密码讲堂 | 第 14 讲 国密 SSL 证书及相关国密标准

笔者在第 13 讲了 SSL 证书中最重要的 9 个字段及相关国际标准，本讲就对应地讲一讲国密 SSL 证书中最重要的 9 个字段及相关的已有的和正在制定中的国密标准。

大家从上一讲可以看出，国际算法 SSL 证书在发展过程中不断完善密码算法，用户之所以出现文章开头所讲的一堆 SSL 证书安全问题，这是历史原因造成的。而国密 SSL 证书起步晚，现在还处于起步阶段，所以没有这些历史包袱，没有这些安全问题，这是幸事。但是，零信浏览器在预置各家 CA 的国密根证书时还是发现了不少问题，所以本讲还是值得一讲的，有助于提升国密 SSL 证书的安全水平，有助于安全的使用商用密码来实现 https 加密，有助于普及国密 https 加密来保障我国网站系统安全。本文就以零信官网部署的国密 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。

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。

参考国际标准，国密 SSL 证书也必须有 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

(C) 2023 零信技术（深圳）有限公司

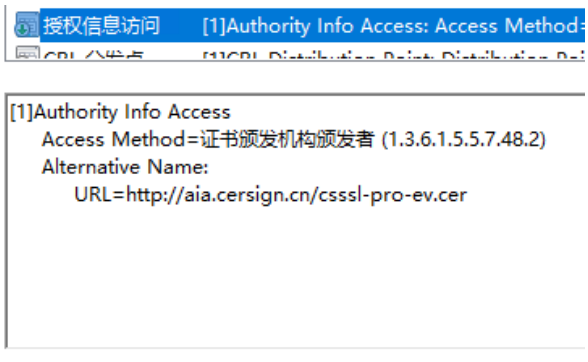
选择，因为太多域名会导致 SSL 证书文件变大，这就会增加浏览器同服务器握手时的流量，不仅浪费了流量，而且影响浏览器的 SSL 证书验证效率，降低了用户体验。

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 机构的国密根证书预置申请时发现有多家 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。请注意：AIA 字段只能是 http 方式访问，不能是 https 方式访问，某个银行部署的国密 SSL 证书没有部署完整的证书链，零信浏览器试图访问 AIA 时网站自动跳转到 https 方式访问而无法获取 AIA 文件，从而导致了这个银行网站无法正常显示国密 https 加密连接。

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。



(C) 2023 零信技术（深圳）有限公司

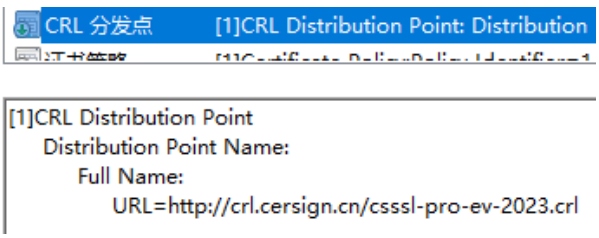
证书策略(Certificate Policy)这也是必须有的字段，明确告诉证书相关者这张证书的签发依据的 CPS(认证业务声明)的访问网址，用户可以直接点击证书常规中显示的“颁发者说明”直接访问这个网址。同时还会显示 Policy Identifier(OID)，一般至少有两个 OID，一个是定义此证书类型的 CA 自用 OID，另一个是此证书遵循的国密标准证书类型的 OID，如上图中的 1.2.156.157933.14 就是零信浏览器定义的国密 EV SSL 证书 OID，因为目前还没有国密标准定义的国密 SSL 证书类型 OID。

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。



(C) 2023 零信技术（深圳）有限公司

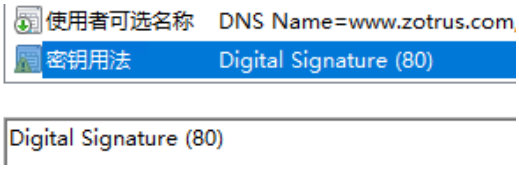
联机证书状态协议(OCSP)是一个能实时查询证书是否被吊销的计划替代 CRL 的协议，意在解决 CRL 文件可能很大(必须下载整个 CRL 文件才能查询到某种证书是否被吊销)，以及吊销列表发布不及时等问题，其优点是无需下载整个 CRL 文件，只需把要查询的证书的序列号给 OCSP 查询是否已吊销而返回一个“是”或“否”即可，这的确是一个高效率的解决方案。

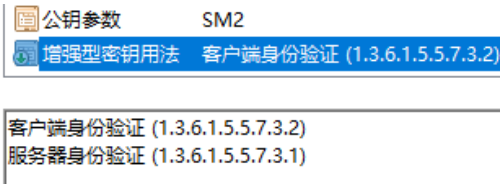
现在，国际标准已经决定废弃 OCSP，原因是随着所有常用网站都已经实现了 https 加密，用户浏览器不断地访问地 OCSP 系统泄露了用户的访问轨迹，这不利于保护用户隐私。所以，CA/浏览器论坛已经修改标准把目前的“OCSP 必须和 CRL 可选” 改为 “CRL 必须和 OCSP 可选”，并有专家提议把在证书透明机制中增加证书吊销查询功能。无论怎么变，证书吊销查询服务是 CA 机构必须提供的，这样浏览器就可以验证这张证书是否被吊销，从而能及时停止使用已吊销的证书。

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。国密算法SSL证书是双用法证书，其签名证书的密钥用法是“Digital Signature (数字签名)”，其加密证书的密钥用法是“Key Encipherment (密钥加密)”，但浏览器只展示签名证书。

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

(C) 2023 零信技术（深圳）有限公司

已经有 102 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的原因，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 系统公示怎么办呢？零信浏览器对于国际 SSL 证书，同谷歌浏览器一样是不信任的，提示“不安全”。但对于国密 SSL 证书，由于国密证书透明标准还在立项制定中，零信浏览器仅提示“证书不透明”。

如下左上图为 Windows 证书查看器看到的国密 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 行应该显示日志数据的签名算法，但是由于 Window 不在支持国密算法，所以不显示这一行信息，第 4 行显示的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。大家再看看如下左下图，这是目前零信浏览器的证书查看器展示的 SCT 列表字段信息，同谷歌浏览器一样并不解析这个字段，因为即使像 Window 那样解析一串大家看不懂的数字也没有任何意义，而是改在加密锁标识下面展示证书透明信息，如下右图所示，零信浏览器详细展示这张国密 SSL 证书有几个国密证书透明数据(3)、签名算法(SM2)和由哪些厂家的国密证书透明日志系统提供日志服务，一目了然。

以上讲清楚了国密 SSL 证书对照国际 SSL 证书中最关键的 9 个字段，这些字段遵循相关国密标准，包括 GM/T 0016、GM/T 0006、GM/T 0024、GB/T 38636 等，其他参数标准还在参考国际标准制定国密标准中，包括国密 SSL 证书基线标准、国密 EV SSL 证书标准、国密 CA

(C) 2023 零信技术（深圳）有限公司

系统网络安全要求、国密证书透明规范和国密证书自动化管理规范。而上面讲述的 9 个参数在国密标准来没有出台之前各家签发国密 SSL 证书的 CA 机构应该比照国际标准 SSL 证书执行，零信浏览器就是比照国际标准，如证书有效期判断、SSL 证书类型判断都参考国际标准来展示 UI。只有业界在相关国密标准还没有出台之前都能参照国际标准来严格要求国密 SSL 证书的签发和使用，才能真正保障国密 SSL 证书的安全，真正实现国密 HTTPS 加密来保障我国重要网站系统安全。

王高华

2023 年 8 月 21 日于深圳

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