密码讲堂 | 第 13 讲 SSL 证书及相关国际标准

本计划在第 13 讲开始讲加密 DNS，但是笔者最近看到一个非常重要的单位的内网部署使用的 SSL 证书有非常多的安全问题，零信浏览器无法正常访问这个内网系统，这个用户就说是零信浏览器的问题，因为某个浏览器可以正常访问。笔者发现这不是个个案，因为这个内网是一个覆盖全国的系统，所以笔者决定再多讲几讲 SSL 证书，可以理解为 SSL 证书进阶知识，供有兴趣进阶了解 SSL 证书的读者学习。本讲先讲一讲 SSL 证书相关的国际标准。

还是先让大家了解一下这个有 N 个安全问题的 SSL 证书有哪些问题，以便同时对比了解国际标准是怎么要求的：

(1) 这张 SSL 证书的公钥为 RSA 算法 1024 位，非常不安全！

国际标准要求 2010 年 12 月 31 日停止签发 1024 位证书，并于 2013 年 12 月 31 日禁用 1024 位证书，国家密码管理部门也已发类似通知要求，但是居然这么重要的内网系统在国际标准要求禁用 1024 位证书的十年后的今天还在使用 1024 位 RSA 算法 SSL 证书！

(2) 这张 SSL 证书的签名算法为 SHA1，非常不安全！

国际标准要求在 2015 年 12 月 31 日停止签发 SHA1 证书，从 2017 年 1 月 1 日起 Windows 停止支持 SHA1 证书，但是 7 年后的今天这个重要的系统还在使用 RSA 算法 SHA1 证书！

(3) 这张 SSL 证书没有使用者可选名称(SAN)字段！

只有 CN 字段=10.xx.xx.xx 的 IP 地址，这是一个大问题，因为浏览器验证 SSL 证书绑定的域名或 IP 地址是只读取 SAN 字段信息的，没有这个字段就无法判断证书绑定的 IP 地址是否同用户正在访问的网站 IP 地址一致，当然会有“不安全”警告。

(4) 这张 SSL 证书没有“服务器身份验证和客户端身份验证”的增强密钥用法(EKU)！

没有增强密钥用法等于就是没有定义这种证书是 SSL 证书，当然也就无法实现双向认证。

(5) 这张 SSL 证书没有必须有的(Critical)“密钥用法”！

没有密钥用法，就甚至不能称之为证书，这是一个非常严重的问题。

(6) 这张 SSL 证书没有可访问的吊销列表和授权信息访问(AIA)网址，反正是内网无法访问外网，这还可以接受。但不了解服务器部署 SSL 证书是否同时部署了中级根证书，如果没有，则无法验证证书。

(7) 这张 SSL 证书没有证书策略字段，更没有证书透明 SCT 列表。

(8) 这张 SSL 证书在内网使用，绑定的是内网 IP 地址 10.xx.xx.xx，这个不是大问题，但是这张 SSL 证书都已经过期一年多了还在使用，这是个大问题。

相信大家已经从上面的各种问题能看出这张 SSL 证书依据国际标准是根本不允许使用的，正常功能的浏览器也是无法正常同服务器握手成功的。据了解，这张 SSL 证书居然是某个国内知名的“技术领先”的厂商的 CA 系统签发的，一个 CA 系统厂商是生产签发 SSL 证书的系统的，不懂 SSL 证书的话如何能生产出合格的 CA 系统？这更加让笔者深感普及 SSL 证书知识的重要性。其实，大家如果有心的话，随便打开一个正常网站，查看一下 SSL 证书的参数就能知道正常的 SSL 证书应该有哪些字段，本文就以零信官网部署的国际 SSL 证书为例，重点讲一讲几个重要的字段。

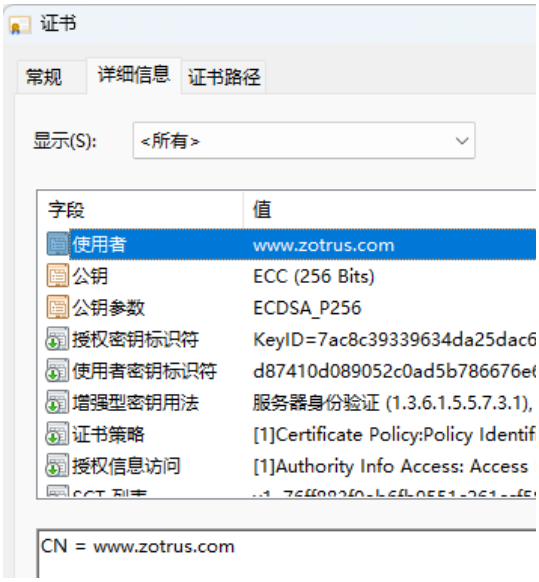
1. **使用者**(Common Name, CN) 和 **使用者可选名称(**Subject Alternative Name, SAN)

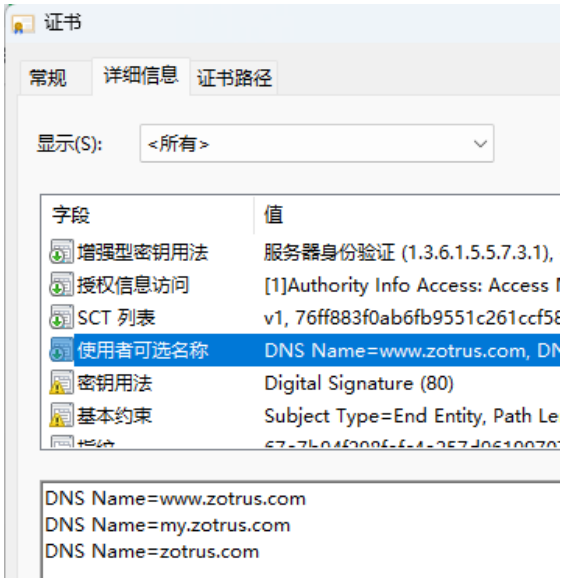
“**使用者**”是 Windows 证书查看器新启用的名称，原先名称是“通用名称”，就是 Common Name 的直译，只能包含一个域名，一个单域或一个通配域名，这个字段是 X.509 证书标准中

标准字段，在 Netscape 发明 SSL 证书时被用于绑定网站的域名，在邮件证书中用于绑定电子邮件地址，在客户端身份证书中用于绑定个人姓名或单位名称，在代码签名证书和文档签名证书中用于绑定单位名称。

但是，随着 SSL 证书的普及应用，一张证书绑定一个域名无法满足用户的应用需求，所以 X.509 规范就增加了一个扩展项：Subject Alternative Name(SAN)，主题备用名称 或 **使用者可选名称**，这个扩展字段可以是域名、电子邮件地址、IP 地址、网址等信息，允许写入多条数据，这就有了多域证书。2000 年 5 月发布的国际标准 RFC 2818 指定主题备用名称作为将域名添加到 SSL 证书的首选方法，弃用以前将域名添加到通用名称字段的方法。

CA/浏览器论坛制定的基线标准要求 SAN 中必须包含通用名称中的域名或 IP 地址，从而有效地使 SAN 成为与网站域名相匹配的唯一必需验证依据，通用名称字段已经被弃用，但允许 CA 签发含有通用名称的 SSL 证书，仅作为过去的技术遗产而存在。谷歌浏览器从 58 版本(2017 年 3 月)开始就根本不再检查通用名称字段的信息，只查看和验证 SAN 字段，这实际上是加快了浏览器验证 SSL 证书时间，提升了用户体验。





也就是说：SSL 证书标准要求必须有 SAN 字段，必须把网站域名写入到这个字段，这个字段可以写入多个域名和 IP 地址，但一般不会超过 100 个，绑定太多的域名也不是很好的选

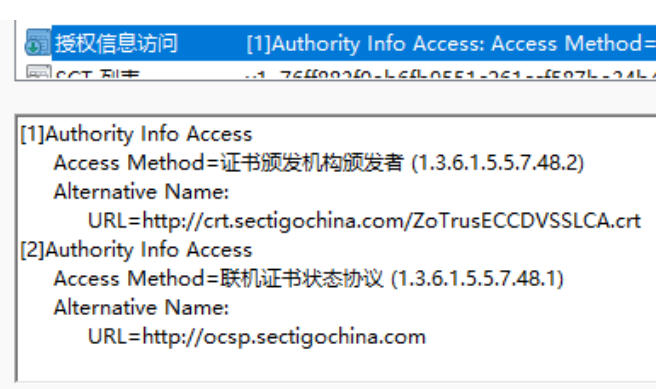
择，因为太多域名会导致 SSL 证书文件变大，这就会增加浏览器同服务器握手时的流量，不仅浪费了流量，而且影响浏览器的 SSL 证书验证效率，降低了用户体验。

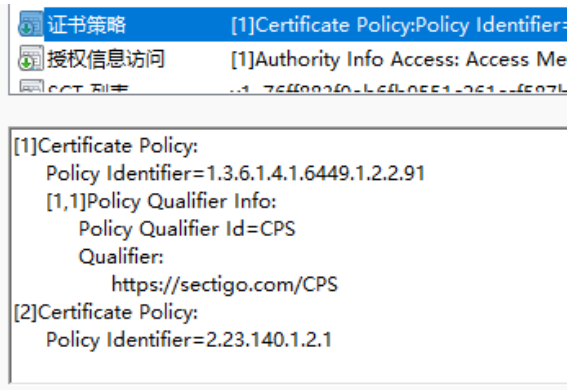
2. **授权信息访问**(Authority Info Access, AIA) 和 **证书策略**(Certificate Policy, CP)

授权信息访问(Authority Info Access)，简称为 AIA，意思是证书签发者信息访问网址，用于告诉浏览器这张证书是哪个签发 CA 签发的，去哪里可以下载签发者证书用于验证用户证书是否真的是这个签发 CA 签发的，这个信息必须包含在用户证书中，以便浏览器能获得证书签发者的证书来验证用户证书。

零信浏览器在处理各家 CA 机构的可信根认证申请时发现有多家 CA 签发的用户证书和签发 CA 都没有 AIA 信息，这样即使预置信任了根证书也由于无法往上验证而使得浏览器无法显示为可信证书。有些用户证书中有 AIA 信息，但是无法访问，这就等于没有，所以这个字段必须有，并且一定要确保 AIA 网址可访问，而且必须是正确的签发 CA 证书。

也就是说，这个字段影响了浏览器是否可以正常识别和验证网站部署的 SSL 证书，当然非常重要。这个字段中还有一个联机证书状态协议信息，这个留到下面同 CRL 字段一起讲。





证书策略(Certificate Policy)这也是必须有的字段，明确用户这张证书的签发依据的 CPS(认证业务声明)的访问网址，用户可以直接点击证书常规中显示的“颁发者说明”直接访问这个网

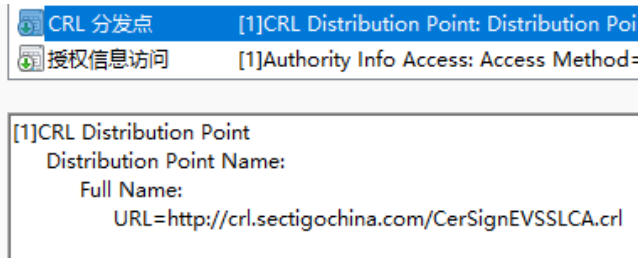
址。同时还会显示 Policy Identifier(OID)，一般至少有两个 OID，一个是定义此证书类型的 CA 自用 OID，另一个是此证书遵循的国际标准证书类型的 OID，如下图中的 2.23.140.12.1 就是 CA/浏览器论坛定义的 DV SSL 证书 OID。

可以毫不夸张地讲，没有证书策略这个字段就是不可信的证书，因为签发者没有公开告知用户是依据什么标准来签发这张证书的、是如何验证用户身份的等等。这是一个必须有的字段。

3. **证书吊销列表**(Certificate Revocation List, CRL) 和 **联机证书状态协议**(Online Certificate Status Protocol, OCSP)

如果 CA 机构错误签发了证书，则必须马上吊销这张证书，或者用户怀疑网站部署的 SSL 证书私钥泄露，则用户也应该马上通知 CA 机构吊销这张证书。而证书吊销后如何告知浏览器此证书已经吊销，这就是**证书吊销列表**(CRL)，证书中的“**CRL 分发点”**字段就是告诉浏览器和其他方这张证书的吊销列表访问网址，浏览器可以下载吊销列表文件(.crl)来验证此证书是否在吊销列表中。请注意：如果这个签发根有很多张证书被吊销的话，这个吊销列表文件会很大，一个有 324 条吊销记录的文件大小为 12K，所以，目前谷歌的 CRL 的发布方式是每 7 天启用一个新的吊销列表文件，零信 CA 系统是每年启用一个新的吊销列表文件，而不是传统的使用一个一直不变的吊销列表文件。

大家应该可以看出：使用吊销列表文件的不好之处就是可能文件会很大，这样浏览器下载这个吊销文件并验证用户证书的时间会变长，这会影响用户体验。当然，吊销列表文件是定期发布的，国际标准要求至少每 7 天必须发布一次，有效期最多不能超过 10 天，也就是说在吊销列表文件未到期之前是不用重复下载的。而为了能及时发布已吊销的证书，国际标准要求 SSL 证书被吊销后必须在 24 小时内发布包含了此吊销证书序列号的新的吊销列表。



联机证书状态协议(OCSP)是一个能实时查询证书是否被吊销的计划替代 CRL 的协议，意在解决 CRL 文件可能很大(必须下载整个 CRL 文件才能查询到某种证书是否被吊销)，以及吊销列表发布不及时等问题，其优点是无需下载整个 CRL 文件，只需把要查询的证书的序列号给 OCSP 查询是否已吊销而返回一个“是”或“否”即可，这的确是一个高效率的解决方案。

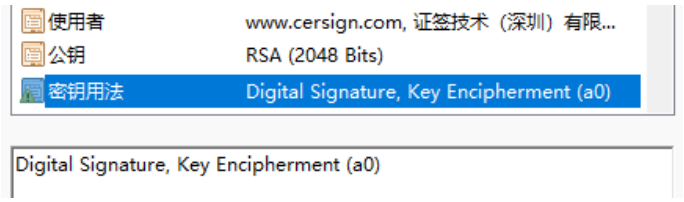
但是，现在国际标准又计划废弃 OCSP，原因是随着所有常用网站都已经实现了 https 加密，用户浏览器不断地访问地 OCSP 系统泄露了用户的访问轨迹，这不利于保护用户隐私。所以，CA/浏览器论坛计划修改标准把目前的“OCSP 必须和 CRL 可选”改为“CRL 必须 OCSP 可选”，并有专家提议把在证书透明机制中增加证书吊销查询功能。无论怎么变，证书吊销查询服务是 CA 机构必须提供的，可以只有 CRL 或者只有 OCSP，必须有一个或者两个全有，这样浏览器就可以验证这张证书是否被吊销，从而能及时停止使用已吊销的证书。

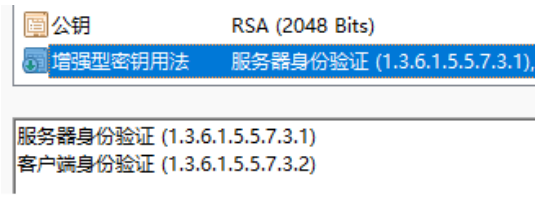
4. **密钥用法**(Key Usage, KU) 和 **增强密钥用法**(Extended Key Usage, EKU)

密钥用法是SSL证书必须有的关键字段，顾名思义这个字段用于说明这张证书是干什么用的。RSA算法SSL证书应该是“Digital Signature, Key Encipherment (数字签名，加密)”，而ECC算法SSL证书则是“Digital Signature (数字签名)”，这两种算法在https加密中的作用是不一样的。

增强密钥用法则不是关键字段，但是必须有的字段，这个字段进一步说明这张证书的用途，SSL证书的EKU字段值为“服务器身份验证 (1.3.6.1.5.5.7.3.1)，客户端身份验证

(1.3.6.1.5.5.7.3.2)”，意思是这张SSL证书既用于服务器的身份认证，也可以用于同其他服务器通信时的一个客户端的身份认证，一般用于服务器与服务器之间的加密通信。SSL证书至少必须有“服务器身份验证”这个EKU，用于“向远程计算机证明服务器的身份”，没有这一项就无法实现同客户端证书的双向认证。



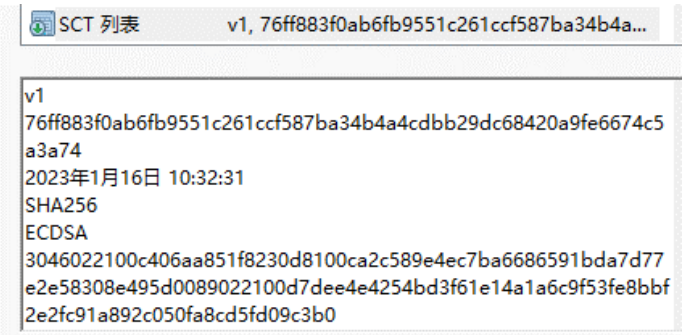


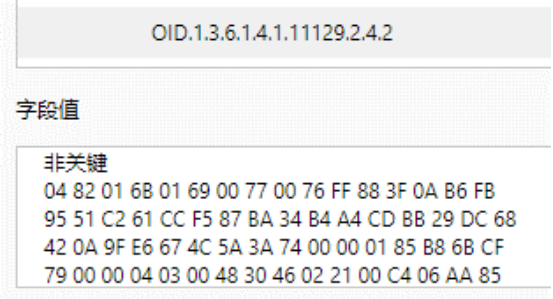
5. **证书透明日志签名数据列表**(SCT List)

这个字段是判断 SSL 证书是否可信的两个要素之一，因为一个 CA 机构如果不敢把自己签发的 SSL 证书公示的话，谁都能想象出这个 CA 可能想干什么。这就是为何自 2013 年以来已经有 97 亿多张全球信任的 SSL 证书都已经在证书透明日志系统透明备案公示，一个负责任的公共信任的 CA 是愿意公示其证书签发行为的，是愿意接受公众监督。而如果有 CA 机构不提交 CT 系统公示，怎么办？如果 SSL 证书中没有 SCT 列表字段，则谷歌浏览器直接不信任，如果有，则必须满足几个条件：(1) CT 日志服务必须是通过谷歌认证并预置谷歌浏览器中信任(包括 Chromium)；(2) 证书有效期小于 180 天必须包含 2 个 SCT 数据，大于 180 天必须包含 3 个。否则，谷歌浏览器一样不信任，提示“不安全”。

如下左图为 Windows 证书查看器看到的 SCT 列表字段信息，已经解析了 SCT 数据，第 1 行是证书透明版本号，目前全球各大 CA 和浏览器都在使用 V1 版本；第 2 行是证书透明日志服务器 ID，第 3 行是证书透明日志系统的签名时间，第 4 行则是日志数据的签名算法(SHA256/ECDSA)，第 5 行就是证书透明日志的签名数据。这些数据用于浏览器验证这张 SSL

证书是在哪个证书透明日志系统备案的、是何时备案的、证书透明日志系统是否是浏览器信任的等等，只有通过验证，浏览器才会正常显示加密锁标识。大家再看看右图，这是目前谷歌浏览器展示的 SCT 列表字段信息，根本就没有解析这个字段，这也是不可思议的事情，也许是谷歌急于推出自己的证书查看器还来不及解析这个字段，希望将来的版本能正常展示证书透明日志信息。





按照谷歌证书透明政策，对于非公共信任的企业 CA，则可以没有 SCT 列表字段。当然，为了保障企业 CA 签发的 SSL 证书安全，也可以部署企业 CT 系统为 SSL 证书提供证书透明服务，但谷歌浏览器不查验企业 CT 中的 SCT 列表数据。

以上讲清楚了 SSL 证书中最关键的 9 个字段，这些字段遵循由国际标准组织-CA/浏览器论坛制定的国际标准，包括：SSL 证书基线标准、EV SSL 证书标准和 CA 系统网络安全要求，另外还有两个 RFC 国际标准，包括：证书透明(RFC6962)和自动化证书管理标准(RFC8555)，SSL 证书中 SCT 列表字段遵循的就是 RFC6962 标准，本文并没有讲到 RFC8555 标准，因为本文仅讲解 SSL 证书的各个字段的含义和要求，并不涉及到 SSL 证书的自动化申请和部署，这个知识点已经在密码讲堂第八讲讲过，大家可以查看第八讲的内容。

SSL 证书由 Netscape 于 1994 年发明到现在已经将近三十年了，SSL 证书相关标准也一直

在不断完善中，目前 SSL 证书相关标准有两条线，一条线属于基础类标准，一般都会形成 RFC 标准，与 SSL 证书相关的 RFC 标准有：RFC2818、9110、5785、7230、6962、9162、8555 等等。另一类是应用类标准，这些标准则是由 CA/浏览器论坛来负责制定，并据此形成 WebTrust 审计标准，审计机构依据 WebTrust 审计标准来审计 CA 机构是否遵循这些标准来运营 CA 系统签发各种全球信任的数字证书。我国 CA 机构或企业自建 CA 系统，如果需要签发 RSA/ECC 算法 SSL 证书，当然应该参考和遵循这些标准，无论是否预置浏览器信任，遵循这些标准是为了保证 SSL 证书的安全，从而保障采用 SSL 证书实现的 https 加密流量安全。

下一讲内容预告 | 第 14 讲 国密 SSL 证书及相关国密标准

本讲详细讲解国密 SSL 证书中对照国际 SSL 证书标准必须有的最重要的 9 个字段的含义和作用，这些字段都是国密 SSL 证书必须有的而且不能错的字段。本文可供国密 SSL 证书使用者、CA 机构和 CA 系统提供商学习参考。

王高华

2023 年 6 月 25 日于深圳

请关注公司公众号，实时推送公司 CEO 精彩博文。