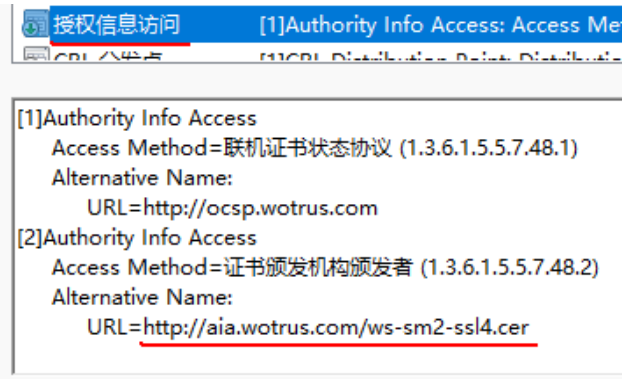
国密 SSL 那些事儿

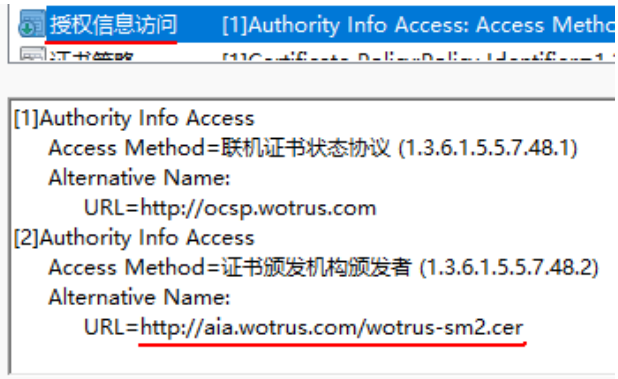
零信技术即将发布的第一个产品就是零信浏览器，其中一个最大的亮点就是支持国密 SSL 证书实现国密 https 加密。零信浏览器是基于开源的 Chromium 研发的，最主要的改动就是增加了对国密 SSL 的全面支持，这涉及到 SM2/SM3/SM4 算法的支持和对《GM/T 0024 SSLVPN 技术规范》和《GB/T38636-2020 信息安全技术传输层密码协议(TLCP)》两个国密标准规范的支持。当然，更重要的是对各家 CA 的国密根证书的信任预置，本文就讲讲这件事。

为了让用户能全面体验零信浏览器对国密 SSL 证书的支持，我们计划在浏览器正式发布时就已经预置几家已经签发了不少国密 SSL 证书的 CA 的国密根证书。在我们处理各家 CA 提交的国密根证书信任预置申请过程中，我们发现了我国 CA 签发的国密 SSL 证书还存在不少问题，还有很大了提升空间，希望本文能有助于提升国密 SSL 证书相关方的国密 SSL 相关技术水平，包括签发国密 SSL 证书的 CA 机构、部署国密 SSL 证书的用户、国密浏览器厂家等，大家共同努力提升我国国密 SSL 证书的技术水平和应用水平。

第一个问题：用户证书和签发 CA 证书没有 AIA 信息。

AIA 是 Authority Info Access 的缩写，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公钥来验证用户证书。当然，签发 CA 也必须有 AIA 信息，以便浏览器验证签发 CA 是否是由已经预置信任的顶级根证书签发。如下图左图为沃通 CA 的用户证书 AIA，右图为签发 CA 的 AIA。





我们很遗憾地看到申请零信浏览器根预置的 CA 中有多家 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，请一定要确保 AIA 网址可访问，并

且是正确的签发 CA 证书。

第二个问题：用户证书没有身份认证级别标识 OID。

国际标准中定义了 4 种不同认证级别的 SSL 证书的 OID, DV SSL 证书 OID：2.23.140.1.2.1，IV SSL 证书 OID：2.23.140.1.2.3，OV SSL 证书 OID：2.23.140.1.2.2，EV SSL 证书 OID：2.23.140.1.1，SSL 证书中策略中有这些 OID 就可以使得浏览器只需读取这些 OID 就知道这张 SSL 证书的身份认证级别，就可以根据不同的认证级别展示不同用户界面，如 EV SSL 证书展示绿色地址栏和单位名称。

但是，我们发现只有个别 CA 签发的国密 SSL 证书中有这些 OID，大部分 CA 签发的国密 SSL 证书中并没有包含这些 OID，也许是考虑到用这些 OID 不太合适吧，因为国际 CA/浏览器论坛中定义的这些 OID 后面明确说明了这些 OID 仅适用于满足相关国际标准签发的 SSL 证书，而目前国密算法还没有纳入 CA 相关的国际标准中。也就是说，如果国密算法 SSL 证书使用这些 OID 应该是不合适的，虽然国际 CA/浏览器论坛可能不会找麻烦。

怎么办？首先，希望国家主管部门能尽快从国家根使用的 OID 架构中定义 4 个 OID 用于定义证书的身份认证级别。当然，这可能是远水解不了近渴，所以，零信浏览器可信根证书认证计划定义了 4 个用于不同认证级别的 OID，申请预置信任的 CA 都可以免费使用这些 OID 来标识不同认证级别的 SSL 证书，具体有：DV SSL 证书：1.2.156.157933.11，对应国际 OID：2.23.140.1.2.1；IV SSL 证书：1.2.156.157933.12，对应国际 OID：2.23.140.1.2.3；OV SSL 证书：1.2.156.157933.13，对应国际 OID：2.23.140.1.2.2；EV SSL 证书：1.2.156.157933.14，对应国际 OID：2.23.140.1.1。有了这些 OID，浏览器就可以准确地识别国密 SSL 证书的认证级别，从而可以正确地显示不同的用户界面。

第三个问题：用户证书没有增强密钥用法、没有吊销列表(CRL 和 OCSP)、没有使用者可选名称。

这些都是不应该有的问题，但是很遗憾有些CA签发的国密SSL证书没有增强密钥用法(EKU)，这是必须有的：服务器身份验证 (1.3.6.1.5.5.7.3.1)和客户端身份验证(1.3.6.1.5.5.7.3.2)，只有有了这两个EKU才能证明这张证书是SSL证书，所以这个是必须有的。

而吊销列表当然也是必须有的，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有效，是否被吊销。而使用者可选名称，这也是必须有的，否则浏览器就无法正常获取证书绑定的域名信息，也就无法正常展示SSL证书了。

第四个问题：用户部署 SSL 证书没有带上签发 CA 证书。

这个问题是需要 CA 机构提醒用户在部署国密 SSL 证书时，必须带上签发这张 SSL 证书的

中级根证书，这样浏览器在同服务器握手时就可以获得签发 CA 证书，就不需要从用户证书中 AIA 网址去获取，能更快速验证证书是否可信。如果有的 CA 短时间内无法在用户证书中增加 AIA 网址，则必须要求用户在部署证书时带上中级根证书，这也不失为一个临时补救的方法。推荐 CA 为用户提供常用的服务器的用户证书文件时直接为用户提供加中级根证书的证书绑定文件，如 Nginx 服务器就是把签发 CA 证书同用户证书叠加在一起即可。请注意：不需要加上顶级根证书，加上去会增加 SSL 握手的流量，降低通信效率，增加服务器带宽消耗。

今天就说这四件事，还有一个很重要的问题比较复杂，非三言两语说得清楚，下次独立写一篇文章来讲。希望本文所讲的四个问题能引起签发国密 SSL 的 CA 机构和使用国密 SSL 证书的用户的高度重视，改进这些问题有利于浏览器能快速验证证书是否可信和正确展示证书的身份认证级别，同时也就改善了浏览器用户的体验。

最后，笔者希望国家主管部门能及时发布国密 SSL 证书相关的 CA 基线标准，规范国密 SSL 证书的签发和使用。同时希望各个国密 SSL 证书相关方能一起努力，把国密重器用好，共同为普及国密 SSL 证书应用做贡献，让国密 SSL 证书真正能为保障我国互联网安全发挥最大的作用，进而有力推动已经成为国际标准的 SM2/SM3/SM4 算法的国际化广泛接受和使用，共同推动 SM2 算法能早日纳入 SSL 证书相关国际标准中，早日实现用户可以像现在自由选择 RSA/ECC 算法的 SSL 证书一样自由选择 RSA/ECC/SM2 算法，而无需部署两张不同算法的 SSL 证书，笔者坚信这一天一定会到来，也期待通过大家的努力能早日到来。

王高华

2022 年 4 月 20 日于深圳

请关注公司公众号，实时推送公司 CEO 精彩博文。