90 天 SSL 证书对策一：政务篇

90 天 SSL 证书的倒计时开始了，我国做好准备了？该如何应对国际标准将把 SSL 证书有效期从目前的 1 年缩短到 90 天，笔者将针对四个不同的行业提出相应的对策，分四篇：政务篇、企业篇、云平台篇和 CA 篇，先写政务篇，因为政务系统数据传输加密最重要。

一、网上政务服务，让人民获得感满满

从“群众跑来跑去，领导批来批去，部门转来转去”到“最多跑一次”；从“门难进、脸难看、事难办”到阳光、规范的标准化政务服务；从“一站式办结”到“一网通办”。改革开放 40 多年来，我国政务服务效能提升的轨迹，可感可触。有了网上政务平台，个人在线填写表单、上传材料，政务大厅网上受理和审批，证照结果直接快递到家。网上政务平台应用范围还在不断拓展，覆盖全国甚至海外，并且在应用体验和效率提升方面不断深度优化。可以说，网上政务服务不只是打通服务人民群众的“最后一公里”，而是逐渐变成服务的“零距离”，这折射出了政府“让群众少跑腿，让信息多跑路”的理念和实践。

二、电子政务云平台，为网上政务服务提供一体化一站式算力服务

电子政务云平台是指结合了云计算技术的特点，对政府管理和服务职能进行精简、优化、整合，并通过信息化手段在政务上实现各种业务流程办理和职能服务，为政府各级部门提供可靠的基础 IT 服务平台。

电子政务云是为政府部门搭建一个底层的基础架构平台，把传统的政务应用迁移到云平台上，共享给各个政府部门使用，提高其服务效率和服务能力。

各地的电子政务云平台是根据全国一体化大数据中心体系布局整合算力资源，为政府部门提供绿色集约、共享共用、安全可靠的一体化算力服务，为经济运行、政务服务、市场监管、社会治理的政务履职提供技术支撑，是落实政府“让群众少跑腿，让信息多跑路”的理念的技术保障。

三、电子政务云平台的核心安全是全面实施 HTTPS 加密

政务云平台除了投资建设机房、网络设施、服务器、软件系统、网络防护设备、带宽等基础设施外，最核心的安全建设就是全面实施 HTTPS 加密，而这一点却往往被忽视了，因为政务云平台的规划和建设仍然是基于自家机房建设的思路，仍然是几十年来固有的单位内网建设思路，仍然是城堡加固的思路。所以，在规划建设时仍然是大量采购传统的网络安全设备如防火墙、杀毒、IDS、IPS、WAF 等，而遗漏了更重要的密码应用的投资规划。

其实，政务云平台不是一个内部网，是一个跨区的城域网，是一个跨市的省域网，是一个跨省的国域网，实际上同公共云平台一样就是一个互联网云平台，只不过是政府单位专用而已。理清这个思路就不会只关注政务云平台机房的安全防护，也就是只关注城堡的防护。政府“让群众少跑腿，让信息多跑路”的理念就是要让数据流动起来，数据从群众的手机和电脑跑到政务数据资源中心的服务器中，那就必须要保护数据在跑腿的路上的安全。这是政务云平台安全的关键，而不是仅仅保护政务云平台机房设备的安全而已。这是一个政务云平台建设的安全理念需要更新的要务，大家天天讲云服务、云计算，但是安全防护仍然停留在城堡防护思路上，这是跟不上目前形势的，重点是要保证数据从群众手中产生到政务数据资源中心的传输安全。因为无法控制群众使用数据的网络环境是否安全，唯一能做的是实现数据传输链路加密，这就是 HTTPS 加密。

准确理解了这一点，大家就不难理解美国政府《联邦零信任战略》对 HTTPS 加密的苛刻要求了，不仅要求所有政府网站系统必须实现 HTTPS 加密，而且同常用的浏览器厂商合作预置要求浏览器在访问所有.gov 域名的政府网站时只能使用 HTTPS 加密协议访问，不能使用不安全的明文传输协议 HTTP 访问。这是一个保护用户数据在途中安全的闭环实现，确保了用户数据只能通过加密通道传输到政务系统中，这一点非常值得我国政务云平台借鉴。

而我国要实现 HTTPS 加密必须是采用商用密码算法实现，不能采用 RSA 密码来实现，这就加大了实现 HTTPS 加密的难度，本来只需采购 SSL 证书部署在 Web 服务器上即可实现 HTTPS 加密，但是现有的系统都只需支持 RSA 密码体系，不支持商密体系。这就要求“国密改造”，改造 Web 服务器支持国密算法和国密 SSL 证书，但由于改造难度很大，导致了现在的大量的政务系统仍然是 HTTP 明文传输方式让群众数据在跑腿的路上“裸奔”。采用 RSA 密码不合规，而采用商用密码又很难，这是所有政务云平台建设者面临的“两难”难题，两难的结果是既没有实现最基本 RSA 算法 HTTPS 加密，也没有实现必须的国密算法 HTTPS 加密，这就是目前大量的政府网站和政务系统仍然在“裸奔”群众数据的主要原因。

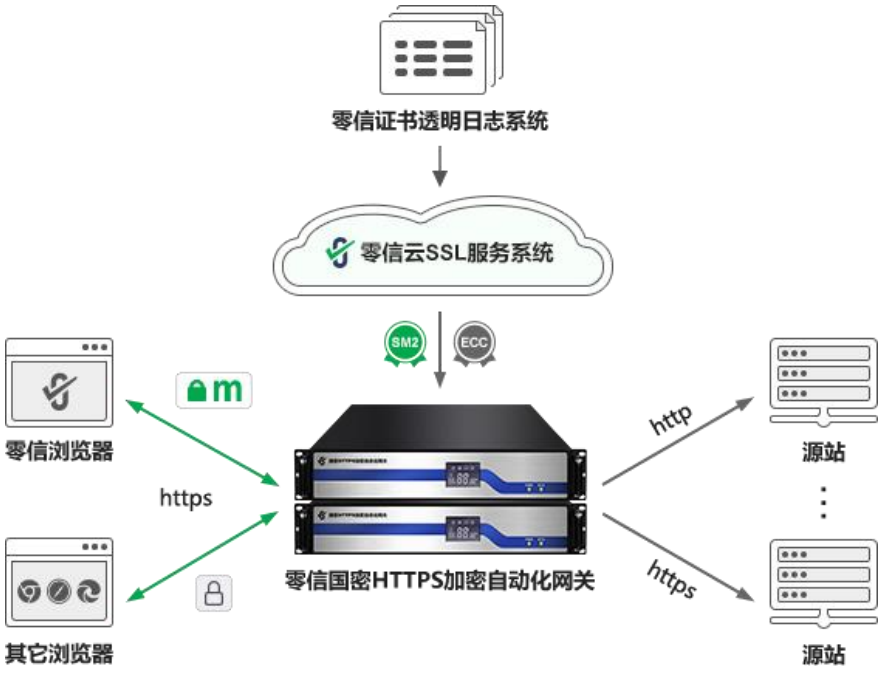
必须强调的是，不只是浏览器访问 Web 系统才需要 HTTPS 加密，常用的政务 APP 也是同

浏览器一样的客户端软件，一样必须采用 HTTPS 加密连接政务服务器，才能保证用户数据从政务 APP 到政务服务器之间的传输安全，并且政务 APP 必须采用浏览器一样的严格检查 SSL 证书是否可信、是否过期、是否被吊销和是否正确绑定了需要访问的网址，也必须支持国密算法实现国密 HTTPS 加密。

四、全面实现商密 HTTPS 加密的唯一可行方案是部署国密 HTTPS 加密自动化网关

虽然政务云平台的 HTTPS 加密基础通信安全面临两难的局面，但是政务云平台建设者们仍然还是在努力前行，根据《中国 SSL 证书市场发展趋势分析简报-2023Q3》的数据，我国.gov.cn 域名的国际 SSL 证书的申请量是 16282 张，而根据全国党政机关事业单位互联网网站标识管理服务平台的统计数据，已发放标识总量达到 113004 个，也就是说至少有 11 万多个政府网站在互联网上可访问，这些可访问的网站都应该部署 SSL 证书实现 HTTPS 加密，但是证书申请总量只有 16282 张，只是网站数量的七分之一**(14.41%)**，为何这么低呢？当然不是经费问题，是部署 SSL 证书实现 HTTPS 加密太难了。

是否有一个解决方案彻底解决“两难”的难题？当然有，这就是零信技术全球独家推出的国密 HTTPS 加密自动化解决方案。用户无需向 CA 申请国际 SSL 证书和国密 SSL 证书，无需在原 Web 服务器上安装 SSL 证书，也无需在服务器上安装 ACME 客户端软件，原 Web 服务器无需升级改造支持国密算法，什么也不用动，不改动目前的国际密码体系中的业务系统，只需在原服务器之前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，直接一步到位自动化实现国密 HTTPS 加密。



这是突破了“国密改造”传统思路的解决方案，国密改造很难，那就不改造，保留现有的基于国际密码体系的用户端系统和服务端业务系统，由网关来自动化对接零信云 SSL 系统，自动化为网站域名配置双算法双 SSL 证书，双证书全部支持证书透明，由网关来实现国密加密算法到国际加密算法和明文 HTTP 的协议和算法转换，提供类似于 CDN 或 WAF 的 HTTPS 加密卸载转发服务。

零信技术这个创新解决方案是一个端云一体的解决方案，有两个“端”，一个是零信网关，部署在服务器端，另一个是零信浏览器，在用户端免费使用，为用户提供端到端的国密 HTTPS 加密通道，让群众的数据从产生就通过国密加密通道安全地“跑路”到政务云数据中心服务器中，这不仅是国密合规的要求，更重要的是保证了政务数据不会在“路”上被打劫，不会被非法窃取和非法篡改，让群众不仅不用跑腿把事情办了，而且是不以泄露群众个人数据为代价的少跑腿，是能让人民群众真正享受安全的政务服务的少跑腿，只有这样才能真正让老百姓有幸福感和获得感，否则群众一上政务系统办事马上就有推销电话来骚扰群众，这不是老百姓所要的少跑腿，因为如果不实现网站 HTTPS 加密，那么群众的电话号码和个人敏感数据就非常容易在数据跑腿的路上被泄露。如果政务服务不是标准的 B/S 架构，而是 App/S 架构，则政务 APP 也必须同时支持国密 HTTPS 加密。

只有让政务云平台所有服务器实现国密 HTTPS 加密，才能真正使得政府“让群众少跑腿，让信息多跑路”的理念安全地落地，让老百姓幸福感和获得感满满，确保在目前的不确定的国际形势下的电子政务服务能可靠地不中断地为老百姓提供安全的网上政务服务。

有诗为证：

网上政务服务，让人民群众能少跑腿。

让信息多跑路，政务平台建设是关键。

电子政务平台，为政务提供算力保障。

政务核心安全，数据多跑路全程加密。

国密加密网关，零改造实现数据加密。

网关自动加密，不间断可靠政务服务。

商用密码应用，保障政务系统的安全。

群众数据安全，幸福感和获得感满满。

王高华

2023 年 10 月 19 日于深圳

请关注公司公众号，实时推送公司 CEO 精彩博文。