美国政务云平台 HTTPS 加密应用研究与启示

俗话说：他山之石可以攻玉。本文通过分析互联网公开信息所获取的美国政务云平台 HTTPS 加密应用情况，得出了可供我国政务云平台 HTTPS 加密应用借鉴的非常有参考价值的一些深度思考，并提出了一个适合我国国情的创新解决方案，可供相关产业机构、市场分析机构和政府部门规划决策参考。

一、 美国政务云平台简介

根据美国政务云官网 cloud.gov 介绍，cloud.gov 是一个安全合规的平台即服务。Cloud.gov 帮助联邦政府机构以更快、以用户为中心的方式为公众提供政务服务。Cloud.gov 使得联邦政府机构能够专注于为用户提供政务服务，而无需管理底层服务基础设施。Cloud.gov 内置合规性支持可帮助联邦政府机构创建合规政务服务并持续保证合规。Cloud.gov 同时为用户提供平台即服务(PaaS)和合规即服务(CaaS)。

Cloud.gov 由美国总务管理局(U.S. General Services Administration) 的技术转型服务组合中的一个团队构建和维护。Cloud.gov 是一项成本可收回的服务，通过向使用其服务的联邦机构收取费用来筹集资金。其使命不仅是让政府机构更容易采用云部署，使政府机构能够快速向公众提供服务，同时是以最少的工作量实现政务应用安全性和合规性方面的最佳实践。

值得注意的是，cloud.gov 提供的政务云服务是在商业云基础设施提供商亚马逊的云服务基础上提供的政务云服务，而不是自建政务云基础设施，这能节省大量的基础设施投资，同时由于集中采购也会比各个政府机构单独采购商业云服务更节省费用。

二、 美国政务云平台 HTTPS 加密应用研究

互联网政务平台的一个最主要的应用是 Web 服务，最重要的安全保障措施就是 HTTPS 加密。美国政府早在 2015 年 6 月 8 日就由总统管理和预算办公室(OMB)执行办公室发文《M-15-13》，要求所有联邦政府网站和电子政务服务建立 https 安全连接，并给出了时间表—各联邦政府机构必须在 2016 年 12 月 31 日之前为所有网站和服务启用安全连接(HTTPS)，并支持 HSTS(强制 HTTPS)。

Cloud.gov 最早于 2015 年 12 月开始测试使用 Let’s Encrypt 提供的免费 90 天 SSL 证书自动化管理服务，直到 2023 年 4 月 6 日才正式为美国政府门户网站 www.usa.gov 启用 SSL 证书

自动化管理服务，这个 HTTPS 加密自动化实施过程历时 8 年完成。可以说，美国政务云的 SSL 证书自动化过程是同全球商业网站的自动化过程几乎是同时开始，并在 SSL 证书自动化化系统非常成熟时适时启用，非常有远见和有魄力。笔者于 2017 年 3 月在由思科(北卡罗来纳州)承办的 CA/浏览器论坛春季工作会议上聆听了美国政务云的运营负责人 Eric Mill 的演讲，当时就真实感受到了美国政务云在推动强制 HTTPS 加密的决心和信心，回国后也写了相关的文章。当时还只是在推动普及 HTTPS 加密，而 SSL 证书自动化管理也就是顺理成章的事情，因为要想普及 HTTPS 加密，如果没有自动化是无法实现的。

我们再看看 www.usa.gov 部署的 SSL 证书是什么样的，如下图所示，这是一张由 Let's Encrypt 自动化签发 90 天免费 SSL 证书。Cloud.gov 采用第三方开源供应商 Let's Encrypt 签发的全球信任 SSL 证书，自动化实现 HTTPS 加密。一旦所需 SSL 证书由 Let's Encrypt 签发，就会将它们自动上传到面向公众服务的负载均衡器上。

如下图所示，这是从国际证书透明日志系统查到的 www.usa.gov 申请的 Let's Encrypt 免费 90 天 SSL 证书的申请时间表，从 2023 年 4 月 6 日起，每 60 天就自动续期，虽然 SSL 证书有效期为 90 天，但已经提前安排续期，以免 CA 系统由于各种原因导致的无法签发证书而影响 HTTPS 加密正常运行。可以看出，美国政府官网从 2023 年 4 月 6 日正式启用 HTTPS 加密自动化服务，已经连续实施了将近两年时间，在此之前网站部署的是一年期 Sectigo SSL 证书。

证书申请日期	2023/4/6	2023/6/5	2023/8/4	2023/10/3	2023/12/2	2024/1/31	2024/3/31	2024/5/30	2024/7/29	2024/9/27	2024/11/26	2025/1/26
两次相隔天数		60	60	60	60	60	60	60	60	60	60	60

大家可以使用零信浏览器访问美国政府官网，显示效果如下图所示，不仅会显示加密锁标识，而且还会显示绿色地址栏和显示“美国政府”，这是网站部署了 EV SSL 证书所显示的效果，为何此网站部署的是仅验证域名的 DV SSL 证书但显示 EV SSL 证书效果呢？这是因为此网站通过了零信浏览器的 EV 认证，以弥补 DV SSL 证书的身份缺失问题。显示中文“美国政府”则是零信浏览器 EV 认证支持中英文，中文版本显示中文单位名称，其他版本则显示英文单位名称。

另一个更值得注意的是 WAF 防护标识 F (由 Cloud.Gov WAF 提供)，表明美国政府网站已经启用云 WAF 防护，并且这个 WAF 防护是由美国政务云自己提供的，这个是重点。大家都知道，WAF 防护工作原理是从源站回源、SSL 卸载流量分析、拦截恶意流量、转发正常流量的 Web 安全防护服务，这个重要的服务由美国政务云平台自建 WAF 服务来提供而不是商业第三方服务，这与 SSL 证书使用第三方 CA 说明了 WAF 防护更重要，涉及到政务数据的安全流通。

不仅仅是美国政府有政务云平台，英国政府也有- **GOV.UK Digital Service Platform** (英国政府数字服务平台)，正在为超过 1500 个英国政府机构提供服务，并且也一样是自己提供类似美国政务云一样的自建云 WAF 防护服务(由 Govuk Service WAF 提供)。

三、 美国政务云平台 HTTPS 加密应用对我国政务云平台建设的启示

笔者在前两段较为详细地介绍了美国政务云平台 HTTPS 加密的应用情况，包括 HTTPS 加密方式的 WAF 防护情况，其目的当然是希望能对我国政务云建设有所借鉴和启示作用。笔者有如下三个方面的观察和体会供参考。

第一：法规先行，切实执行。

美国政务云全部实现强制 HTTPS 加密，执行的是总统管理和预算办公室(OMB)执行办公室的文件要求。我国的力度更大，不仅有《密码法》，而且有各部委多次联合发文，特别是 2024 年 7 月 1 日施行的《互联网政务应用安全管理规定》，但为何现在的政务网站 HTTPS 加密普及率不到 20%呢？问题还在难在 RSA 密码体系的 SSL 证书申请和部署受制于人，并且也不放心使用，因为已经发生过俄罗斯政府网站 SSL 证书被恶意吊销和断供的安全事件。而要想普及

应用国密 SSL 证书实现国密 HTTPS 加密就需要所有系统都支持国密算法，都需要完成国密改造，这个执行难度更大，需要找到更快更好的技术解决方案。

第二：自动化是唯一正确之道。

美国政务云在全力推动普及应用 HTTPS 加密时，一定是遇到了瓶颈，因为需要在成千上万台服务器上人工申请和部署 SSL 证书的工作量是可以想象的，所以其运营团队很早就开始测试和实施 SSL 证书自动化管理，从证书透明日志系统的数据可以看出，从 2015 年 12 月开始就一直在多个政府网站测试和实施 SSL 证书自动化管理技术方案，最终于 2023 年 4 月正式为美国政府官网实现了 HTTPS 加密自动化。

这也是我国政务云平台必须走的技术路线，当然可以先实现 RSA 密码算法的 SSL 证书自动化管理，但是这是一个需要在 Web 服务器上安装第三方软件的解决方案，也许政务云主管们并不放心这个国外的第三方软件，也许这些重要的 Web 服务器根本就不允许安装任何第三方软件。这可能就是为何我国政务云平台并没有普及采用这个技术方案的主要原因，目前已经部署了 SSL 证书的政府网站中，有 10%左右的县级政府网站实现了 Let’s Encrypt 的 RSA 算法 SSL 证书自动化方案。

为了合规安全，我国政务云平台要实现的是国密 HTTPS 加密自动化，国密 SSL 证书和国际 SSL 证书的双证书自动化管理，这就需要零改造的技术方案，需要不改造现有 Web 服务器的方案，目前市场上唯一已验证并开始实施的技术方案就是零信技术独家率先提出的国密 HTTPS 加密自动化管理解决方案，只需在 Web 服务器前部署零信国密 HTTPS 加密自动化网关即可，自动化实现国密算法 HTTPS 加密，并兼容支持 RSA/ECC 算法，只有这样才能普及实现 HTTPS 加密。

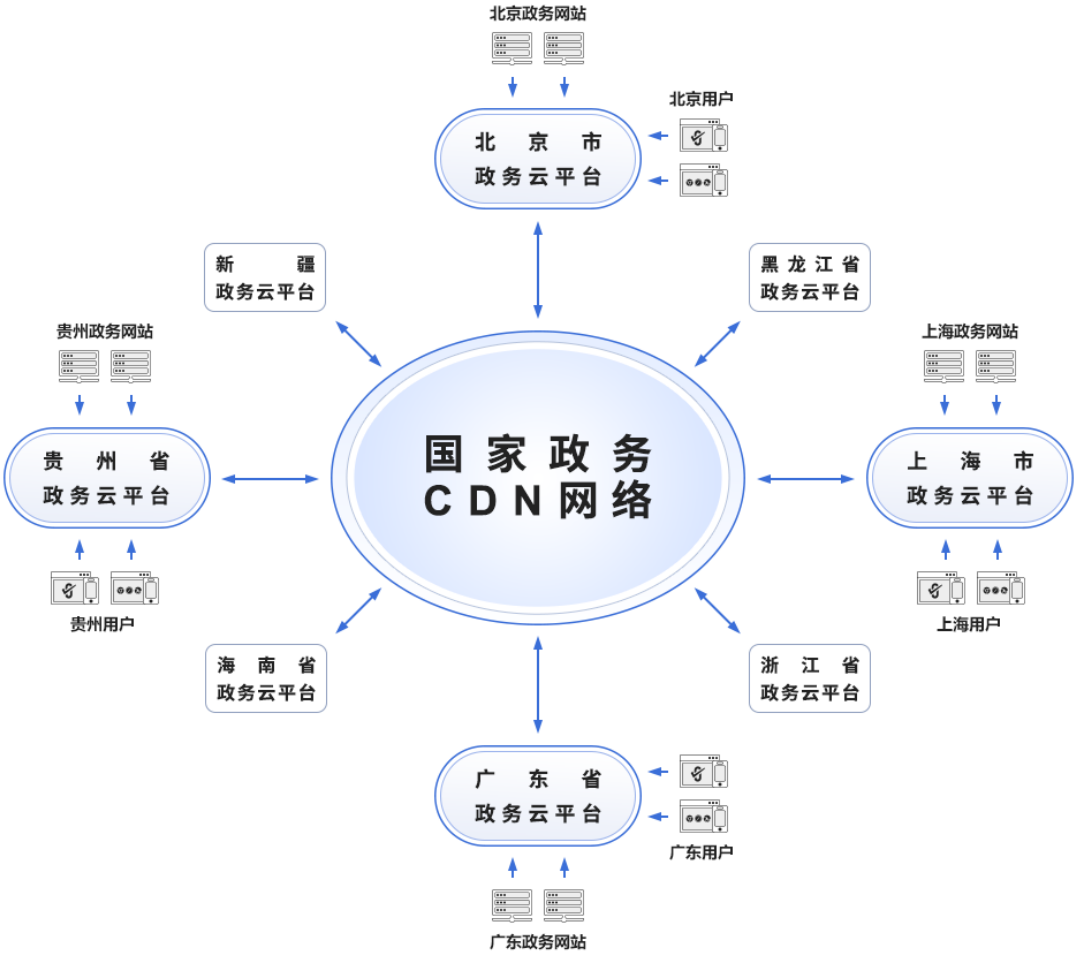
第三：HTTPS 加密和 WAF 防护同步实施

网站安全不仅仅需要 HTTPS 加密，还需要 WAF 防护，但是这个 WAF 防护不是使用第三方的云 WAF 服务，而是应该像美国政务云平台一样采购 WAF 设备建设自己的云 WAF 防护，这是为了切实保障 WAF 防护中的政务数据安全。当然，必须是自动化国密 HTTPS 加密方式下的 WAF 防护，因为 WAF 设备需要支持国密算法卸载 SSL 加密流量，同时需要 HTTPS 加密自动化和 WAF 防护自动化。

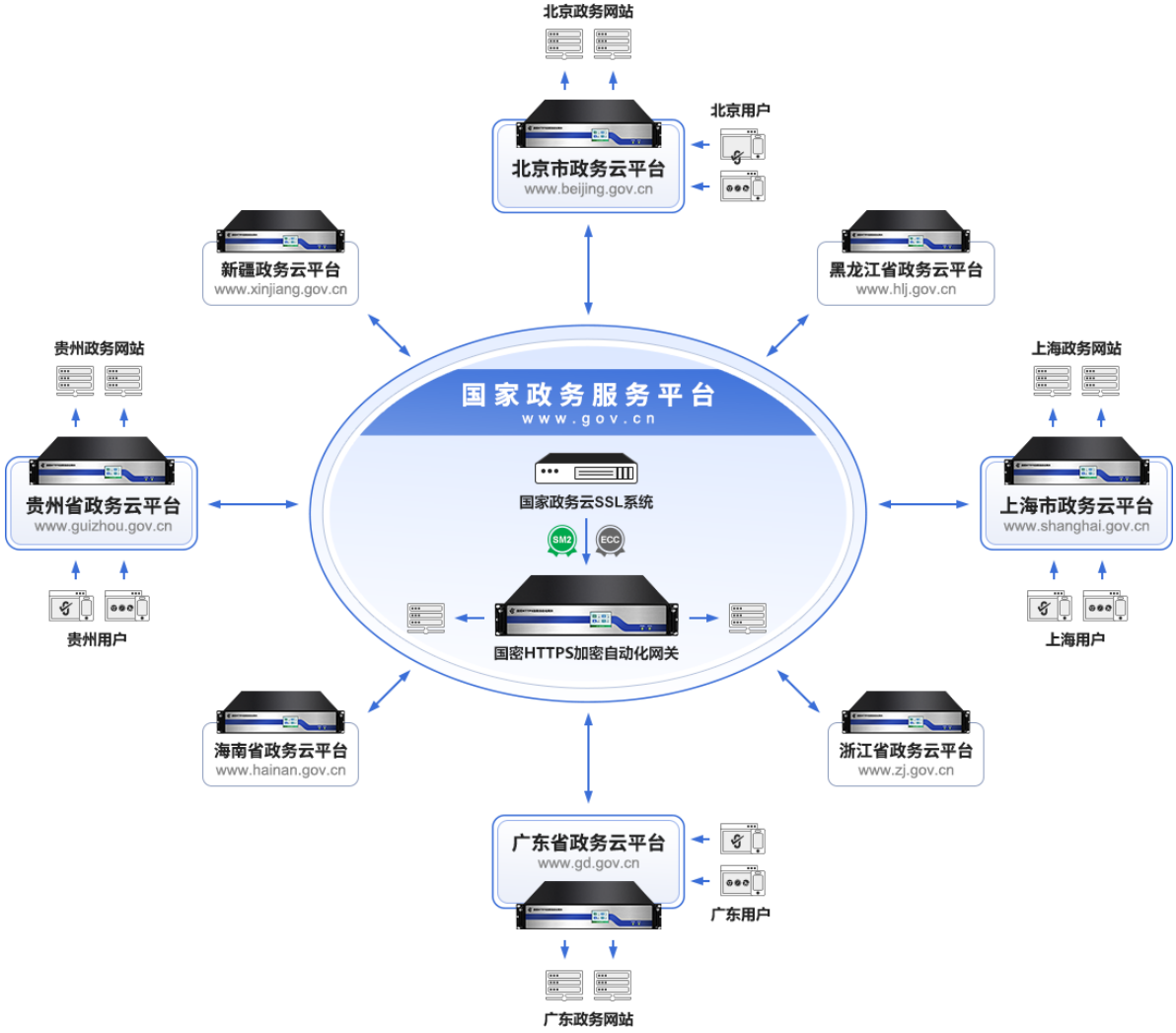
四、建设全国一体化 HTTPS 加密+WAF 防护+CDN 分发的国家政务服务平台势在必行

这是笔者从美国政务云平台建设情况中悟出的一个新思路，我国已经建设了国家政务服务平台，各个部委和各省市自治区也都建设了省级政务服务平台，但是目前都是各自建设管理，并没有发挥其整体优势，中国政府官网和国家政务服务平台以及各省政府官网和省政务服务平台都在各自购买商业 CDN+WAF 防护服务，这不仅不能切实保障政务数据的安全，而且浪费了大量的系统运维费用。

更优的解决方案是基于全国各地的政务服务平台建设全国一体化的 HTTPS 加密+WAF 防护+CDN 分发的国家政务服务平台，各省市的政务服务平台就是一个国家政务专用 CDN+WAF 服务节点，从而构成一个能真正保障政务数据安全的政务专用 CDN 网络，而无需再花钱使用商业 CDN 网络。每个省政务云平台既为本省用户提供本地化政务服务，同时又是全国其他省市和国家政务云平台的 CDN 服务节点，为其他省政务用户提供本地快速安全分发服务，让政务数据不是在商业 CDN 网络上流通而是在政务专用 CDN 网络中安全流通，只有这样才能真正切实保障政务数据安全。



这个政务专用 CDN 网络根本无需再投入一分钱，只需重新规划形成一个 CDN 服务网络即可，这样再也不需要花钱去购买商业 CDN 服务了，不仅省钱而且更加安全，让政务数据只在政务 CDN 网络上安全流通，而不是像现在那样在商业 CDN 网络上流通。而要保障安全流通，就必须支持国密 HTTPS 加密和 WAF 防护，这就需要自动化配置国密 SSL 证书和国际 SSL 证书，自动实现自适应密码算法的 HTTSP 加密和 WAF 防护。目前唯一可行的技术方案就是在国家政务云平台和各省政务云平台增加部署国密 HTTPS 加密自动化网关，这样就是实现了全国一体化的国密 HTTPS 加密+WAF 防护+CDN 分发的国家政务服务平台，为全国用户提供快速安全的政务服务。



同时，为了节省国密 SSL 证书和国际 SSL 证书费用和自主可控，推荐自建国家政务云 SSL 系统，设立国密算法政务专用 SSL 根证书和定制全球信任的国际 SSL 中级根证书，由国密 HTTPS 加密自动化网关自动化对接国家政务云 SSL 系统，自动化为全国所有政务网站签发双算法 SSL 证书，自动化实现自适应算法的 HTTPS 加密自动化和 WAF 防护。当然，由于实现了 SSL 证书自动化，就可以实现像美国政务云一样的 SSL 证书密钥的每 60 天更新一次，确保

密钥安全和 HTTPS 加密安全。

这是一个真正的全国一体化国家政务服务平台，一个集 HTTPS 加密自动化、WAF 防护自动化、CDN 分发自动化于一体的国家政务服务平台，不仅节省大量的购买商业 CDN/WAF 服务的费用，节省大量的购买 SSL 证书费用，更重要的是能快速完成所有政务系统的国密改造和 IPv6 改造，切实保障政务数据只在政务专用 CDN 网络流通，真正实现普及商用密码来保障我国政务数据安全，真正切实保障个人和企业机密信息安全，真正让人民群众在信息化发展中有更多的获得感、幸福感和安全感。

王高华

2025 年 2 月 5 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 201 篇(共 58 万 5 千多字)和英文 84 篇(10 万 9 千多单词)。