解读《互联网政务应用安全管理规定》

昨晚十点，网信办官网和公众号发布了由网信办、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》)，笔者认为这是一件大事，就连夜写了本解读文章，今早上班就交给小编发布，希望不仅对机关事业单位如何尽快满足《规定》要求有所帮助，更重要的是希望能帮助 CA 机构和密码从业者能看到此《规定》中的巨大商机并及时抓住商机，及时帮助所有机关事业单位和关键信息基础设施运行单位及时满足规定的要求。

一、 重点解读与密码相关的八条规定

第一条就非常重要：为保障互联网政务应用安全，根据《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《党委（党组）网络安全工作责任制实施办法》等，制定本规定。也就是说，这是依法做出本《规定》。稍微有点遗憾的是没有列出《中华人民共和国密码法》，不过这不影响其重要意义，因为已经列出的法律和本《规定》中都有《密码法》相关的条款。

第二条则是明确定义了什么是互联网政务应用，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。就是各个以.gov.cn 为域名的政府网站，各个政府部门的官网，同时包括小程序、公众号和电子邮件服务。

第三条则是明确地强制要求互联网政务应用必须采取技术措施和其他必要措施，防范内容篡改、攻击致瘫、数据窃取等风险，保障互联网政务应用安全稳定运行和数据安全。很明显，这就要求政府网站系统都必须实现 HTTPS 加密来保障政务数据传输安全。

这一点可以通过第二十九条来印证：互联网政务应用应当使用安全连接方式访问，涉及的电子认证服务应当由依法设立的电子政务电子认证服务机构提供。“应当使用安全连接方式访问”就是 HTTPS 加密方式访问，而不能是 HTTP 明文不安全连接方式访问，这是必须的。后一句则是明确了这个 HTTPS 加密连接方式所采用 SSL 证书必须由拥有电子政务电子认证服务资质的 CA 机构来提供，这一点绝对是国内 CA 机构的大利好，希望各个 CA 机构及时抓住这个大好机会，及时具备为机关事业单位用户签发商密 SSL 证书和国际 SSL 证书的能力。

第二十八条专门对 CDN 服务提出了要求，结合第二十九条的 HTTPS 加密要求，也就是

说，CDN 必须支持商密 HTTPS 加密，这就是给目前的 CDN 服务提供商提出了更高的安全要求，因为目前只有极个别 CDN 服务提供商支持商密 SSL 证书和支持商密 HTTPS 加密。

不仅仅是第二十九条是 CA 机构的 SSL 证书业务利好，第三十条也是对 CA 机构的传统 USB Key 证书业务的利好：对与人身财产安全、社会公共利益等相关的互联网政务应用和电子邮件系统，鼓励采用电子证书等身份认证措施。

而第三十五条则是明确了对政务电子邮件安全的要求：鼓励机关事业单位基于商用密码技术对电子邮件数据的存储进行安全保护。请特别注意：这里已经明确指出必须采用商用密码技术来实现电子邮件的加密存储，也就是实现电子邮件的端到端加密。

第四十二条则是要求所有列入关键信息基础设施的互联网门户网站、移动应用程序、公众账号，以及电子邮件系统的安全管理工作，参照本《规定》有关内容执行，而不仅仅是机关事业单位的互联网政务应用。

二、CA 机构和密码产业者应该如何抓住商机？

《规定》总共有四十四条，上面重点解读了其中与商用密码相关的八条，非常值得所有 CA 机构和密码产业者好好琢磨，好好体会，从而发掘这其中的巨大商机。笔者特在此基于上面的解读，给大家提供一些发掘巨大商机的思考方向。

第一：实现“安全连接方式访问”的关键密码产品是 SSL 证书，CA 机构必须具备双算法 SSL 证书的可靠供给能力。

双算法 SSL 证书是指商密算法 SSL 证书和国际算法 SSL 证书，Web 服务器必须部署双 SSL 证书，实现自适应加密算法的 HTTPS 加密，才能满足互联网政务应用的公众服务普适性要求。而为了保障 SSL 证书的自身安全可信，国际 SSL 证书都实现了证书透明，商密 SSL 证书也必须实现证书透明，特别是政务应用所需的 SSL 证书，只有透明公示才能保证及时发现错误签发和恶意攻击签发的商密 SSL 证书，才能从加密的源头来保障政务应用的 HTTPS 加密安全。

目前市场上只有零信技术的三个商密证书透明日志系统可供各 CA 机构免费使用，希望有更多的商密证书透明日志系统可用，特别是希望有国家级的更加权威的证书透明日志系统能早日为保障政务应用所需的商密 SSL 证书安全提供权威透明备案公示服务。

第二：既然所有互联网政务应用都必须实现商密 HTTPS 加密，那我们应该思考：用户到底需要什么样的商密 HTTPS 加密解决方案呢？

根据中央编办所属的全国党政机关事业单位互联网网站标识管理服务平台发布的数据，已经发放网站标识的政务网站有 11 万多个，这 11 万多个网站都必须部署商密 SSL 证书来实现 HTTPS 加密，如果采用的传统向 CA 申请 SSL 证书去网站部署，不仅工作量巨大，而且 Web 服务器升级改造难度也很大，这 11 万多个网站很难在本规定的施行之日(7 月 1 日)完成。

唯一的可行的快速实现方案只有自动化，采用商密 HTTPS 加密自动化管理解决方案，这就是零信技术历时 3 年打造的解决方案，用户只需在网站服务器之前部署零信国密 HTTPS 加密自动化网关即可一小时完成网站商密改造，自动化实现商密 HTTPS 加密安全保护，实现使用 HTTPS 安全连接方式访问，满足《规定》的要求。

第三：对于不想部署网关或者没有地方部署网关(如使用云主机服务)的单位，怎么办?

可以选购零信国密 HTTPS 加密自动化云服务，这是一个网上共享网关的解决方案，一样可以为机关事业单位实现商密 HTTPS 加密自动化。而对于需要 CDN 服务的省级政府网站，则可以选购零信国密 HTTPS 加密自动化云服务专业增强版，这是基于阿里云 CDN 加边缘 WAF 打造的商密 HTTPS 加密自动化云服务，自动化实现商密 HTTPS 加密的 CDN+WAF 云服务，用户无需向 CA 申请双 SSL 证书，由云服务自动化配置双算法 SSL 证书，自动化实现商密 HTTPS 加密。

笔者也希望目前各大 CDN 服务提供商都能尽快升级系统为政务用户提供商密 HTTPS 加密 CDN 服务，零信技术可以提供云 SSL 服务和证书自动化管理配套服务，让各个 CDN 都能自动化实现双 SSL 证书的自动化供给和部署。

第四：要求实现互联网政务应用的商密 HTTPS 安全连接方式访问，就需要商密浏览器，怎么办？

《规定》要求互联网政务应用必须采用商密 HTTPS 加密安全连接方式访问，则需要支持商密算法的浏览器来安全访问政务网站。完全免费的商密浏览器--零信浏览器就可以发挥大作用了，零信浏览器不仅完全免费的、干净无广告，而且支持商密证书透明，优先采用商密算法实现 HTTPS 加密，同时兼容 RSA 算法 HTTPS 加密，完全能满足普及应用商密算法访问政务服务网站的要求。普及商密 HTTPS 加密，需要完全免费的商密浏览器。这就像 RSA 算法 HTTPS 加密在全球普及使用一样，完全免费的四大浏览器起到了非常重要的作用。

希望市场上有更多的完全免费的、无广告的商密浏览器，共同助力普及商密 HTTPS 安全连接方式访问政务应用，从而真正实现“保障互联网政务应用安全稳定运行和数据安全”的目标。

三、《规定》就是互联网政务应用的中国零信任战略

美国管理和预算办公室 (OMB) 于 2022 年 1 月 26 发布了《联邦零信任战略》(Federal Zero Trust Strategy)，该战略对美国互联网政务应用提出了零信任安全五大目标和行动计划，对政务应用的身份安全、设备安全、网络安全、应用安全和数据安全提出了具体要求，其中最核心的要求也是要求所有政务应用都必须强制实现 HTTPS 加密，并且只能是 HTTPS 加密方式访问，而且还特别强调无论是互联网政务应用还是内网政务应用，都需要 HTTPS 加密。同时也明确要求了加密 DNS 服务和电子邮件加密服务。

由此可见，《规定》可以理解为就是我国互联网政务应用的零信任战略，并且是必须采用商用密码来保障我国互联网政务应用安全和关键信息基础设施安全的战略，这不仅将有力保障我国互联网政务应用的安全，为老百姓提供安全可靠的政务服务，而且将大大推动商用密码在我国互联网的普及应用，使得各行各业都能普及应用商用密码来保障我国网络空间安全可信。

王高华

2024 年 5 月 23 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 167 篇(共 45 万 3 千多字)和英文 66 篇(8 万 1 千多单词)。。