零信浏览器为 Windows 打商密算法补丁

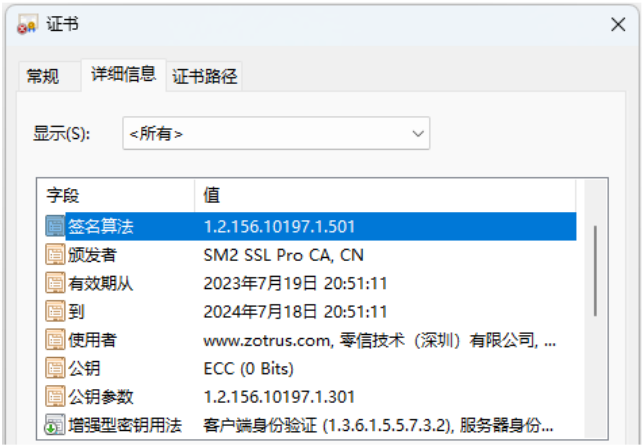
这是一件利国利民利全球的大事，笔者必须写篇文章好好讲一讲这事。本文先请读者看看 Windows 目前是如何展示商密 SSL 证书的，再请大家看看安装了今天发布的零信浏览器最新版本 2401 后，Windows 是如何展示商密 SSL 证书的，最后会讲一讲这件事的重要意义-利国利民利全球。

一、Windows 是如何展示商密 SSL 证书的？

Windows 不支持商密算法，这个大家也能理解，毕竟不是国产操作系统，甚至大家也能心安理得地接受这个现实。笔者从 2019 年 4 月 4 日创立我国第一个商密 SM2 算法 SSL 根证书时就在想：如果 Windows 能支持商密算法，那该多好哦。5 年过去了，笔者并没有看到 Windows 支持商密算法，点击商密 SSL 证书，证书查看器虽然能正常显示证书绑定域名、颁发者和证书有效期信息，但是仍然由于无法识别商密算法而显示“验证信任关系时，系统层上出现了一个错误”，如下左图所示，这个提示很准确，的确是 Windows 在系统层不支持商密算法。如下左图所示。点击查看证书路径，只能显示用户证书绑定的域名，不显示证书链，证书状态显示为“该证书有一个无效的数字签名”。这绝对是误报！这张商密 SSL 证书一定是有一个有效的数字签名，只是 Windows 无法验证此数字签名而已。

继续查看证书详细信息，如下左图所示，“签名算法”字段显示 OID：1.2.156.10197.1.501，“公钥参数”字段也是显示 OID：1.2.156.10197.1.501，而不是像 RSA 算法 SSL 证书一样显示算法名称“sha256RSA”和 RSA (2048bits)。由于 SM2 算法也是一种椭圆曲线算法(ECC)，所以，

Windows 能识别出商密 SSL 证书的公钥为 ECC 算法，但是由于无法识别椭圆曲线参数而显示公钥长度为 0 bits，实际是 256 bits，并且也能正确显示各个字节数据，如下右图所示。



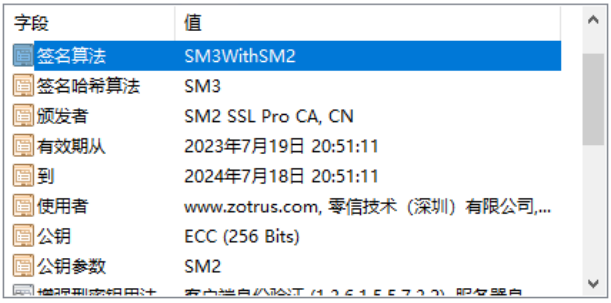
二、零信浏览器给 Windows 打补丁后，又会怎样显示商密 SSL 证书？

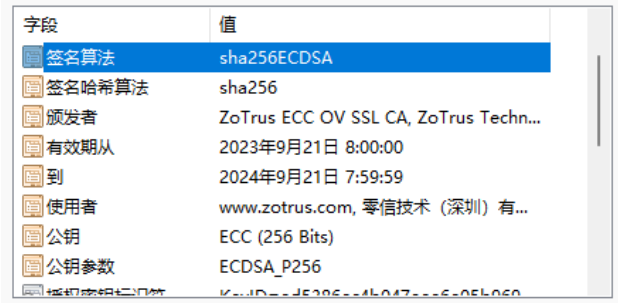
2021 年 6 月笔者重新创业，在这 3 年里，笔者带领研发团队努力打造了 3 个商用密码应用生态：商密证书透明生态、商密证书自动化管理生态、内网 SSL 证书应用生态，并打造了这 3 个生态中必不可少的核心产品，包括：零信浏览器、零信国密证书透明日志系统、零信云 SSL 服务系统、零信国密证书自动化服务系统、零信国密 HTTPS 加密自动化网关、零信国密 HTTPS 加密自动化云服务、证签国密 SSL 证书和国际 SSL 证书(公网 SSL 证书和内网 SSL 证书)等等。但是，最广泛使用的 Windows 系统不支持商密算法，无法正常显示商密 SSL 证书和各家 CA 机构签发的 USB Key 证书，这一直是挂在笔者心头中的一件大事。

直到零信浏览器发布了支持 USB Key 证书双向认证的 2311 版本，才触动了笔者决定研发一个 Windows 补丁，让 Windows 能支持商密算法证书验证，能像 RSA 算法证书一样正常展示商密算法证书，能像 RSA 客户端证书一样使得浏览器能弹出商密证书完成双向认证，而不是目前的各家 USB Key 厂商自己编程实现或者根本没有实现。

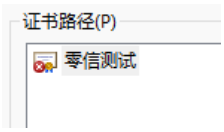
今天，零信浏览器发布了 2401 版本，从这个版本开始，零信浏览器在安装后会自动给 Windows 打补丁，使得 Windows 能像支持 RSA/ECC 算法证书一样完成证书验证和正常展示，如下左图所示，Windows 能正常显示证书常规信息，不会提示验证信任关系失败。如下右图所示，能正常显示证书路径，证书状态显示“该证书没有问题”。请注意：这是 Windows 在支持了商密算法后的证书查看器显示的证书验证信息，而不是零信浏览器提示的，零信浏览器在发布时就已经在浏览器内正常展示商密 SSL 证书了。

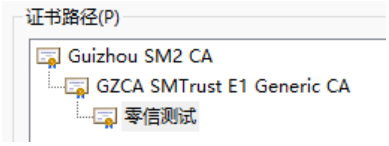
继续查看证书详细信息，如下左图所示，能正常显示此证书的签名算法是“SM3WithSM2”，签名哈希算法为 SM3，公钥为 ECC(256bits)，公钥参数为 SM2，全部正确。请读者朋友再使用谷歌浏览器访问零信官网，下载其 ECC 算法 SSL 证书，其证书详细信息展示如下右图所示，可以看出 Window 能像 ECC 算法一样展示 SM2 算法 SSL 证书，都是 ECC (256 bits)公钥，而公钥参数则分别显示为 SM2 和 ECDSA_P256，因为 SM2 算法同 ECDSA_P256 算法的唯一不同就是采用了不同的椭圆曲线参数。

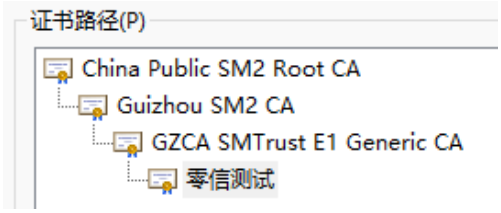




当然，不仅仅是能展示商密 SSL 证书，一样可以正常展示各家 CA 签发的 USB Key 证书，如下左图所示，这是没有打补丁之前贵州 CA 签发的用户证书的展示，无法正常显示证书链。而在安装了零信浏览器后，如下中图所示，就能正常显示用户证书的三级证书链，正常支持用户证书的双向认证。如果用户电脑没有安装贵州 CA 的国密根证书，则会显示国家根为顶级根的四级证书链，如下右图所示。





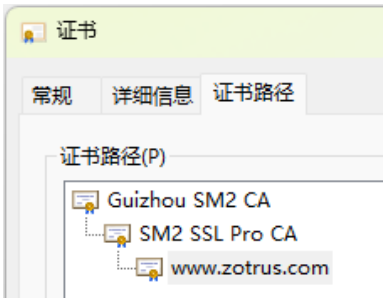


三、Windows 支持商密算法有何最大意义？

零信浏览器为 Windows 打了商密算法支持补丁，不仅大大方便了中国用户查看 SM2 算法数字证书，包括 SM2 SSL 证书、SM2 客户端证书、SM2 邮件证书、SM2 代码签名证书和 SM2 文档签名证书，更重要的是可以让 Windows 能像处理 RSA/ECC 算法数字证书一样处理 SM2 算法证书，充分利用 Windows 强大的证书应用能力来支持各种 SM2 算法证书应用，如最常用的双向认证。这是意义之一。

意义之二就是大大方便了全球用户认识和了解 SM2 算法数字证书，特别是 SM2 SSL 证书，因为用户如果看到一张证书 Windows 显示为“验证信任关系时，系统层上出现了一个错误”和“该证书有一个无效的数字签名”，第一感觉就是这张证书有问题，从而提高了警惕而不会去关注这张证书了，这不利于宣传我国的商用密码算法。

零信浏览器用户已经覆盖全球一百多个国家和地区的用户，零信浏览器这次为 Windows 打商密算法补丁后，全球用户不仅能在零信浏览器地址栏领略 SM2 算法 SSL 证书风采，而且下载此证书后能让 Windows 正常显示证书链和证书详细信息，这非常方便了全球用户能认识和了解 SM2 算法 SSL 证书，有利于这个已经成为 ISO 国际标准的密码算法在全球范围的应用，让全球用户有了一个 RSA 算法以外的新选择，为全球互联网用户提供一个可选的中国密码算法方案，让 SM2 算法同 RSA 算法一道共同保障全球互联网安全。



四、欢迎免费使用零信浏览器，让您的电脑完美支持商密算法

零信浏览器以其卓越的性能、丰富的功能和对商密算法的全面支持，不仅赢得了中国用户的喜爱，成为了中国市场第一市场份额的商密浏览器。而且，由于全球独家支持 EV 认证的绿色地址栏、独家展示网站 WAF 防护标识、独家支持实时验证 PDF 文档数字签名和展示签名者可信身份、独家特别展示证书透明等特色功能，同时受到了全球上百个国家和地区用户的欢迎，全球用户数正在不断快速上升中。

笔者强烈建议所有新老用户 下载 安装零信浏览器最新的版本，而不是老版本升级，这样才能使得 Windows 完美的支持商密算法，完美地查看商密算法数字证书，完美地实现商密客户端证书的双向认证。同时，由于 Windows 已经完美支持商密 SM2 算法数字证书，期待有更多的全球厂商能开发出更多的各种商密证书应用，共同为普及商密算法做贡献，让全球用户有更多的密码算法选择，用商密来保障全球互联网安全。

有诗为证：

视窗补丁零信打，
普及商密立新功。
视窗系统识商密，
优选商密保安全。

王高华

2024 年 5 月 16 日于深圳

欢迎关注零信技术公众号，实时推送每篇精彩 CEO 博客文章。
已累计发表中文 166 篇(共 45 万多字)和英文 67 篇(8 万 2 千多单词)。。