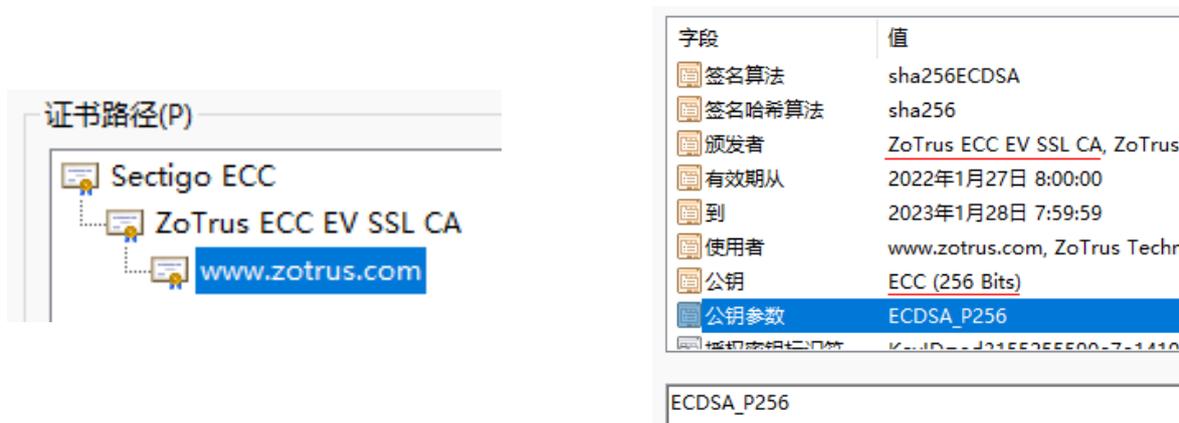


SSL 证书链采用 ECC 算法有何特别优势？

什么是 ECC 算法，什么是 ECC SSL 证书？还是让大家直观地看看零信官网部署的 SSL 证书吧，大家点击安全锁标识就能查看证书链，如下左图所示，顶级根证书是 Sectigo ECC 根，采用 ECC 算法(384 位)；中级根证书是 ZoTrus ECC EV SSL CA，就是我们自己的中级根证书，也是采用 ECC 算法(256 位)；而用户证书也是采用 ECC 算法(256 位)，如下右图所示，这就是一个全链都是采用 ECC 算法的实际 SSL 证书部署案例。



什么是 ECC 算法？这是一种采用椭圆曲线的密码算法，我国商用密码 SM2 也是一种采用椭圆曲线的密码算法，只是采用了不同的曲线实现密码算法。

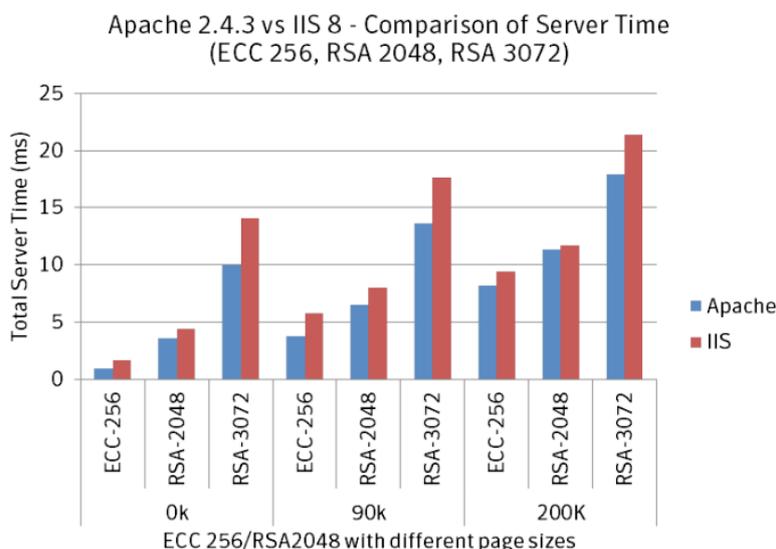
大家都知道，为了保证 RSA 算法的密钥安全，密钥长度一直在不断增加，从 512 位增加到 1024 位，现在的用户证书必须是 2048 位，中级根证书则是 3072 位，顶级根证书则必须是 4096 位了，位数越来越长，对服务器 CPU 和内存及网络带宽的要求也就越来越高，这就是为何大家的电脑硬件需要不断的升级的原因之一。这对于当下移动互联网普及的时代，对手机终端的要求更是一个大问题，为了实现 RSA SSL 证书的 https 加密需要消耗不少 CPU 和内存，当然也就需要消耗不少电量，大家手机的电量上网时间太长的话，耗电非常快，电池一下子就没电了，这是原因之一，因为所有常用的网站都已经部署了采用 RSA 算法的 SSL 证书。

而采用 ECC 算法的 SSL 证书要求的是 256 位，密钥长度只有 RSA 的 2048 位的八分之一，如下左图所示，网站部署绑定一个域名的 RSA SSL 证书时，浏览器需要下载中级根证书和用户证书的大小为 4.24K(电脑显示为 3K+3K)。如下右图所示，网站部署绑定一个域名的 ECC SSL 证书时，浏览器需要下载中级根证书和用户证书的大小为 2.74K(电脑显示为 2K+2K)，也就是说，采用 ECC SSL 证书实现每次 SSL 证书的握手能节省 1.5K 带宽，对于一个日访问量

高达 1000 万次的网站，是可以节省不少带宽费用的。如：目前阿里云用的 SSL 证书绑定了 218 个域名，加上中级根证书合计文件大小为 9.93K，比 ECC SSL 单域证书大 7.19K，按日访问量 1000 万次计算，大概一年要多花 20 万元带宽费用。

名称	大小	类型	名称	大小	类型
Sectigo RSA.crt	3 KB	安全证书	Sectigo ECC.crt	1 KB	安全证书
CerSignDVSSLCA.crt	3 KB	安全证书	ZoTrusECCDVSSLCA.crt	2 KB	安全证书
RSASSL-www-cersign-com.crt	3 KB	安全证书	ECCSSL-www-zotruse-com.crt	2 KB	安全证书

节省带宽费用可能对互联网巨头是小事，但是，让我们再看看赛门铁克(Symantec)做的专题研究，如下图所示，Apache 服务器部署 256 位的 ECC SSL 证书和部署同等加密强度的 3072 位 RSA SSL 证书，Web 服务器对 ECC 算法的响应速度是 RSA 的 18 倍！也就是说，用户访问一个部署了 ECC SSL 证书的网站只需要 1 秒，而访问一个部署了 RSA SSL 证书的网站需要 18 秒！这个数据对于需要追求极致用户体验的互联网巨头们应该是一个比较震撼的数据吧，实验用的 Apache 和 IIS 服务器软件，现在流行用 Nginx 服务器软件，估计性能差距更大。



ECC 算法由于密钥更短，不仅能改进用户体验，还能降低用户手机的 CPU 能耗和流量，并且能降低网站服务器的 CPU 和内存资源，还能节省带宽费用，并且还能全面支持完美全向加密(PFS)，具有更好的抗攻击能力。正因为 ECC 算法有这么多优秀特点，各大互联网巨头如内容分发服务巨头 CloudFlare 官网和其用户都是部署 ECC SSL 证书，如下左图所示；谷歌官网和油管(YouTube)等网站也都是部署 ECC SSL 证书，如下右图所示。

字段	值
签名算法	sha256ECDSA
签名哈希算法	sha256
颁发者	Cloudflare Inc ECC CA-3, Cloudflare, Inc., US
有效期从	2021年9月18日 8:00:00
到	2022年9月18日 7:59:59
使用者	www.cloudflare.com, Cloudflare, Inc., San Fra...
公钥	ECC (256 Bits)
公钥参数	ECDSA_P256
增强型密钥用法	KeyID=5a37...bb0750-046700b4456-d02

字段	值
签名算法	sha256RSA
签名哈希算法	sha256
颁发者	GTS CA 1C3, Google Trust Services LLC, US
有效期从	2021年12月27日 16:11:32
到	2022年3月21日 16:11:31
使用者	www.google.com
公钥	ECC (256 Bits)
公钥参数	ECDSA_P256
增强型密钥用法	服务器身份验证 (1.3.6.1.5.5.7.3.1)

这些大流量的网站都已经部署使用了 ECC SSL 证书，这应该能打消有些用户对 ECC 算法是否得到广泛的系统和设备支持的怀疑。简单地说吧，只有早就不再使用的操作系统 Windows XP 和 iPhone 4 才不支持 ECC 算法，其他所有系统和设备都支持。

正是由于 ECC SSL 证书性能优越，笔者才向大家极力推荐网站部署 ECC SSL 证书，定制的 SSL 中级根证书也采用 ECC 算法。大家也已经看到上面展示了零信官网的是三级证书链都是采用 ECC 算法，我们的 ECC SSL 中级根证书由 Sectigo ECC 顶级根证书定制签发。

Sectigo 是全球唯一一家拥有两个最老的 ECC 算法顶级根证书的 CA，一个是 2008 年的，一个是 2010 年的，我们选择从 2010 年的顶级根证书定制 ECC 中级根证书，是因为不太喜欢用 Comodo 的老品牌，因为 2010 年的根证书已经有 12 年，已经够老了，如果还有更老的设备不信任这个根证书的话，Sectigo 也提供了一个更老的 2004 年的根证书 AAA Certificate Services 的交叉签名证书。

颁发给: COMODO ECC Certification Authority	颁发给: USERTrust ECC Certification Authority	证书路径(P) Sectigo (AAA) USERTrust ECC Certification Authority 颁发者: AAA Certificate Services 有效期从 2004/1/1 到 2029/1/1
颁发者: COMODO ECC Certification Authority	颁发者: USERTrust ECC Certification Authority	
有效期从 2008/3/6 到 2038/1/19	有效期从 2010/2/1 到 2038/1/19	

总之，为了提升网站访问用户的浏览体验，为了降低网站服务器的 CPU、内存和带宽的消耗，为了节能环保省电，强烈推荐定制 ECC 算法 SSL 中级根证书用于为用户签发 ECC SSL 证书，因为 ECC SSL 证书一定会成为首选 SSL 证书，特别是大流量的网站。笔者很高兴地看到阿里云 WAF 支持 ECC SSL 证书，使得零信官网能成功部署 ECC SSL 证书。

王高华

2022 年 3 月 3 日于深圳

请关注公司公众号，实时推送公司 CEO 精彩博文。

