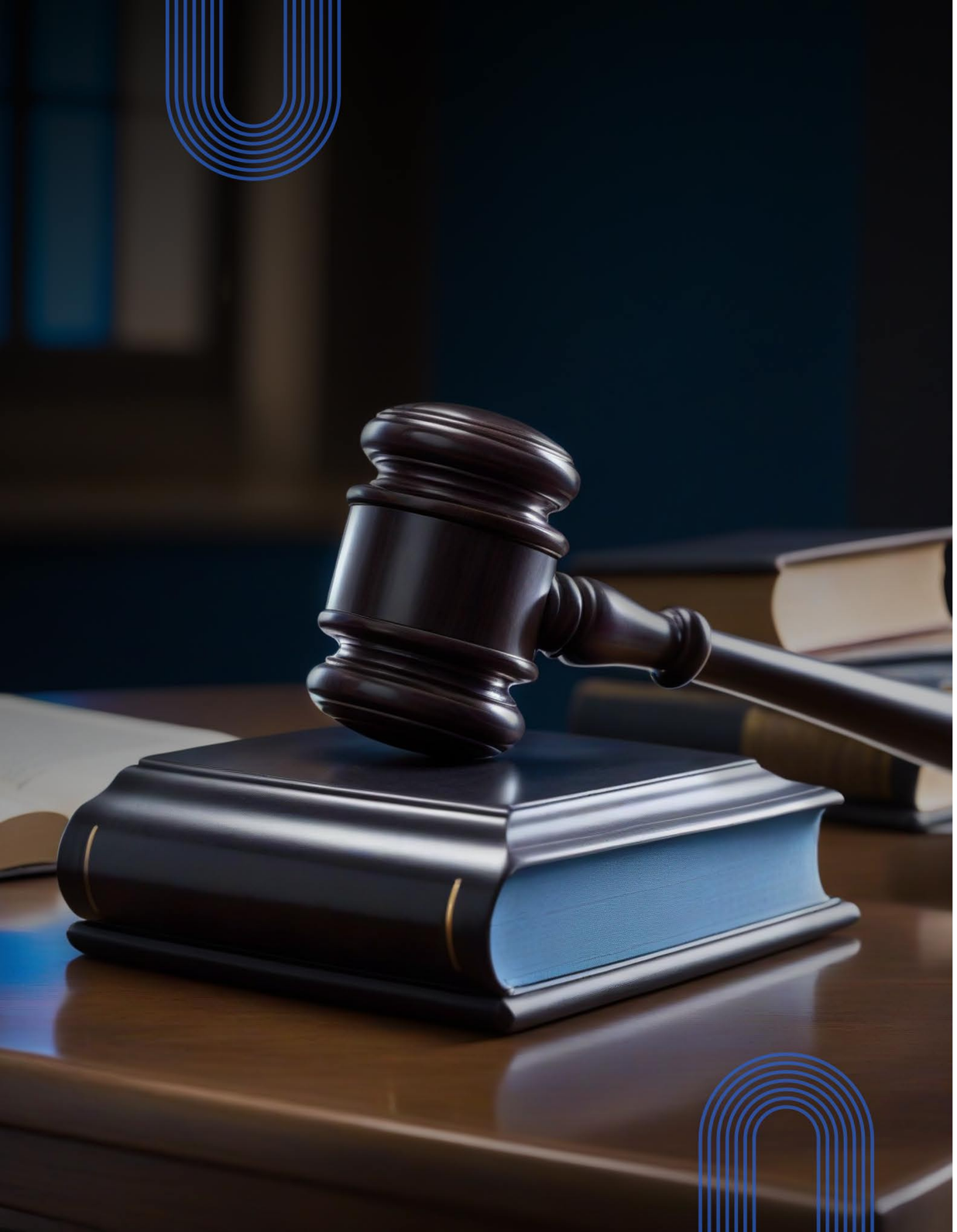
零信®
ZoTrus

互联网政务应用系统升级改造方案

一个网关搞定四个棘手的政务应用系统升级改造难题

https://www.zotrus.com



2024年7月有两个非常重要的网站安全管理规定正式实施，一个是网信办联合中央编办、工信部和公安部四部委联合发布的《互联网政务应用安全管理规定》(以下简称《规定》)于2024年 7月1日 起施行，第二个是国家密码管理局发布的《国家密码管理局商用密码随机抽查事项清单（2024年版）》(以下简称《清单》)公告于2024年 7月19日 起施行。工信部联合八部委于2024年 4月20日 印发了《关于推进IPv6技术演进和应用创新发展的实施意见》，要求在2025年底初步形成以IPv6演进技术为核心的产业生态体系，进一步推动基于“IPv6+”的网络安全产品和服务在政府、电信、金融等重点行业普及应用(以下简称《实施》)。

《规定》和《清单》是关于互联网政务应用安全的到目前为止最为严格的要求，可以理解为这是摆在政府网站和政务应用系统IT主管们面前的最为棘手的必须尽快解决的难题。而《实施》则是在还没有按《规定》和《清单》完成基于IPv4的政务应用安全改造的情况下，又要求完成基于IPv6的改造，这个双重改造任务是压在各级政府机关事业单位IT部门的重担。

本解决方案先解释落实这三个文件规定的难度在哪，再给出真正能多快好省地为政府用户解决这些棘手的难题的最佳方案。

一、《规定》、《清单》和《实施》为政务应用安全提出了哪些要求？

首先，《规定》是如何界定互联网政务应用的？哪些单位和哪些应用受《规定》的约束。《规定》第二条 “各级党政机关和事业单位（简称机关事业单位）建设运行互联网政务应用，应当遵守本规定”，这一条明确了所有政府机关和事业单位的官网和其他可以通过互联网访问的政务服务系统都受《规定》的约束。到底是哪些网站？第五条明确了党政机关网站必须以“.gov.cn”或“.政务”为后缀，事业单位网站必须以“.cn”或“.公益”为后缀，也就是这些域名的网站都必须遵守此《规定》，这是规定了适用范围。

《规定》还明确定义了什么是互联网政务应用，那就是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：凡是能通过互联网访问的政府官网、事业单位官网、所有政务服务系统和政务电子邮件系统都受此《规定》约束。但请注意：《规定》第四十二条明确了“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”，虽然这些单位可能不是机关事业单位，但是只要属于关键信息基础设施，一样受《规定》约束。

互联网政务应用就是用户可以通过浏览器或APP浏览政务信息和办理各种政务服务的服务系统，是通过HTTP或HTTPS协议实现的互联网Web应用。《规定》第二十九条要求应当使用安全连接方式访问互联网政务应用，这就是要求网站必须实现全站HTTPS加密，而不是不安全的HTTP明文方式。《规定》同时规定政务网站系统必须使用电子政务电子认证服务机构签发的商密SSL证书来实现HTTPS加密方式访问，也就是HTTPS加密必须同时支持商密算法和国际算法，不能仅仅部署国际SSL证书。《规定》第十七条要求政务应用通过等保三级认证，必须有Web应用安全防护，也就是必须购置WAF设备或云WAF服务来保障政务Web应用安全。一句话就是：互联网政务应用安全的核心是 HTTPS加密 和 WAF防护。

《规定》要求所有政务应用都必须使用商用密码实现HTTPS加密安全连接，而随后发布的《清单》则是《规定》的后续检查监督工作，检查这些政务应用是否采用了商用密码进行保护，是否正确采用和采用后是否有效，最厉害的是随机抽查，凡是《规定》约束的网站系统都有可能被抽查到，而如果被查到有违法行为，不仅是可以依据《密码法》最高罚款100万元，而且还可以依据《规定》第四十一条“对违反或者未能正确履行本规定相关要求的，按照《党委（党组）网络安全工作责任制实施办法》等文件，依规依纪追究当事人和有关领导的责任”，也就是既会有罚款还会有行政处罚。

这就是7月份连续出台的两个政府文件的联动呈现的执法力度，这些要求比美国政府签发的总统行政命令要求政府网站都必须实现HTTPS加密的力度还要大，并且对于被抽查单位来讲，执行难度更大，因为实现国际算法HTTPS加密要比实现国密算法HTTPS加密要容易得多。

而4月份出台的《实施》结合7月份出台《规定》和《清单》，则是要求政务应用系统不仅必须在现有的IPv4网络中实现所有政务应用系统的国密HTTPS加密，同时还要求在IPv6网络中实现。这就给互联网政务应用安全又增加了一倍工作量，也许还是双倍的系统建设投资和系统维护。

二、 政务应用系统为何急需升级改造？有哪些需要改造的？

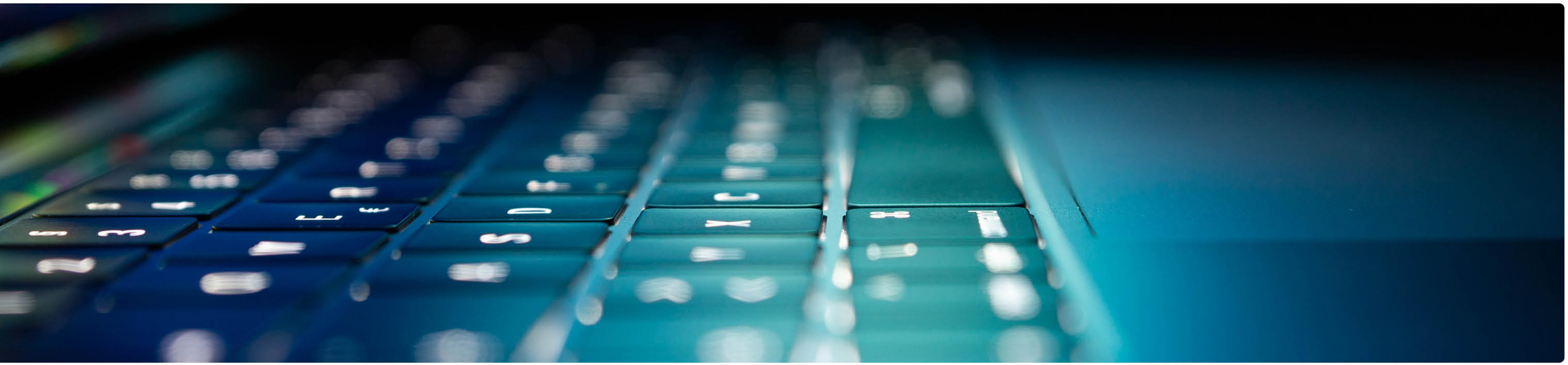
我国的政务应用服务系统经过这么多年的不断建设和完善，已经基本上实现了满足用户网上办理各种政务业务的需要，特别是手机政务APP和小程序的普及使用，极大地方便了老百姓使用政务应用服务。但是，由于用户的网络使用环境非常复杂，无法保证网络环境是可信的，用户的电脑环境和手机环境也非常复杂，无法保证政务应用的操作系统环境是安全的，这些都对政务应用系统的安全防护提出了更高的要求，政务应用系统必须解决因随时可用而带来的便利的同时而带来的网络威胁和数据传输安全威胁，政务应用系统升级改造的核心是国密HTTPS加密和WAF防护，这是《规定》所要求的，也是《清单》所要抽查的，就是急需升级改造的部分。

	数量	增长%	检索域名	默认https	启用国密	WAF防护	安全评级
中国大陆	16,905	1.48%	*.gov.cn	是	否	有	B+
中国台湾省	29,269	135.51%	*.gov.tw	是	否		B+
中国香港特别行政区	2,827	45.80%	*.gov.hk	是	否		B+
中国澳门特别行政区	454	-2.58%	*.gov.mo	是	否		B+

根据零信任安全研究院发布的《中国SSL证书市场发展趋势分析简报-2024Q2》的统计数据，我国31个省市自治区政府域名所申请的有效国际SSL证书数量合计为 1768 张，而同期香港政府网站申请的有效国际SSL证书数量为 2827 张，这就是我国大陆地区政务应用的HTTPS加密应用差距。而所有.gov.cn域名申请的SSL证书总数为 16905 张，这个总数只有一个台湾省的一半多一点，只占与发起《规定》的单位之一的中央编办发布的党政机关事业单位网站标识发放总数 110617 个的 15.28%，也可以理解为我国政务应用网站的HTTPS加密比例低于 20%，超过 80% 的互联网政务应用都是不符合《规定》和《清单》要求的，都是急需升级改造的。

排名	省市自治区	数量	增长%	占比%	检索域名	默认https	部署国密	WAF防护	安全评级
1	上海市	254	17.59%	14.37%	shanghai.gov.cn, sh.gov.cn	是	否		B
2	浙江省	181	-4.23%	10.24%	zj.gov.cn	是	否		B+
3	北京市	128	-1.54%	7.24%	beijing.gov.cn	是	否	有	B+
4	海南省	113	5.61%	6.39%	hainan.gov.cn	是	是		B+
5	广西壮族自治区	101	5.21%	5.71%	gxzf.gov.cn	否	否		
6	广东省	77	1.32%	4.36%	gd.gov.cn	否	否		
7	天津市	70	12.90%	3.96%	tj.gov.cn	是	否	有	A
8	宁夏回族自治区	69	11.29%	3.90%	nx.gov.cn	是	否		B+
9	云南省	62	-4.62%	3.51%	yn.gov.cn	是	否		B+
10	河南省	61	8.93%	3.45%	henan.gov.cn	是	否		B+
11	山东省	58	18.37%	3.28%	shandong.gov.cn, sd.gov.cn	否	否		
12	江西省	47	4.44%	2.66%	jiangxi.gov.cn	否	否		
13	甘肃省	46	12.20%	2.60%	gansu.gov.cn	是	否		B+
14	吉林省	45	12.50%	2.55%	jl.gov.cn	否	否	有	
15	重庆市	44	33.33%	2.49%	cq.gov.cn	是	否		
16	贵州省	40	11.11%	2.26%	guizhou.gov.cn	否	否		
17	黑龙江省	40	14.29%	2.26%	hlj.gov.cn	是	否	有	B+
18	河北省	39	25.81%	2.21%	hebei.gov.cn	否	否		
19	安徽省	38	0.00%	2.15%	ah.gov.cn	是	否	有	A
20	陕西省	35	-16.67%	1.98%	shaanxi.gov.cn	否	否		
21	湖南省	35	9.38%	1.98%	hunan.gov.cn	是	是		
22	新疆维吾尔自治区	33	0.00%	1.87%	xinjiang.gov.cn	是	有(登录页)		B
23	青海省	31	93.75%	1.75%	qinghai.gov.cn	否	否		
24	辽宁省	23	64.29%	1.30%	ln.gov.cn	是	否		B+
25	福建省	21	5.00%	1.19%	fujian.gov.cn, fj.gov.cn	是	否		B+
26	江苏省	19	0.00%	1.07%	jiangsu.gov.cn, js.gov.cn	否	否		
27	西藏自治区	18	50.00%	1.02%	xizang.gov.cn	否	否		
28	内蒙古自治区	15	0.00%	0.85%	nmg.gov.cn	是	否	有	A
29	山西省	11	0.00%	0.62%	shanxi.gov.cn	是	否		B+
30	湖北省	9	12.50%	0.51%	hubei.gov.cn	否	否		
31	四川省	5	25.00%	0.28%	sc.gov.cn	是	否		B+
	合计	1768	8.27%			19	3	6	

而在31个省市自治区中，省级政府官网实现了国际算法HTTPS的也只有19家，还要12家仍然是明文HTTP方式访问，不符合《规定》和《清单》要求。而实现了国密HTTPS加密的只有两家，这更是与《规定》和《清单》要求相差甚远，这些都是急需升级改造的。



为何这么多互联网政务应用没有实现HTTPS加密？

2.1

从统计数据来看，我国政府网站和政务应用系统HTTPS加密普及率低于20%，这么低的原因不外乎两个：一是政务应用前后台管理系统众多，实现HTTPS加密已经很难了，更何况是要改造底层密码算法才能实现国密HTTPS加密就更难了；二是改造投资资金不足，因为多个方面都要求升级改造，大大增加系统投资和维护成本。其中SSL证书部署是最大的难题，一个省政务平台至少有上万个网站系统，有些省有几万个，这么多系统需要人工部署SSL证书，并且是双证书(国际SSL证书和国密SSL证书)，这个工作量巨大，带来的运维成本也是巨大的，并且每年必须更新一次。这是政务应用系统建设和运维面临的 第一个大难题，这也就不能理解为何还有大量的政务应用系统还是以不安全的明文HTTP方式提供服务的主要原因，但这是违反了《规定》和随时可能被《清单》抽查到的，必须解决这个难题才能满足《规定》和《清单》的要求。

为何几乎所有互联网政务应用都没有实现国密HTTPS加密？

根据统计数据，31个省市自治区中只有海南省政府官网和湖南省政府官网实现了国密HTTPS加密，国务院45个部委中只有公安部官网实现了国密HTTPS加密。这些数据也印证了各个政府网站IT主管抱怨的国密改造难的问题，因为要想实现国密HTTPS加密，不仅要向CA购买和申请国密SSL证书，而且还要改造Web服务器支持国密算法和国密SSL证书，但是有些政务应用Web服务器根本是无法改造支持国密算法的。据了解，这些需要通过密评的政务应用有的单位只好建设两套系统，一套是正在使用的仅支持RSA算法的老系统，一套是仅用于通过密评的仅支持SM2算法的新系统，两套系统采用不同的域名访问。也就是说：政务应用系统所面临的不仅仅是RSA算法SSL证书的人工部署维护的费时费力问题，同时也面临SM2算法SSL证书的人工部署维护的费时费力问题，双算法SSL证书部署面临双倍的工作量和双倍系统的投资。这是政务应用系统面临的　第二个大难题，这个难题严重影响了所有互联网政务应用彻底完成国密改造的进度、广度和深度，当然也是违反了《规定》和随时可能被《清单》抽查到的，必须解决这个难题才能满足《规定》和《清单》的要求。

是否所有互联网政务应用都采用了WAF防护？

互联网政务应用系统面临的 第三个难题 就是WAF防护和CDN分发，在各种Web应用攻击不断加剧的形势下，政务应用系统不仅需要网络层的防火墙防护，而且更需要Web应用层的安全防护，这就必须购置WAF设备或云WAF服务。WAF系统是一个前置在Web服务器的Web应用反向代理流量分析转发服务，CDN分发服务也是一个前置在Web服务器的Web应用反向代理转发服务，两者都必须支持HTTPS加密，都必须像Web服务器一样为其申请和部署SSL证书，也就是必须纳入SSL证书的安装部署和定期更新工作中，同时也必须支持国密算法。而市场上大量的WAF设备、云WAF服务和CDN服务都不支持国密算法和国密SSL证书，这也严重影响了政务应用系统普及WAF服务和CDN服务来保障政务应用系统的Web应用安全。请注意，《规定》第二十八条要求CDN服务必须支持国密HTTPS加密。这些互联网政务应用安全要求不仅仅是等保、密保和关保的要求，而且同时是《规定》的要求。

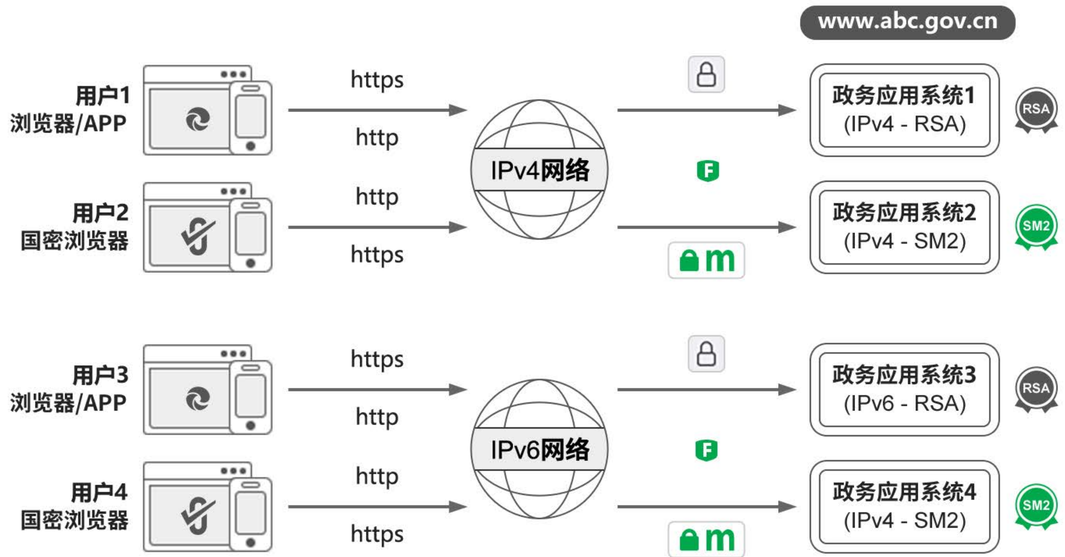
是否所有互联网政务应用都支持IPv6网络访问?

互联网政务应用系统面临的 第四个难题是IPv6网络升级改造，这就要求Web服务器必须支持IPv6网络访问。据实际查询，31个省市自治区政府官网青海省政府官网不支持IPv6解析和访问，其余30个省市自治区政府官网都支持IPv6解析，而19个支持HTTPS安全方式IPv4访问的省市自治区政府官网中，有个多家不支持IPv6网络HTTPS安全方式访问。而支持国密HTTPS加密的湖南省和海南省政府官网并不支持IPv6网络的国密HTTPS加密安全方式访问。这说明政务应用系统为了满足IPv6网络支持的要求，大部分都只是完成了HTTP明文方式的IPv6改造，或者部分完成了HTTPS加密方式的IPv6支持，没有一家省政府官网支持IPv6网络的国密HTTPS加密安全方式访问。这说明大量的政务应用并没有满足《实施》的要求，也同时没有满足《规定》的要求，是一定通不过《清单》检查的。

三、 是否有解决方案可以实现一箭四雕，搞定四大难题？

从上面的分析可以得出这样的结论：为了满足国密改造和IPv6改造的合规要求，大量政务应用系统正在采用错误的建设方案建设了4套政务应用系统来满足要求各种合规要求，这不仅仅是大大增加了政务应用系统投资的问题，而且是大大增加了政务应用系统的复杂性和维护难度，从而降低了政务应用系统的可靠性，这只能理解为这是一个为了应对合规检查的无奈之举。

为了更加形象地说明互联网政务应用安全目前的解决方案存在的问题，如下图所示，一个政务服务网站(www.abc.gov.cn)建设了4套一样的系统来满足4种不同用户的电子政务服务需求，用户1使用浏览器/APP通过IPv4网络HTTP或HTTPS方式访问政务应用系统1，这就要求在政务应用系统上部署RSA算法SSL证书，这是传统的方式，也是目前大多数政务网站的工作方式。而为了满足国密合规的要求，则又另外建设一套支持国密算法的政务应用系统2，来满足用户使用国密浏览器和国密算法实现HTTPS加密安全方式访问政务服务的需求，要求在政务应用系统2上部署国密SSL证书。而为了保障这两个系统的Web应用安全，必须购买WAF设备或云WAF服务。为了满足IPv6的合规要求，又另外建设了政务应用系统3和系统4来满足IP4/IPv6网络用户使用国密浏览器和不支持国密算法的浏览器能访问政务服务的要求。这样的同一个域名网站同时建设4套系统绝对不是一个个例，很多政务应用系统都是这么设计和建设的。



这种建设方案，不仅浪费了大量的系统建设费用，其核心问题并没有真正得到解决，那就是SSL证书的人工申请和部署难题，这是一个一年需要为超过每套系统1万台，4套系统就是4万台的政务应用服务部署SSL证书的难题。而为了保证SSL证书密钥安全，国际标准计划把SSL证书有效期从目前的1年改为90天，也就是说，原先一年更新一次的工作量将翻5倍，一年要更新5次，现在的要为1万台服务器部署SSL　证书将变成相对于为5万台服务器部署SSL证书，4套系统就是要部署20万台服务器，这将是一个不可能实现的任务，根本无法完成《规定》、《清单》和《实施》所要求的合规工作，必须找到好的解决方案来解决这些难题。

大家可能会想到ACME技术(自动化证书管理环境)，通过检索谷歌证书透明日志系统发现，截至到今天，“.gov.cn”域名申请的有效SSL证书数为16953张，有993个域名申请的是自动化部署的Let’s Encrypt的国际SSL证书，占比为6%。这应该与政务应用系统服务器不能随便安装第三方软件有关，因为要想实现证书自动化，目前的国际方案是必须在Web服务器安装一个ACME客户端软件。而即使妥协一下允许安装这个国外的客户端软件，有些较老的服务器也许不支持安装这个客户端软件。还有，这个解决方案只能自动化部署RSA/ECC算法SSL证书，不能实现国密SSL证书的自动化部署，无法实现国密HTTPS加密自动化。并且市场上的WAF设备/CDN服务都还不支持ACME技术，仍然需要人工申请和部署SSL证书。

也就是说：要解决政务应用系统面临的四大难题，只有自动化实现HTTPS加密这一条路。但是，国外的需要在服务器上安装第三方客户端软件的HTTPS加密自动化解决方案无法解决我国政务应用系统安全面临的问题，因为：

01 Web服务器不能或无法安装ACME客户端软件，但是需要实现HTTPS加密自动化；

02 不想改造或者无法改造Web服务器，但是需要支持国密算法实现国密HTTPS加密，实现国密HTTPS加密自动化；

03 不想手动为WAF设备部署SSL证书，但是希望实现HTTPS加密方式的WAF防护自动化；

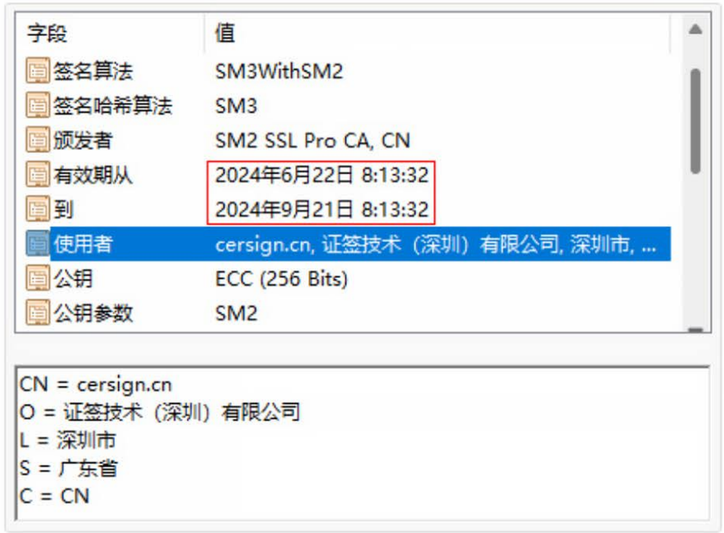
04 不想升级改造Web服务器和内部网络以支持IPv6，但是可实现用户使用IPv6网络访问政务应用系统。

这些都是摆在所有党政机关事业单位的IT主管们面前的现实问题和技术难题，必须寻找一个好的解决方案彻底解决这4个棘手的难题，而不是现在的建设四套不同的政务应用系统的方案。

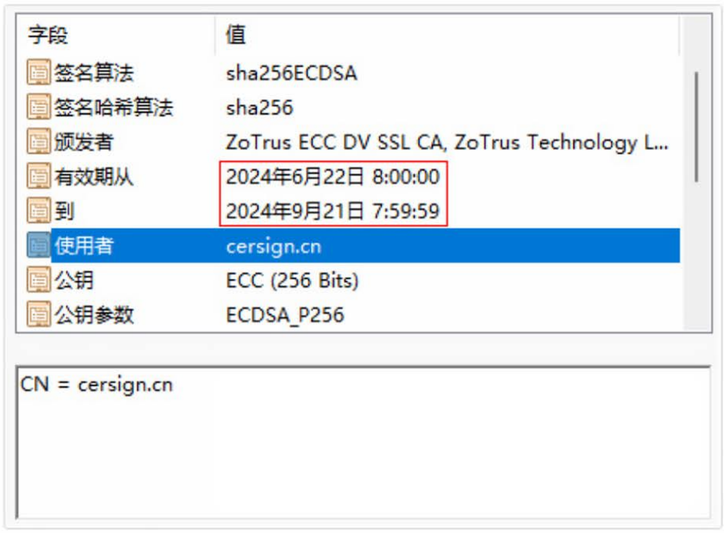
四、 零信网关，自动化搞定政务应用系统升级改造四大难题

目前市场上可用的能解决以上难题的解决方案只有一个：部署零信国密HTTPS加密自动化网关，这是一个为我国HTTPS加密自动化量身打造的具有国际先进水平的自动化证书管理产品，是目前唯一一个通过商用密码产品认证的国密HTTPS加密自动化网关产品，也是唯一一个遵循《自动化证书管理规范》密码行业标准的网关产品，一个采用高性能密码卡打造的高端高性能网站安全硬件密码设备，是一个集HTTPS加密加速、HTTPS卸载转发、国密算法模块、SSL证书自动化、WAF防护、负载均衡等多项功能于一体的专用于HTTPS加速和卸载的硬件密码设备，内置专业级高性能硬件密码卡实现高速密码运算和网络包转发，并且对内置操作系统、网络协议、SSL/TLS协议、ECC算法和SM2算法都进行了专业的深度优化，实现了业界领先的极致性能。

零信国密HTTPS加密自动化网关最大的特点和特色是用户无需向CA申请SSL证书，自动化申请双算法SSL证书(国密OV SSL证书和国际DV SSL证书)、自动化部署双SSL证书、并且已经提前满足将来90天有效期证书政策，自动化实现国密HTTPS加密，自适应加密算法，支持国密算法和国密证书透明的国密浏览器采用SM2算法实现国密HTTPS加密，不支持国密算法和国密证书透明的其他浏览器采用国际ECC算法实现HTTPS加密。这是一个端云一体的创新解决方案，零信网关内置国密ACME客户端，自动对接零信云SSL系统，自动化完成双算法SSL证书申请、部署和续期，确保业务系统零改造实现HTTPS加密，不间断地自动化为多达255个不同域名的业务系统提供自动化HTTPS加密服务和WAF防护服务。

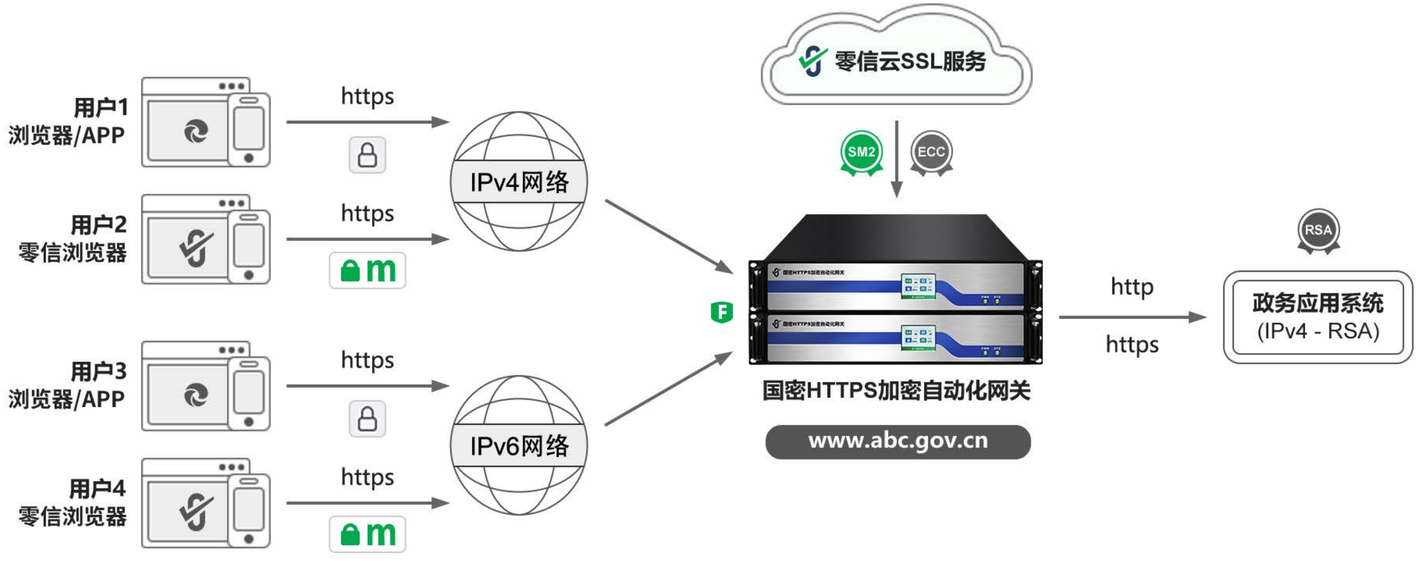


公网SM2 SSL证书



公网ECC SSL证书

传统方案需要为同一域名政务网站建设四套系统来满足四种不同用户使用政务服务的需求，而零信技术的创新方案是：只需部署零信国密HTTPS加密自动化网关，无需建设多余的三套系统，最早建设的第一套IPv4网络的政务应用系统零改造，零安装SSL证书，自动化满足四种用户的政务服务需求，如下图所示。



互联网政务应用系统部署零信国密HTTPS加密自动化网关后，可以实现：

HTTPS加密自动化

这是由零信网关自动化实现明文HTTP协议和HTTPS加密协议的转换工作。零信网关让原政务应用系统Web服务器零改造，零安装ACME客户端软件，零申请和零安装SSL证书，只需一次配置政务应用域名，5年内自动化免费为多达255个网站申请和部署双算法SSL证书(国际DV SSL证书+商密OV SSL证书)，自动化自适应加密算法实现HTTPS加密，自动化完成国密改造。不用担心证书有效缩短到90天，因为网关会自动化申请证书、自动化续费和重新部署证书，不怕即使将来缩短到1天，不仅大大节省大量的SSL证书费用，而且彻底把系统运维工程师解放出来，让机器去自动化完成申请和部署SSL证书这个费时费力的苦力活，让工程师们有精力去做更有价值的政务应用系统安全运维工作。

国密HTTPS加密自动化

这是由零信网自动化实现国际算法HTTPS加密和国密算法HTTPS加密的两个不同的密码体系的转换工作。零信网关让原政务应用系统无需升级改造就可以实现国密HTTPS加密，再也无需为了国密改造而单独建设一套支持国密算法的政务应用系统，只需在现有的政务应用系统前部署零信国密HTTPS加密自动化网关即可，无需改造Web服务器以支持国密算法，无需申请和安装国密SSL证书，自动化配置国密OV　SSL证书，自动化实现国密HTTPS加密，原政务应用系统零改造，自动化完成国密改造，满足各种法律法规的合规要求。更重要的是：这是自动化实现国密HTTPS加密的解决方案，一切工作由机器自动化完成，当然也不用担心SSL证书有效期缩短的问题，机器会自动化定期申请和安装双SSL证书。

3

WAF防护自动化

这是由零信网关自动化实现Web流量清洗和转发工作，并且是自动化卸载HTTPS加密流量后的流量安全保护，用户无需另外花钱购置WAF设备或云WAF服务，也无需为部署和更新WAF设备或WAF服务所需的SSL证书发愁，只需部署零信国密HTTPS加密自动化网关，就可以自动化实现HTTPS加密方式的WAF防护，WAF防护的检测能力和识别能力都达到A级(最高级别)，防护性能甚至超过售价百万的WAF设备，并且是同时支持国际算法HTTPS加密和国密算法HTTPS加密自动化的WAF防护。

4

零改造搞定IPv6支持

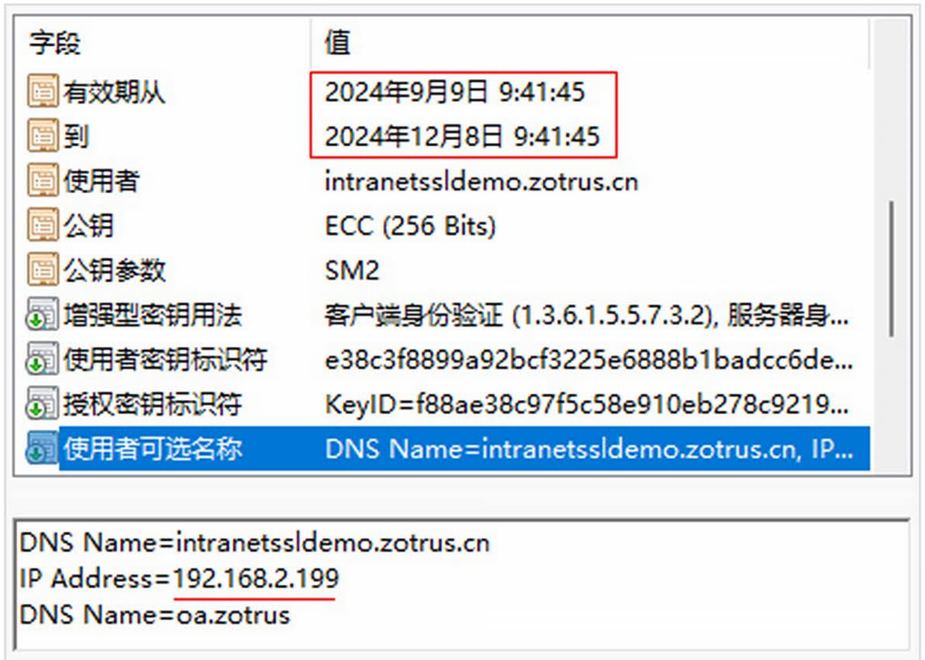
这是由零信网关自动化实现IPv6网络协议和IPv4网络协议的两个不同网络协议的转换，并且是同时支持HTTP流量、RSA算法HTTPS流量和SM2算法HTTPS流量。原政务应用系统Web服务器无需改造，但可以满足用户使用IPv6网络访问位于网关后的IPv4网络的政务应用系统，由零信网关实现IPv6到IPv4的自动化转换，并且是HTTPS加密方式的IPv6安全访问，优先采用国密HTTPS加密方式的IPv6访问。

免费配套国密浏览器

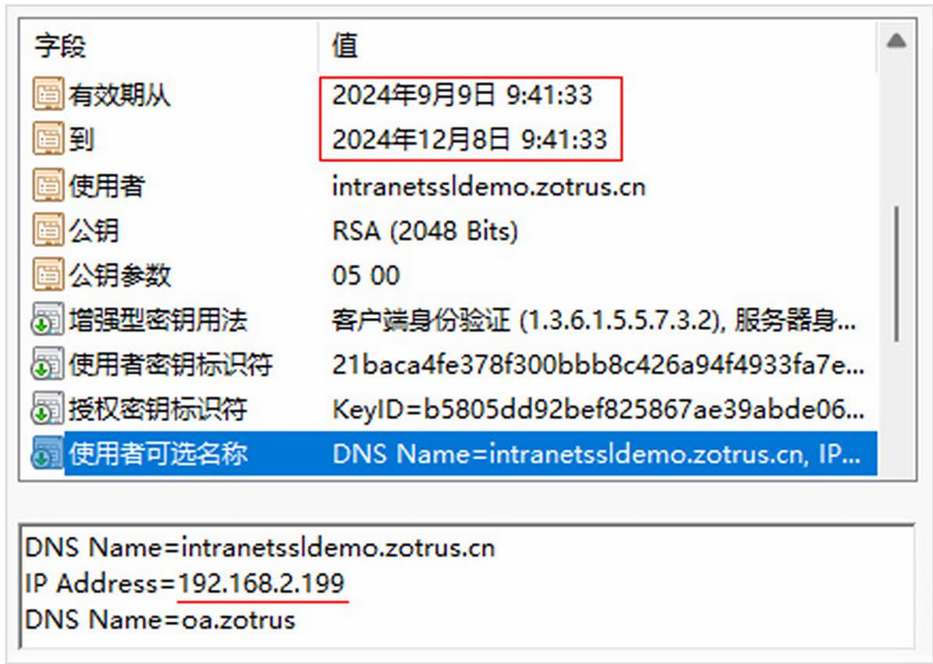
5

要实现国密HTTPS加密，仅有网关实现自动化国密HTTPS加密是不够的，还需要用户端有浏览器支持国密HTTPS加密访问。而目前市场上的国密浏览器都是收费的，这无法满足普及国密算法的需要。零信技术免费配套提供不限数量使用的国密浏览器—零信浏览器，一个干净无广告的基于谷歌内核的同时支持RSA/ECC/SM2三算法的高性能通用浏览器，优先采用国密算法安全访问政务应用系统，确保了即使RSA算法SSL证书被非法吊销也不会影响用户正常访问政务应用系统和正常使用政务应用服务。零信网关还免费赠送零信浏览器网站可信EV认证，让零信浏览器在地址栏绿色显示政务应用网站单位名称，提升政府官网和政务应用系统的防假冒网站能力，有力保障政务应用用户账户安全和政务应用系统安全。

以上解决方案不仅仅适用于位于公网的互联网政务应用(政府官网、公众服务系统和政务管理系统)，同时适用于位于政务外网和内网的各种政务内部管理系统，零信网关支持自动化申请和部署零信浏览器信任的内网SSL证书(RSA和SM2算法)，支持内网IP地址和内部主机名，以满足政务外网和内网流量加密安全的应用需求。并且支持90天有效期的密钥安全要求，以满足即将到来的国际标准和国密标准要求。



内网SM2 SSL证书



内网RSA SSL证书

五、 零信创新方案为党政机关事业单位提供了六大超值服务

零信技术提供的自动化证书管理方案，不仅可用于互联网政务应用和政府官网的HTTPS加密自动化和WAF防护自动化，而且还能用于政务外网和内网的所有政务管理系统的国密HTTPS加密自动化，其超值价值体现在如下6个方面：

01 自动化，彻底解放运维工程师，不再需要人工申请和部署证书，节省人力成本150万元；

02 自动化，配置双算法SSL证书，不再需要花钱买证书，节省证书成本623万元；

03 自动化，WAF防护，不再需要花钱买WAF设备，节省WAF设备购置100万元；

04 自动化，无需建设RSA/SM2两套政务应用系统，节省系统重复建设成本N 个 100万元；

05 自动化，无需建设IPv4/IPv6两套政务应用系统，节省系统重复建设成本N 个 100万元；

06 免费配套提供干净无广告的基于谷歌内核的高性能国密浏览器，节省国密浏览器购买费用。

上面这些都是看得见的经济效益，还有无法计算的社会效益，主要体现在如下6个方面：

01 自动化，快速满足国密合规要求、等保和关保合规要求，满足《规定》《清单》《实施》的最严格合规要求；

02 自动化，快速部署国密SSL证书，保障政务应用系统不会受到地缘政治的SSL证书断供影响，保障国家安全稳定；

03 自动化，不会出现人工申请和部署SSL证书的忘了到时续期和部署的严重安全问题；

04 自动化，实现一站一密钥一证书，彻底解决了人工部署通配证书的共用密钥安全问题；

05 自动化，覆盖政务应用所有公网和内网业务系统，实现国密HTTPS加密全覆盖和普惠安全；

06 自动化，真正实现现有的政务应用系统零改造，不影响现有政务业务系统正常运行，无缝升级完成国密改造和IPv6改造。

六、唯有自动化，才能安全提供不间断的政务应用优质服务

国家有关部门之所以在7月份连续发文《规定》和《清单》，是因为普及商用密码来保障我国政务应用安全的形势迫在眉睫，因为互联网政务服务是老百姓已经离不开的最重要的互联网应用。但是，互联网政务应用系统的国密改造是一个全生态的改造，涉及到方方面面，难度非常大。零信技术的国密HTTPS加密自动化解决方案创新地把很难改造的基于RSA密码体系的政务应用系统变成了无需改造，直接在其基础上增加一个网关就可以自动化完成国密HTTPS加密，并且是自适应加密算法，自动化配置双算法SSL证书，以满足政务应用用户既可以使用国密浏览器采用国密算法使用网银服务，而可以使用不支持国密算法的其他浏览器采用国际算法使用政务应用服务。零信网关实现了一个网关搞定政务应用升级改造4个棘手的难题，是互联网政务应用系统升级改造的首选产品。

不仅如此，要想保障政务应用Web 系统全程安全，政务应用还需要改进政务APP 和小程序的 SSL 证书验证机制，因为现在用户使用政务 APP或小程序已经比使用浏览器登录政务应用系统更普及，这就要求政务 APP能像浏览器一样支持国密算法和国密 SSL 证书，像浏览器一样严格验证政务应用系统部署的 SSL证书，必须验证 SSL 证书是否可信、是否域名匹配、是否过期和是否被吊销等各种证书安全问题，只有这样才是一个安全的政务APP。并且必须优先采用国密算法实现 HTTPS 加密，这样才能保证政务应用系统不受 RSA 证书的可能存在的安全风险的制约，才能真正保证为用户提供不间断的安全的电子政务服务。