政府网站纯国密 HTTPS 加密时代来了

笔者一直没有找到来自宝鸡市的零信浏览器用户数持续快速增长的原因，直到最近一个零信浏览器的用户在线询问为何某个政府网站使用零信浏览器无法正常访问时，才找到了真相，今天特撰文聊聊这事。

一、 某政府网站只部署国密 SSL 证书，开启纯国密时代！

这个仅部署国密 SSL 证书的政府网站是宝鸡市住房维修资金服务中心的互联网政务应用系统—住宅专项维修资金管理系统，这是一个为业主建立专项维修资金的缴存、使用、结存等服务的政务应用系统，由成都鹏业软件股份有限公司中标承建。

如果使用谷歌浏览器访问，则提示：使用了不受支持的协议。客户端和服务器不支持一般 SSL 协议版本或加密套件。也就是说：服务器仅支持不一般的 SSL 协议和加密套件，这个不一般的 SSL 协议就是国密 SSL 协议和国密加密套件。

很明显，这个网站系统不仅国密合规，而且已经满足网信办、中央编办、工信部和公安部联合发布的《互联网政务应用安全管理规定》(以下简称《规定》) 的要求，已经完成国密改造支持国密 HTTPS 加密。但是，这个网站居然只部署国密 SSL 证书实现 HTTPS 加密，用户

无法使用常用的四大浏览器访问了，并没有像传统国密改造那样部署双算法双 SSL 证书。笔者作为最早提出双算法双 SSL 证书同时部署的方案提出者，也着实惊到了，一句话：这个网站主管或单位领导有魄力，点赞！

二、 政府网站只部署国密 SSL 证书，时机成熟吗？

一定有政府网站主管会提出这样的疑问，笔者在看到宝鸡市住建局的大胆作为后的现在可以肯定地回答这些有疑问的主管们：时机已经成熟！

为何笔者这么肯定地认为政府网站只部署国密 SSL 证书的时机已经成熟呢？实现国密 HTTPS 加密需要三个核心产品：Web 服务器国密算法支持模块、国密 SSL 证书、国密浏览器，如果这三个产品在市场上能充足供应，并且充分竞争，那么国密 HTTPS 加密的时机就已经成熟。

先说 Web 服务器国密算法支持模块，市场上有多家提供这个模块，有收费和免费的，零信技术也曾免费提供，但是最根本的市场供应转折点就是完全免费的阿里系铜锁 SSL 的完全开源免费使用，使得 Web 服务器国密改造就不再是难事了。零信技术也是不仅自己的产品在用，而且直接向用户推荐使用。

第二个就是国密 SSL 证书，这是实现国密 HTTPS 加密的关键产品，目前市场上有十几家 CA 机构都能签发国密 SSL 证书，这个市场供应也是非常充足的。只是还有不少 CA 机构签发的国密 SSL 证书不支持国密证书透明，但这目前并不影响正常使用。

第三个重要的产品是国密浏览器，RSA 国际算法在全球范围的普及应用于 HTTPS 加密，其最大的功劳是常用的四大浏览器(谷歌 Chrome、微软 IE/Edge、苹果 Safari 和火狐浏览器)的完全免费供应。而要想普及国密 HTTPS 加密，当然必须有国密浏览器，目前市场上已有多家公司提供国密浏览器，但是国密浏览器的充足供应的转折点就是高性能的、干净无广告的、支持国密算法和国密证书透明的零信浏览器的完全不受任何限制的免费使用，这是政府用户敢只部署国密 SSL 证书的最大底气，用户不用花钱购买国密浏览器，不给最终用户造成任何使用负担，只需推荐最终用户使用完全免费的零信浏览器即可。

实现国密 HTTPS 加密所需的三大产品，已经实现了市场上的充足供应，并且两大核心产品都是完全免费使用，其中 SSL 证书不仅价格公道，还有完全免费供应的。这就是这个政府网站敢于仅部署国密 SSL 证书的底气，因为仅部署国密 SSL 证书不影响为老百姓提供互联网政务服务。

三、 政府网站只部署国密 SSL 证书，有什么好处？

宝鸡市这个政府网站仅部署国密 SSL 证书，当然也一定是全面权衡了利弊的。笔者就站在政府用户的角度给总结一下有哪些好处，供正在选型国密 HTTPS 加密改造的政府用户决策参考。

第一：合规、明智

各种法律法规都要求政府官网和政务服务网站都必须完成国密改造，过等保，过密评，有些单位的做法是消极的应对，蒙混过关即可，而实际正在运行的政府网站系统仍然是 HTTP 明文不安全方式或者 RSA 算法 HTTPS 加密方式运行。

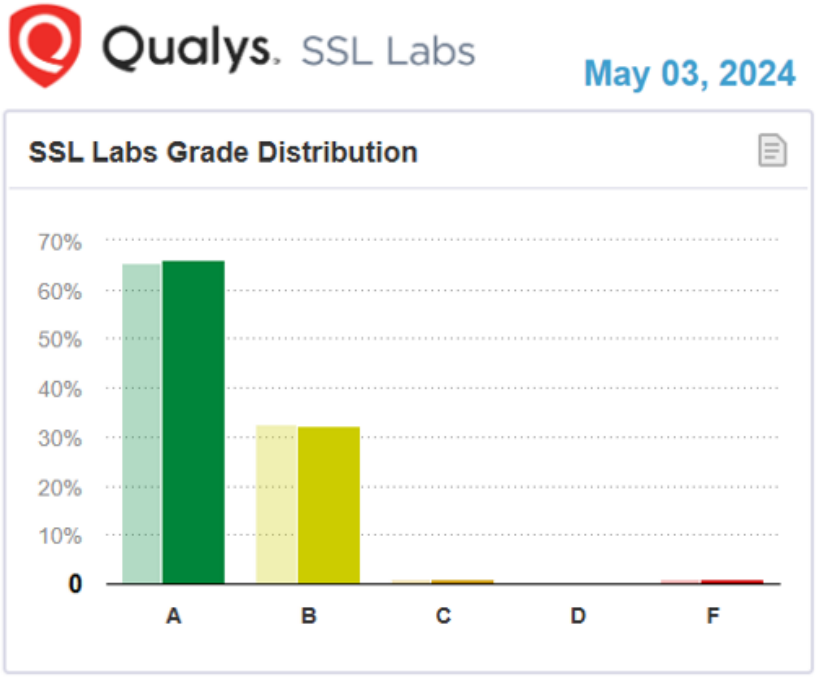
而最明智和更高明的做法是反正必须完成国密改造，索性就一步到位，让所有系统直接上国密了，不再搞两套，直接满足各种法律法规的要求。

第二：更省钱

这一点也非常重要，国际算法 SSL 证书再便宜也还是要花钱的，何不直接只买国密 SSL 证书更省钱呢？

第三：更安全

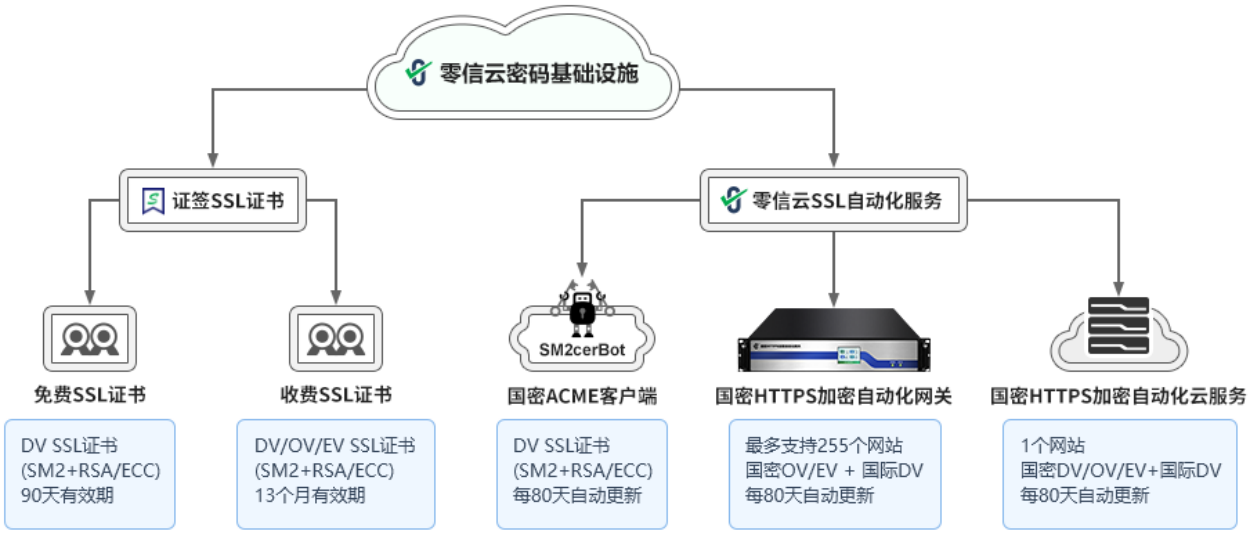
这一点可能有些读者不能理解。根据权威的 Qualys SSL 实验室监测数据表明：全球 SSL 证书部署中只有 66%的网站达到 A 级(安全)，32%为 B 级(不安全)，还有 2%网站处于极不安全的 C/D/F 级。这些不安全的原因是没有关闭各种不安全协议和加密套件，也就是说，RSA 密码体系中的 SSL 协议从 30 年前推出到现在一直在不断的完善中，但是仍然有大量的系统还是使用不安全的协议和加密套件，而导致了部署 RSA 算法 SSL 证书的网站的不安全。



而国密算法(SM2/SM3/SM4)和相关的国密 SSL 协议标准由于起步晚，一开始就直接采用了非常安全的协议和密钥长度，不存在像 RSA 算法 SSL 证书那样的许多历史遗留的不安全协议，所以，如果直接部署国密 SSL 证书，就不用考虑像部署国际 SSL 证书那样还需要同时解决各种存在的不安全的协议修补问题，更简单和更安全。有兴趣了解这方面知识的读者，可以看一下读者在 2021 年写的文章《网银 SSL 证书部署还有漏洞？》。

四、 零信技术给足政府用户底气，可以大胆实施纯国密算法 HTTPS 加密

零信技术为政府用户提供了完整的一站式纯国密 HTTPS 加密解决方案，而不仅仅是提供完全免费的国密浏览器—零信浏览器。零信技术投资建设了功能完善的云密码基础设施，为用户提供证签品牌 SSL 证书和零信品牌证书自动化服务，前者为传统 SSL 证书服务，需要用户自己申请国密 SSL 证书和安装国密算法支持模块后部署国密 SSL 证书，每年都要部署一次；后者为用户提供自动化证书服务，用户无需申请和部署 SSL 证书，也无需改造原 Web 服务器，自动化为用户配置国密 SSL 证书，自动化续期证书。



1. 敞开供应完全免费的 90 天有效期的国密 SSL 证书

欢迎在线申请证签品牌公网免费 SSL 证书，仅限于公网域名和公网 IP 地址申请使用，完全免费，90 天证书有效期，可供测试和试用，国密 SSL 证书从证签自有根签发，仅零信浏览器信任，支持国密证书透明。同时免费配套提供全球信任的国际 SSL 证书，也是 90 天有效期，由 Sectigo 顶级根给证签定制的中级根签发，所有浏览器都信任。

同时，欢迎在线申请证签品牌内网免费 SSL 证书，支持内网 IP 地址和内部主机名，同时支持公网 IP 地址和公网域名，完全免费，90 天证书有效期，可供测试和试用，国密 SSL 证

书和国际 SSL 证书都从证签自有根签发，支持国密证书透明，仅零信浏览器信任，其他浏览器不支持内网 SSL 证书。

2. 欢迎选购由贵州 CA 国密根证书签发的国密 SSL 证书，国民价格

欢迎在线选购证签品牌公网收费 SSL 证书，仅限于公网域名和公网 IP 地址申请使用，国民价格，13 个月证书有效期，国密 SSL 证书从拥有 CA 许可证的贵州 CA 国密根签发，支持国密证书透明，所有国密浏览器都信任，同时免费配套提供全球信任的国际 SSL 证书，13 个月证书有效期，由 Sectigo 顶级根给证签定制的中级根签发，所有浏览器都信任。

同时，欢迎在线选购证签品牌内网收费 SSL 证书，支持内网 IP 地址和内部主机名，同时支持公网 IP 地址和公网域名，13 个月证书有效期，国密 SSL 证书和国际 SSL 证书都从证签自有根签发，支持国密证书透明，仅零信浏览器信任，其他浏览器不支持内网 SSL 证书。

政府客户案例：湖南省人民政府官网、深圳市人民政府官网等上百家政府单位

3. 欢迎选用完全免费的国密 HTTPS 加密自动化客户端软件 SM2cerBot

对于希望自动化搞定国密 HTTPS 加密的用户，可以 免费下载 国密 HTTPS 加密自动化客户端软件 SM2cerBot，这是一个同目前国际上流行的需要用户在 Web 服务器上安装 ACME 客户端软件一样的解决方案，不一样的是国密 ACME 客户端软件为用户自动化申请和部署国密 SSL 证书和国际 SSL 证书，满足用户国密合规和全球信任的双需求。

国密 ACME 客户端软件 SM2cerBot 免费自动化申请和部署的国密 SSL 证书从证签自有根签发，支持国密证书透明，仅零信浏览器信任，同时免费配套的全球信任的国际 SSL 证书由 Sectigo 顶级根给证签定制的中级根签发，所有浏览器都信任。鉴于研发资源有限，目前 SM2cerBot 仅支持特定的 3 个版本操作系统，需要用户自行搞定软件安装和配置，不提供技术支持。

国密 ACME 客户端软件 SM2cerBot 实测网站：https://sm2test.cersign.cn，双算法 SSL 证书设置为每天自动化更新双 SSL 证书，欢迎同时使用零信浏览器和其他浏览器查看和检验实际部署效果。

4. 欢迎选购国密 HTTPS 加密自动化网关

这是零信技术的拳头产品，彻底解决用户要求 Web 服务器零改造的难题，用户只需在原 Web 服务器前面部署 零信国密 HTTPS 加密自动化网关，就可以自动化实现国密 HTTPS 加密和 WAF 防护。原 Web 服务器无需申请和安装 SSL 证书，无需安装国密支持模块，无需安装国密 ACME 客户端软件，由零信网关自动化对接零信云 SSL 服务系统，同时为最多 255 个网站提供国密 SSL 证书和国际 SSL 证书，自动化实现自适应加密算法的 HTTPS 加密，零信浏览器优先采用国密算法实现 HTTPS 加密。

零信国密 HTTPS 加密自动化网关自动化为用户网站配置的国密 OV SSL 证书由贵州 CA 国密根签发，支持国密证书透明，所有国密浏览器都信任，国际 DV SSL 证书由 Sectigo 国际根定制的零信品牌中级根证书签发，所有浏览器都信任。零信网关不仅让用户不再操心 SSL 证书的申请和部署问题，同时每 80 天自动更新双证书，有力保障密钥安全。

零信国密 HTTPS 加密自动化网关为用户提供四大超值服务：一是 5 年最多为 255 个网站自动化配置双算法 SSL 证书的市场价值高达 623 万元，二是 5 年持续为最多 255 个网站自动化配置 SSL 证书节省运维工程师费用 150 万元，三是免费配套的高性能 WAF 服务为用户节省购置 WAF 设备费用高达 100 万元，四是用户不再需要升级改造 Web 服务器支持 IPv6，零信网关自动实现 IPv6 到 IPv4 的协议转换，让 IPv6 用户可以国密 HTTPS 方式访问网站。

5. 欢迎选购国密 HTTPS 加密自动化云服务

零信国密 HTTPS 加密自动化网关是为有多个网站系统需要实现国密 HTTPS 加密自动化而设计的，如果用户只有一个网站希望实现国密 HTTPS 加密自动化，则推荐选用零信国密 HTTPS 加密自动化云服务，这是一个把零信网关部署在云上共享给 255 个网站使用的创新云服务，用户无需购买硬件网关，也无需部署网关，无需向 CA 申请 SSL 证书，无需安装国密支持模块和国密 SSL 证书，无需安装国密 ACME 客户端软件，只需选购零信云服务，设置网

站域名，做两次域名解析即可自动化配置双算法 SSL 证书，自动化实现国密 HTTPS 加密和 WAF 防护。

零信国密 HTTPS 加密自动化云服务自动化为用户网站配置的国密 DV/OV/EV SSL 证书由贵州 CA 国密根签发，支持国密证书透明，所有国密浏览器都信任，国际 DV SSL 证书由 Sectigo 国际根定制的零信品牌中级根证书签发，所有浏览器都信任。零信云服务不仅让用户不再操心 SSL 证书的申请和部署问题，同时每 80 天自动更新双证书，有力保障密钥安全。

零信国密 HTTPS 加密自动化云服务为用户提供四大超值服务：一是为用户节省 SSL 证书费用，二是为用户节省运维工程师费用，三是为用户节省购置 WAF 设备费用，四是用户不再需要升级改造 Web 服务器支持 IPv6，零信云服务自动实现 IPv6 到 IPv4 的协议转换，让 IPv6 用户可以国密 HTTPS 方式访问网站。

五、 纯国密 HTTPS 加密时代已来，普及国密 HTTPS 加密进入快车道

笔者必须在这里给宝鸡市住房维修资金服务中心再次点个大赞，可以毫不夸张地讲，这是国密 HTTPS 加密普及征程上的一个里程碑事件，一个拐点事件，标志着普及国密 HTTPS 加密的三个核心产品已经成熟，并且已经可以敞开供应和多供应商公平竞争，这是一个市场成熟的主要标志。用户是非常精明的，市场是公平的，用户选择了纯国密 HTTPS 加密，当然是看到了其中的超值价值。

也就是说，纯国密 HTTPS 加密时代已来，这个拐点的到来是国家出台相关法律法规规定所希望实现的结果，是 IT 业界和密码业界共同努力的结果，也是所有网站主希望看到的结果，大家继续齐努力，加速实现普及国密 HTTPS 加密，只有普及采用我国完全自主知识产权的商用密码体系才能真正保障我国网络空间安全。

王高华

2024 年 11 月 18 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 192 篇(共 55 万 1 千多字)和英文 80 篇(10 万 3 千多单词)。