密评和密改必须与时俱进

笔者一直想写篇文章吐槽一下目前密评和密改的现状，如重视门禁改造而不重视 HTTPS 加密改造，但是一直不知道如何下笔，毕竟密评和密改对普及应用商用密码是一件利国利民的大好事，笔者作为一个有二十年密码从业经历的密码人，很是欣慰这些年来我国在密评和密改方面所取得的各种成就。也许正是因为爱得越深，也就越觉得还有很大的提升空间，也就越想写篇文章同同行和用户分享笔者的思考。

最近四部委 5 月 22 日发布的《互联网政务应用安全管理规定》(以下简称《规定》)给了笔者灵感，知道该如何下笔了。《规定》绝对是密评工作的方向标，密评和密改工作都必须与时俱进，为《规定》的顺利实施提供最大的支持。但如何与时俱进？本文详细讲述，希望相关从业者和用户都能有所启发、有所行动和知道怎么行动。

一、 什么是密评？为何需要密评？密评与《规定》有什么关系？

密评的全称是商用密码应用安全性评估，是指在采用商用密码技术、产品和服务集成建设的网络和信息系统中，对其密码应用的合规性、正确性和有效性等进行评估。也就是说，密评的目的是为了对必须采用商用密码进行信息加密和安全认证的网络和信息系统进行第三方评估。

1. 密评要评估什么？

密评就是要评估网络和信息系统的密码应用合规性—是否采用了商用密码算法和相关的商用密码产品，评估是否正确采用，评估采用后是否有效，是否能真正用商用密码来保障网络和信息系统安全。这就是密评三要素—是否采用、是否正确采用、采用后是否有效。

《规定》第二十九条要求互联网政务应用应当使用 CA 机构提供的商密 SSL 证书来实现 HTTPS 安全连接方式访问，这就是明确了必须采用、必须正确商用密码来实现 HTTPS 加密连接。这个就需要第三方密评机构来评估是否已经采用，是否正确采用，采用后是否有效。

《规定》第二十八条要求如果互联网政务应用使用 CDN 服务，则 CDN 服务必须支持商密 HTTPS 加密，这是结合第二十九条的解读。这个也需要第三方密评机构来评估政府单位如果使用了 CDN 服务，则 CDN 是否支持商密 HTTPS 加密，是否正确地支持，是否真的是商密 HTTPS 加密。笔者认为，不仅仅是 CDN 服务必须支持，云 WAF 服务也必须支持。

《规定》第三十五条要求政务邮件系统必须采用、必须正确采用商用密码对电子邮件数据进行安全保护。这个也需要第三方密评机构来评估是否已经采用，是否正确采用，采用后是否有效。

2. 密评的对象是谁？

密评的对象是涉及国家安全和社会公共利益的重要领域网络和信息系统的建设、使用、管理单位，包括基础信息网络、涉及国计民生和基础信息资源的重要信息系统、重要工业控制系统、面向社会服务的政务信息系统，以及关键信息基础设施、网络安全等级保护第三级及以上的信息系统。

其中的“面向社会服务的政务信息系统”就是《规定》第二条所指的互联网政务应用，具体是指机关事业单位在互联网上设立的门户网站，通过互联网提供公共服务的移动应用程序（含小程序）、公众账号等，以及互联网电子邮件系统。也就是说，所有互联网政务应用都必须通过密评，这就明确了密评的评测内容，并且是急需评测的内容，因为《规定》将于 7 月 1 日施行。请注意：这个密评包括政府单位官网、政务 APP、公众账号、政务邮件系统共四类系统。

3. 密评的依据是什么？

密评的依据是被测信息系统通过评审的密码应用方案和 GM/T 0054-2018《信息系统密码应用基本要求》，从总体要求、物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全、密钥管理以及安全管理等方面开展评估。

《规定》第十七条就已经明确要求建设互联网政务应用应当落实网络安全等级保护制度和国家密码应用管理要求，按照有关标准规范开展定级备案、等级测评工作，这就是指等保测评和密保密评。“落实安全建设整改加固措施，防范网络和数据安全风险”就是等保整改和密评密改。

这就要求密评必须配合《规定》施行而进行密码应用安全评估工作，必须评估：

(1) 互联网政务应用的物理和环境安全是否正确有效地采用了商用密码技术、产品和服务来保护；
(2) 互联网政务应用的网络和通信安全是否正确有效地采用了商用密码技术、产品和服务来保护；
(3) 互联网政务应用的设备和计算安全是否正确有效地采用了商用密码技术、产品和服务来保护；

(4) 互联网政务应用的应用和数据安全是否正确有效地采用了商用密码技术、产品和服务来保护；

(5) 互联网政务应用的密钥管理是否正确有效地采用了商用密码技术、产品和服务来保护。

二、 什么是密改？密评和密改的重点是互联网政务应用 HTTPS 加密的安全评估和改造

第一部分讲清楚了什么是密评、密评应该为《规定》所要求的互联网政务应用应当落实国家密码应用管理要求评测哪些内容。本部分就重点讲其中的“网络和通信安全”部分，这部分也是“应用和数据安全”的数据流通安全的基础保障。

根据《中国 SSL 证书市场发展趋势分析简报-2024Q1》发布的统计数据，属于《规定》所指的互联网政务应用的 31 个省市自治区政府官网域名申请的国际算法 SSL 证书的申请量为 1633 张，所有政府单位*.gov.cn 域名申请的国际 SSL 证书数量为 16658 张。而根据发布《规定》四部委之一的中央编办发布的全国党政机关、事业单位网站标识发放总量为 111033 个，也就是至少有 11 万多个机关事业单位总共仅申请了 1.6 万多张 SSL 证书，SSL 证书申请普及率为 15%，如果考虑到有许多单位申请了多张 SSL 证书，估计真正的普及率低于 10%。而这不到 10%的 SSL 证书申请量还是国际 RSA 密码算法 SSL 证书，而不是密评和《规定》要求的商密 SSL 证书，目前只有湖南省一个省级政府官网和公安部一个部委官网部署了商密 SSL 证书实现 HTTPS 加密。这就是密改的巨大市场！而《规定》要求这 11 万多个政府官网都必须实现商密 HTTPS 加密，希望相关从业者能看到这个巨大的密改市场！

依据《规定》第二十九条，11 万多个政府官网以及相关的政务服务系统都必须完成密改而通过密评，这个密改就是要实现商密 HTTPS 加密，而不是 RSA 密码算法的 HTTPS 加密。商密 HTTPS 加密是确保“网络和通信安全”的必须和唯一技术手段，没有其他技术方案，只有商密 HTTPS 加密才能保障我国的网络通信安全。也只有实现了商密 HTTPS 加密，才能真正有效的保障“应用和数据安全”，保障数据从政务系统通过 HTTPS 加密方式流通到用户设备中。也只有实现了商密 HTTPS 加密，才能保证政务 CDN 内容分发的数据传输安全。WAF 防护也只有实现了商密 HTTPS 加密，才能真正保证政务 Web 应用安全。

所以说，密评的重点是评估互联网政务应用是否使用了商用密码来实现 HTTPS 加密保护，是否正确实现和采用后是否有效。而根据上面的统计数据，互联网政务应用都需要整改来满足密评的要求，密改工作的重点也是 HTTPS 加密的整改，不仅必须实现 HTTPS 加密，而且必须

实现商密 HTTPS 加密。

但是，采用国际 SSL 证书实现 HTTPS 加密的普及率都不到 10%，这是因为传统的人工向 CA 申请 SSL 证书部署到 Web 服务器上使用比较繁琐，一个省政务平台所管的网站有上万个，根本无法手工普及实现 HTTPS 加密，这绝对不是经费问题，因为市场上有完全免费的 SSL 证书，而是实施难度问题。而如果要实现商密 HTTPS 加密，则就难上加难了，因为不仅仅是需要商密 SSL 证书，还需要 Web 服务器改造支持商密算法，还需要 CDN/WAF 支持商密算法，还需要浏览器和 APP 支持商密算法，这是一个生态改造的难题。

怎么办？目前的密改典型方案就是为某个网站向 CA 申请一张商密 SSL 证书，部署到某个网站上，再买一个商密浏览器，能正常实现商密 HTTPS 加密就算过关了，这是一个仅仅为了勉强“过评”的方案，因为密评的第三个要求是必须确保密码应用的有效性，一个并没有真正在互联网政务应用中实现商密 HTTPS 加密的“过评”就是一个走过场的评测，不满足有效性测评的要求，不是一个真正落实采用商用密码来保证互联网政务应用安全的方案，必将被市场淘汰，因为用户真正所需要的是要保障政务系统安全，保护政务数据的传输安全，而不仅仅是过密评，密评是手段而不是目的。

三、 零信技术商密 HTTPS 加密自动化管理解决方案让密评和密改更容易

零信技术早在 3 年前成立时就已经锚定商密 HTTPS 加密自动化管理解决方案，因为只有自动化才能完美地解决商密 HTTPS 加密改造难题。零信技术创新解决方案是一个端云一体的、零改造、自动化实现商密 HTTPS 加密的解决方案，用户可选：

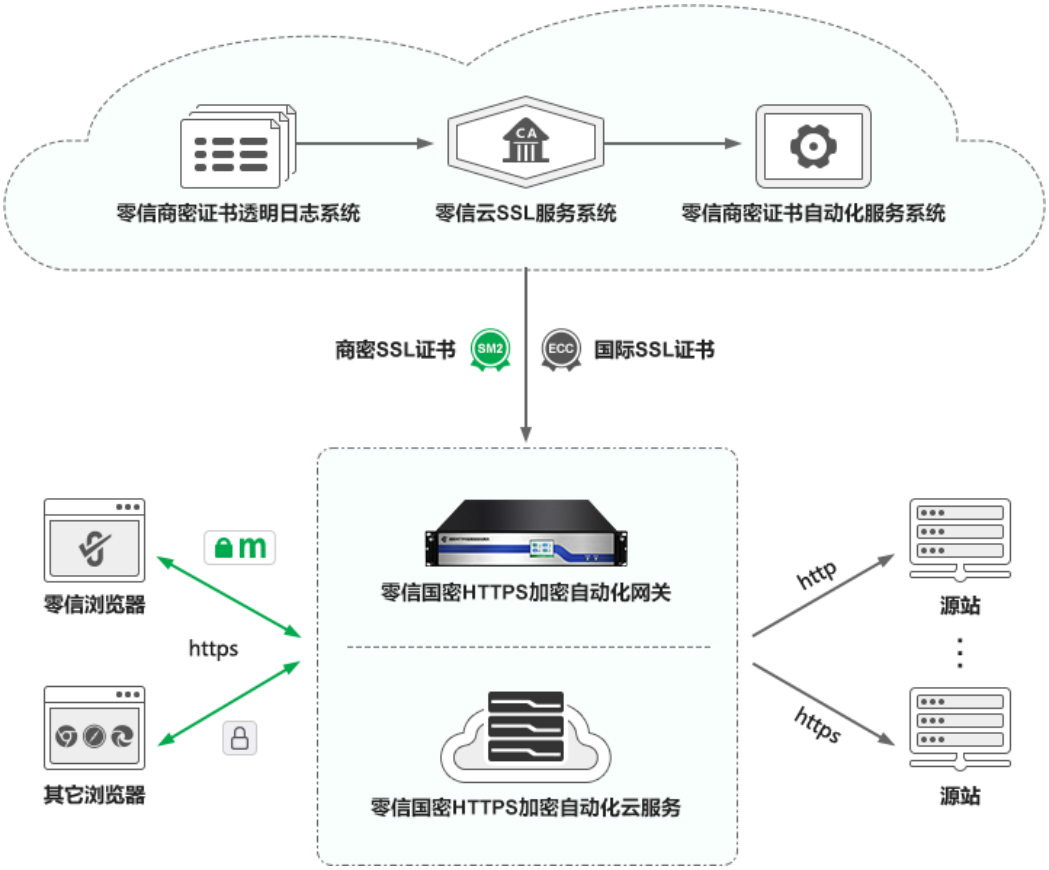
1. 部署零信国密 HTTPS 加密自动化网关

原 Web 服务器零改造，不影响正在运行的业务系统正常为用户提供政务服务，只需在原 Web 服务器前面部署通过商密产品认证的零信国密 HTTPS 加密自动化网关即可，由零信网关自动化对接零信云 SSL 服务系统为用户网站自动化申请商密 SSL 证书和国际 SSL 证书，零信云 SSL 服务系统自动化对接商密 SSL 证书 CA(贵州 CA)和国际 SSL 证书 CA (Sectigo 和上海 CA)的 SSL 证书签发系统，为网关设置的用户网站域名自动化签发商密 SSL 证书和国际 SSL 证书，自动化自适应密码算法实现 HTTPS 加密，满足《规定》的要求。

2. 启用零信国密 HTTPS 加密自动化云服务

仍然是原 Web 服务器零改造，不影响正在运行的业务系统正常为用户提供政务服务，只需选购零信技术部署在全国各地数据中心的通过商密产品认证的零信国密 HTTPS 加密自动化

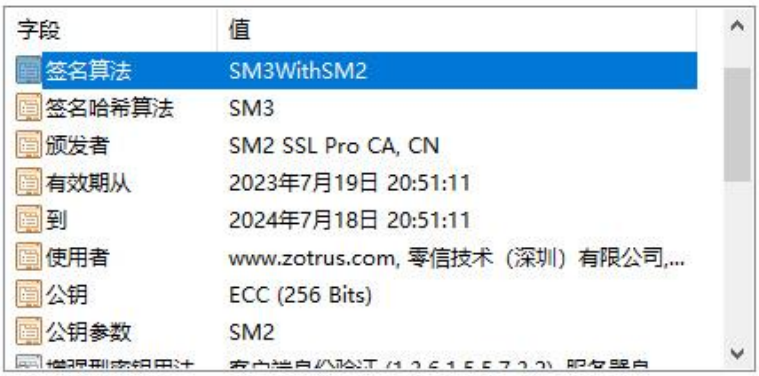
网关所提供 HTTPS 加密自动化云服务即可，无需购买和部署硬件网关，只需做两次域名解析即可快速自动化实现自适应密码算法的 HTTPS 加密，满足《规定》的要求。



3. 免费配套商密浏览器

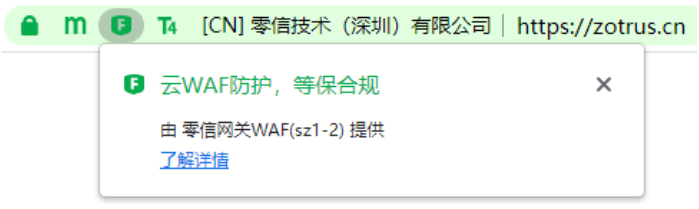
要想实现《规定》要求使用安全连接方式访问互联网政务应用，就得有支持商用密码的浏览器，俗称国密浏览器，但是市场上的国密浏览器都是收费的，这既不符合全球浏览器都是免费的通行规则，也不符合普及商密 HTTPS 加密的应用需求，所以，零信技术为了普及商密 HTTPS 加密，历时两年基于谷歌浏览器内核打造了从底层支持商密算法和商密 SSL 证书、全球独家支持商密证书透明的国密浏览器—零信浏览器，完全免费，干净无广告，实现 SM2/RSA/ECC 三算法的完美支持，优先采用商密 SM2 算法实现 HTTPS 加密访问。

零信浏览器不仅支持商密算法，而且还自动给 Windows 操作系统打商密算法支持补丁，让原先用户无法正常查看商密算法数字证书的 Windows 也能像查看 RSA 算法数字证书一样正常验证、显示和查看商密算法数字证书，包括商密 SSL 证书和商密 USB Key 证书等。这个功能不仅有利于用户查看商密 SSL 证书，而能帮助密评机构验证用户所用的商密数字证书是否合规、是否可信有效。



零信浏览器还有一个创新的 UI 设计就是为密评定制的，那就是地址栏的 **m** 标识，只要互联网政务网站实现了商密 HTTPS 加密，零信浏览器地址栏就会显示商密加密标识 **m**，并显示“商密合规，密保合规”，让网站访问者、网站主办单位、密评机构和密码主管部门都能非常容易地知道这个网站是否采用了商用密码实现 HTTPS 加密，是否正确采用和采用后是否有效，这就是密评所要的结果。对于未能正确部署商密 SSL 证书的网站，零信浏览器会显示为“不安全”，表明这个网站未能正确采用商密技术实现 HTTPS 加密。零信浏览器的这个创新 UI 让密码评测和事后监督更简单。

零信浏览器 UI 还有一个全球独家创新-在地址栏显示 WAF 防护标识 **F**，并显示“云 WAF 防护，等保合规”，让网站访问者、网站主办单位、等保评测机构、密评机构和相关政府主管部门都能非常容易地知道这个网站是否采用了 WAF 防护。零信浏览器能自动识别市场上常用的云 WAF 服务和零信网关 WAF 防护服务，如果网站没有 WAF 防护，或使用了零信浏览器不能识别的 WAF 防护，则零信浏览器不显示 WAF 标识。



4. 自动化让密改不再难，自动化让密改更实在

零信技术商密 HTTPS 加密自动化管理解决方案，是一个创新的端云一体解决方案，端就是零信网关和零信浏览器，云就是零信云密码基础设施，端云紧密配合，让非常棘手的商密 HTTPS 加密改造工作更容易。推荐部署零信网关，为用户提供 5 年不间断的、多达 255 个网站的自动化配置商密 SSL 证书和国际 SSL 证书，自动化为互联网政务应用提供商密 HTTPS 加密服务，让密改不再难，让密改更轻松，让“过密评”和满足《规定》要求合二为一，真正实实在在地采用商用密码来保障互联网政务应用安全。

有诗为证：

密评与时俱进，轻松完成密改。
政务应用合规，当首选自动化。

王高华

2024 年 6 月 17 日于深圳
