级根证书为品牌来统计的。让我们来看看截止到 2023 年 1 月 1 日的数据，全球市场排名前十位的公司及分别签发了多少张有效证书，依次是 Let's Encrypt (4.4584 亿张)、Cloudflare (8641 万张)、DigiCert (4459 万张)、谷歌 (4361 万张)、Sectigo (4347 万张)、亚马逊 (3896 万张)、cPanel (3047 万张)、微软 (2170 万张)、ZeroSSL (1685 万张)、GoDaddy (1021 万张)。

大家看到这个统计数据，也许就能理解为何笔者一直称签发 SSL 证书的公司为"SSL 证书提供商"而不是 CA 机构，因为前十大签发 SSL 证书的公司中，真正的 CA 机构只有两家：DigiCert 和 Sectigo，分别排名第 3 和第 5 位，其他 8 家都是互联网公司或云服务提供商，虽然排名第一位的 Let's Encrypt 在官网称其为一家提供 TLS 证书的非盈利 CA，但笔者把这家公司归类到互联网公司一类。排名第二位的 Cloudflare 是一家互联网云服务提供商，第三位是谷歌，互联网巨头和云服务提供商。第 6 位亚马逊是云服务提供商，第 7 位 cPanel 是互联网公司，第 8 位是微软，软件巨头、互联网巨头和云服务提供商。第 9 位是一个 SSL 证书代理商，属于互联网公司。第 10 位是 GoDaddy，一个老资格的域名注册商和互联网服务提供商。笔者分析这些公司的类型的目的是让大家充分了解 SSL 证书的大玩家是谁，这有利于帮助国内互联网公司和云服务提供商能从中看到商机，一定要自己签发自己品牌的 SSL 证书实现自动化为业务系统配置 SSL 证书，提升云服务的核心竞争力，因为用户需要的不是 SSL 证书，而是 https 加密。

-----下一讲内容预告-----

第 5 讲 什么是顶级根证书？什么是浏览器信任根认证计划？

本讲先接着第 4 讲没有讲的 SSL 证书的证书链、顶级根证书、中级根证书以及 SSL 证书的信任机制，再简单介绍一下目前各大浏览器的信任根认证计划，有利于读者了解 PKI 体系是如何解决网络信任问题的。

王高华

2023 年 3 月 1 日于深圳

(C) 2023 零信技术（深圳）有限公司

请关注公司公众号，实时推送公司 CEO 精彩博文。

(C) 2023 零信技术（深圳）有限公司