一个网关搞定四个棘手的大型企业网升级改造难题

可能有企业 IT 主管的读者朋友看到此文章标题就想说：我们的企业网需要升级吗？有棘手的改造难题吗？不急，请耐心往下看，一定大有收获。

大中型企业都有自己的官网和各种业务管理系统(包括位于公网的公众服务系统和位于内网的内部管理系统)，表面上看一切尚好。但是，请企业 IT 主管们检查一下自己官网和所有业务系统(公网和内网)是否全部实现了 HTTPS 加密，相信一定仍然有许多系统并没有实现 HTTPS 加密，甚至没有一个网站系统实现了 HTTPS 加密，这是因为企业往往只重视传统的位于机房的服务器端安全防护建设，而不重视数据传输安全建设，安全防护观念还没有从传统的基于城堡的安全防护转换到云计算和大数据时代的数据流通全程保护上来。

大家都知道数据资产的重要，数据资产都可以列入财务报表了。但要想保护好自己的宝贵数据资产，很多企业 IT 主管还是传统的保护理念，认为保护数据就是保护服务器的安全，或者做好数据使用的权限管理，或者把数据加密处理保存在数据库，这些都是传统的城堡安全思维。在云计算和移动互联网时代，数据是需要流通的，是一直在流动中，只有流通才能产生价值，才能成为重要资产。而流通就需要用户可以通过浏览器或 APP 访问和使用，这就离不开 HTTPS 加密，数据传输加密是数据处理中最重要的一环，这一环节不安全，其他环节做了再多的安全保护都是无用的，数据传输加密是数据安全木桶理论的地板。

本文重点讲一讲企业在保护重要数据的流通传输安全方面遇到的难题和如何解决这些难题。当然，这个“企业”可以泛指各种组织，包括政府机构，流行词“企业安全架构”就是指一种为组织提供全面保护以抵御网络威胁的策略，美国政府《联邦零信任战略》的第一段就要求所有联邦政府机构的企业安全架构基于零信任原则，其中最重要的一个原则是对明文 HTTP 流量零信任，要求加密所有 HTTP 流量，包括公网和内网流量。

一、 大中型企业网为何急需升级改造？有哪些需要改造的？

我国的企业管理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企业业务发展和各种管理的需要。但是，在目前的云计算和移动互联网时代，数据是在不断流动的，是全国范围甚至全球范围的基于互联网的流动，而不是传统的在内部办公网流动。唯一可行的保护数据流动安全的技术就是 HTTPS 加密，能有效地保障数据从用户浏览器或 APP 到业务系统的

传输链路是加密的，能有效地防止数据在传输过程中的泄露和被非法篡改。

笔者从国际证书透明日志系统检索了如下八家央企域名的有效国际 SSL 证书申请量：国家电网(sgcc.com.cn)：184 张、中国烟草(tobacco.gov.cn)：20 张、中国石化(sinopec.com): 164 张，中国石油(petrochina.com.cn)：22 张、中国铁路(12306.cn)：2 张、中国移动(10086.cn)：224 张、国家电投(spic.com.cn)：23 张、中国船舶(cssc.net.cn)：1 张。从 SSL 证书的申请量就能看出各个企业对 HTTPS 加密的重视程度是不同的，因为大企业一定有许多业务系统，证书申请量少只能说明还要大量的业务系统没有实现 HTTPS 加密，当然有些域名的证书数量少是因为使用了无法保证密钥安全的通配证书。从证书透明日志数据可以看出：中国移动排名第一位，中国船舶官网没有部署 SSL 证书，其 9 七个下属单位网站也大多数没有部署 SSL 证书。

我们再对比一下中美企业对 HTTPS 加密的普及数据，全球排名第一位航空公司是美航(aa.com)，其 SSL 证书申请量是 1656 张，这是我国申请证书最多的航空公司-国航(airchina.com.cn)的 43 张的 38 倍多，是国企中申请证书最多的中国移动的 7 倍多，这个数字就能说明中美企业在信息系统建设上的 HTTPS 加密普及应用水平的巨大差距，同样都是航空公司一定有非常相似功能的业务系统但为何 SSL 证书申请量差这么多？一定是仍然有许多业务系统还没有部署 SSL 证书，这非常值得我国企业高度重视。

笔者思考的是：为何这些企业的官网和许多业务系统都没有部署 SSL 证书？除了传统的防护理念需要更新外，是否是技术因素导致的？因为要实现 HTTPS 加密，传统的方式是企业向 CA 机构购买和申请 SSL 证书，拿到证书后部署到服务器上启用 HTTPS 加密。这个过程如果只管理一两个网站系统，人工操作也许还能承受，但是如果要管理几百几千张 SSL 证书在成千上万台服务器上去使用，这个人工处理的工作量是巨大的。这是大型企业面临的困境，也许 IT 主管们知道必须部署 SSL 证书来实现 HTTPS 加密来保护数据传输安全，但是面对居高不下的人力成本，让大量部署和管理 SSL 证书成为一个令 IT 主管们头痛的难题。怎么办？

人工部署 SSL 证书的另一个困境是由于有太多的服务器需要部署 SSL 证书，运维人员一般采用 Excel 表来记录各个网站的证书何时到期，但仍然会由于各种原因而遗忘了按时续期 SSL 证书。一个真实的案例是爱立信电信设备中的 SSL 证书过期而没有续期，从而导致了移动运营商 O2 的移动数据管理系统崩溃，这使得其 3200 万客户以及全球其他运营商的客户都无法正常使用移动通信服务，业务被中断了二十多个小时才恢复，O2 为此向爱立信索赔数百万美元。笔者前段时间访问 Adobe Sign 服务时发现登录账户的 SSL 证书已经过期了 24 天仍然没有续期，这已经不是笔者见过的第一个证书过期未续期的网站了。

也就是说，在所有系统无论位于公网还是内网都必须普及实现 HTTPS 加密的时代，手工部署 SSL 证书来实现 HTTPS 已经力不从心，即使是大公司也如此。更加严峻的考验还在后头，

谷歌正在推动缩短 SSL 证书有效期为 90 天，这意味着原先一年才申请和安装一次 SSL 证书的行为需要改为一年 5 次！连一年一次都会遗漏，更不用提一年 5 次了，这意味着手动申请和部署 SSL 证书已经不可能。怎么办？

另一个摆在国有企业、金融证券企业和关键信息基础设施系统运维企业(如电信、航空等)面前的另一个 HTTPS 加密难题是国密合规，也就是国密改造，必须申请和部署国密 SSL 证书实现 HTTPS 加密，这个难度比上面所讲的申请和部署国际 SSL 证书实现 HTTPS 加密更加困难，因为涉及面更广，需要升级改造 Web 服务器软件，这极有可能严重影响现有业务系统的正常运行。怎么办？

1. 为何这么多企业网站和业务系统没有实现 HTTPS 加密？

从统计数据来看，我国企业网站和企业管理系统 HTTPS 加密普及率低于 5%, 这么低的原因不外乎两个：一是企业管理前后台管理系统众多，公网实现 HTTPS 加密已经很难了，更何况是大量的内部管理系统也需要实现 HTTPS 加密，因为目前的公网 SSL 证书不支持内网 IP 地址，只能用自签证书或者只能用公网域名证书做内网 IP 地址解析。二是改造投资资金不足和人手不够，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。其中最大的难题是 SSL 证书的部署，一个大型企业少的有上百个、多则成千上万个网站系统，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。这是企业管理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企业管理系统还是以不安全的明文 HTTP 方式提供服务的主要原因，但这不仅让宝贵的企业数据失去了保护，更是违反了国家有关等保、密评和关保的要求。

2. 为何几乎所有企业网站系统都没有实现国密 HTTPS 加密？

按照四部委发布的《互联网政务应用安全管理规定》和其他法律法规的要求，所有列入关键信息基础设施的单位(如水电气、交通、通信、金融、证券等)网站和业务管理系统都必须像政务应用一样实现国密 HTTPS 加密保护。但目前笔者还没有发现一个大型国企官网实现了国密 HTTPS 加密，这个国密改造工作迫在眉睫，怎么改造，在实施之前选择正确的改造方案非常重要。

传统的方式实现国密 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，但是有些企业管理系统 Web 服务器由于是早期建设的系统，并且一直正在可靠运行中，根本不可能停下来实现国密算法支持改造。笔者强烈建议不要采用为了通过等保和密评而建设两套系统的落后方案，已经有了一套是支持 RSA 算

法的老系统，不应该再浪费有限的预算去新增一套是用于通过密评的仅支持 SM2 算法的新系统。也就是说：企业管理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。这是企业管理系统已经面临或即将面临的**第二个大难题**。

3. 是否所有业务系统都采用了 WAF 防护？

企业官网和企业管理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，企业官网和企业管理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，这也严重影响了企业管理系统普及 WAF 服务和 CDN 服务来保障企业管理系统的 Web 应用安全，也就是无法保障宝贵的企业数据的流通安全。

4. 是否所有业务系统都支持 IPv6 网络访问？

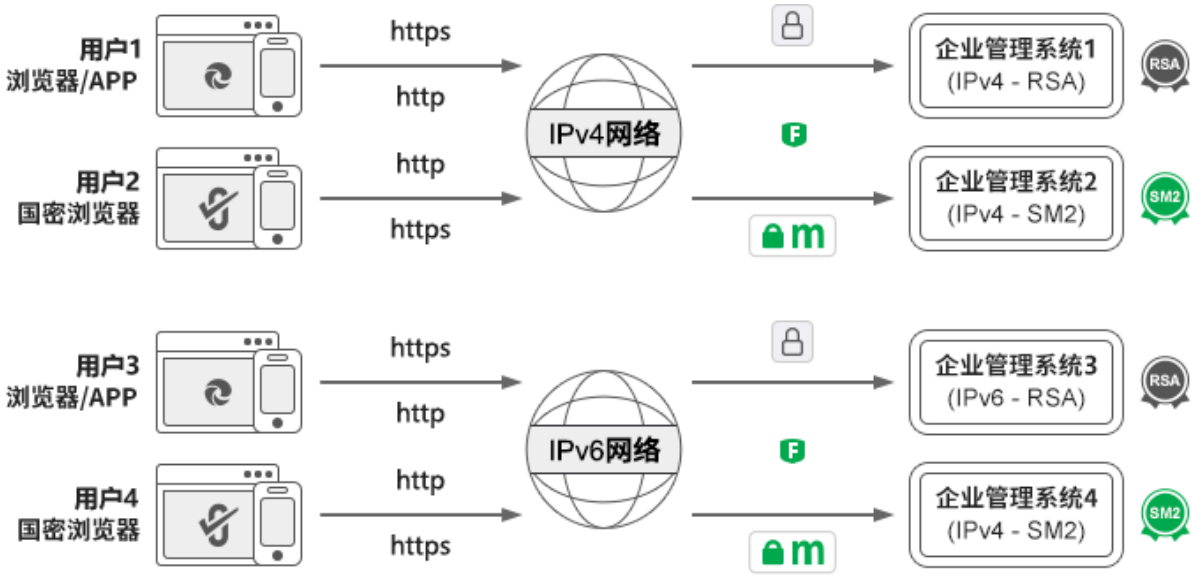
企业管理系统系统面临的第四个难题是 IPv6 网络升级改造，这就要求 Web 服务器必须支持 IPv6 网络访问。为了减轻改造负担，企业在选择改造方案时不应采用为了满足改造要求而另外投资建设一套 IPv6 业务系统，应该选择一个零改造支持 IPv6 网站用户访问的解决方案。

二、 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 HTTPS 加密国密改造和 IPv6 改造的合规要求，大量企业管理系统正在采用错误的建设方案建设了多套企业管理系统来满足要求各种合规要求，这不仅仅是大大增加了企业管理系统投资的问题，而且是大大增加了企业管理系统的复杂性和维护难度，从而降低了企业管理系统的可靠性，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企业网站和管理信息系统安全目前的解决方案存在的问题，如下图所示，一个企业管理系统建设了 4 套一样的系统来满足 4 种不同用户的公众服务和企业管理需求，用户 1 使用浏览器/APP 通过 IPv4 网络 HTTP 或 HTTPS 方式访问企业管理系统 1，这就要求在企业管理系统上部署 RSA 算法 SSL 证书，这是传统的方式，也是目前大多数企业网站系

统的工作方式。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企业管理系统2，来满足用户使用国密浏览器和国密算法实现 HTTPS 加密安全方式访问公众服务和企业管理的需求，要求在企业管理系统 2 上部署国密 SSL 证书。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。而为了满足 IPv6 网络合规要求，又另外建设了企业管理系统 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都能访问公众服务和企业管理的要求。这样的同一个网站系统同时建设 4 套系统绝对不是一个个例，希望企业 IT 主管们不要选择这个错误的建设方案。



这种错误的建设方案，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多套系统成百上千台服务器部署 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 100 台服务器部署 SSL 证书将变成相对于为 500 台服务器部署 SSL 证书，4 套系统就是要部署 2000 台服务器，这将是一个不可能实现的任务，根本无法完成国密改造和 IPv6 改造等各种合规改造工作，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)，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，但是可能有些企业并不愿意在其服务器上安装第三方软件。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：要解决企业管理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企业管理系统安全面临的问题，因为：

(1) 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；

(2) 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；

(3) 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；

(4) 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 网络访问企业管理系统。

这些都是摆在所有企业 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企业管理系统的方案。

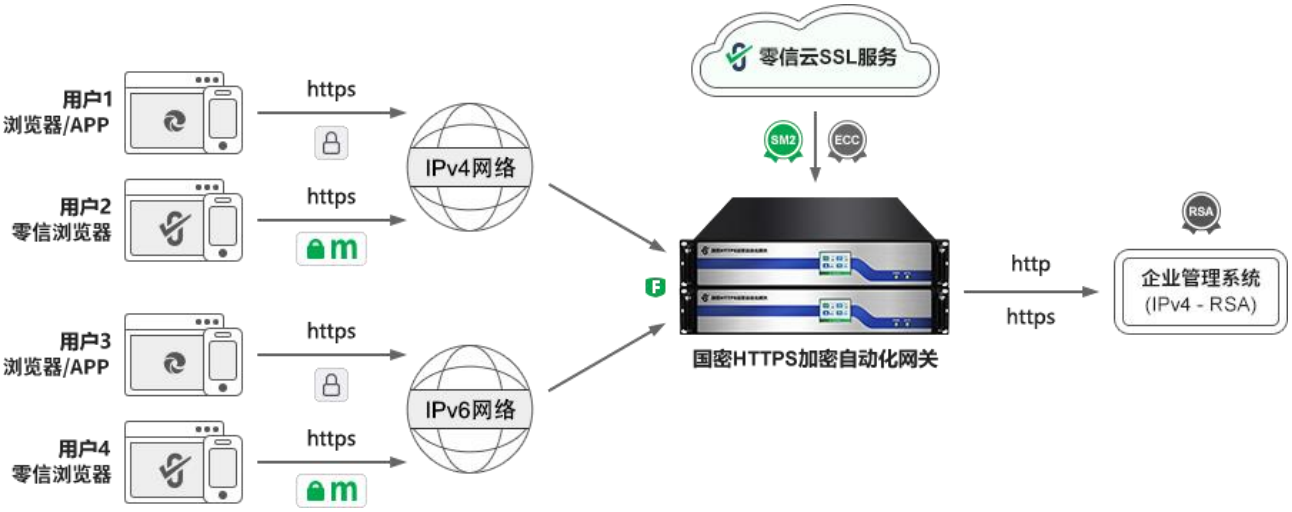
三、 零信网关，自动化搞定企业管理系统升级改造四大难题

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，由零信网关自动化申请双算法 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。

传统方案需要为同一域名企业网站系统建设四套系统来满足四种不同用户使用公众服务和企业管理的需求，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 网络的企业管理系统零改造，零安装 SSL 证书，自动化满足四种用户的公众服务和企业管理需求，如下图所示。



企业网站和企业管理系统部署零信国密 HTTPS 加密自动化网关后，可以实现：

1. **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。零信网关让原企业管理系统 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，只需一次配置企业应用域名，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企业管理系统安全运维工作。

2. **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。零信网关让原企业管理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企业管理系统，只需在现有的企业管理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，原企业管理系统零改造，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**

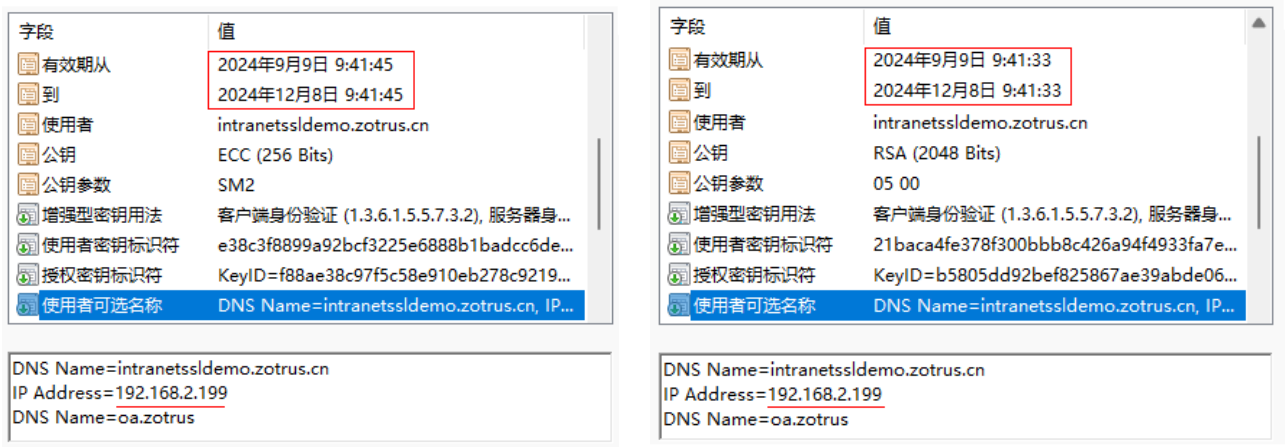
这是由零信网关自动化实现 IPv6 网络协议和 IPv4 网络协议的两个不同网络协议的转换，并且是同时支持 HTTP 流量、RSA 算法 HTTPS 流量和 SM2 算法 HTTPS 流量。原企业管理系统 Web 服务器无需改造，但可以满足用户使用 IPv6 网络访问位于网关后的 IPv4 网络的企业管理系统，由零信网关实现 IPv6 到 IPv4 的自动化转换，并且是 HTTPS 加密方式的 IPv6 安全访问，优先采用国密 HTTPS 加密方式的 IPv6 访问。

5. 免费配套国密浏览器

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企业管理系统，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企业管理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企业应用网站单位名称，提升企业官网和企业管理系统的防假冒网站能力，有力保障企业应用用户账户安全和企业管理系统安全。

需要特别指出的是：以上解决方案不仅仅适用于位于公网的企业官网和企业管理系统，同时适用于位于内网的企业管理系统，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，以满足企业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。



四、唯有自动化，才能不间断地保障企业数据流通安全

依据《数据安全法》第三条对“数据处理”的定义，数据处理包括数据的收集、存储、使用、加工、传输、提供、公开等。在这个七个数据处理环节中，其他六个环节都离不开数据传输，所以，数据安全的“七寸”是数据传输，必须保护数据的传输安全，不做好这个安全保护，其他安全保护都是空中楼阁，这就是数据的“在途”安全，唯一可靠的技术方案就是 HTTPS 加密，数据在全生命周期中的流通传输都必须是通过 https 加密通道传输，当然，依据《密码法》和

其他法律法规，必须采用国密 https 加密来加密数据传输通道，也就是必须部署国密 SSL 证书来实现 HTTPS 加密，只有这样才能有效保障每一个数据处理过程中的数据处于有效保护中，使得数据从生产到销毁的全生命周期都处于持续安全状态。

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，让企业数据通过国密加密通道安全地流通，这不仅是国密合规的要求，更重要的是保证了企业数据不会在“路”上被打劫，不会被非法窃取和非法篡改，保障了企业数据的“在途”安全。

零信国密 HTTPS 加密自动化管理解决方案不仅解决了自动化部署 SSL 证书实现 HTTPS 加密的难题，而且同时解决了国密合规的难题，并且节省了大量的运维人力成本。国密 HTTPS 加密自动化网关最多支持为 255 个网站提供 5 年的不间断的自动化 HTTPS 加密服务，仅自动化免费配置的双算法 SSL 证书的费用就高达 623 万元，再加上节省的 5 年人力成本 150 万元，部署网关为用户节省的开支合计高达 773 万元，这绝对是最值得投资建设的信息化基础设施。零信国密 HTTPS 加密自动化管理解决方案是一个(好处) “多”、“快”速实施、“好”用、“省证书费用和人力成本的最佳解决方案。零信网关实现了一个网关搞定大量企业网升级改造 4 个棘手的难题，是大型企业网升级改造的首选产品。

不仅如此，要想保障企业应用 Web 系统全程安全，企业应用还需要改进企业应用 APP 和小程序的 SSL 证书验证机制，因为现在用户使用企业应用 APP 或小程序已经比使用浏览器登录企业管理系统更普及，这就要求企业应用 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企业管理系统部署的 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企业应用 APP。并且必须优先采用国密算法实现 HTTPS 加密，这样才能保证企业管理系统不受 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企业应用服务和管理信息系统服务。

五、如何抓住大型企业网急需升级改造给业界带来的新机遇？

大家应该已经看到各个法律法规都在要求所有关键信息基础设施运营单位必须完成国密 HTTPS 升级改造和 IPv6 改造，这是硬指标，不仅有违法罚款而且还要追究当事人和有关领导的行政责任，如果相关网络安全和密码业界能真正为这些企业用户提供多快好省的解决方案，一定能拿下这些大订单。这就是已经疲劳和高度内卷的网安市场的新机遇，欢迎有实力的业界企业合作，包括但不限于：

(1) 充分利用好自己的现有大型企业客户资源优势，让这些优质客户了解零信技术这个一劳永逸的创新解决方案，一个能真正帮助用户解决问题并且还很省钱的方案，自动化网关和免费配套双证书包用 5 年，节省证书费用和多余系统建设费用超过千万元。

(2) 对于有意研发自己的自动化网关和自动化 WAF 设备的企业，欢迎合作遵循《自动化证书管理规范》密码行业标准对接零信云 SSL 服务系统，实现自动化为自有网关和 WAF 设备配置全球信任和国密合规的双 SSL 证书，满足用户急需的证书自动化管理硬需求。

(3) 欢迎云 WAF 和 CDN 厂商合作，自动化对接零信云 SSL 服务系统，实现自动化为 WAF 服务和 CDN 服务配置双算法 SSL 证书，满足政府用户对 CDN 和 WAF 服务的国密 HTTPS 加密自动化需求。

(4) 欢迎各个有意提供 SSL 证书自动化解决方案的合作伙伴定制自有品牌的双算法 SSL 中级根证书，为自己的产品和云服务自动化配置自己品牌的全球信任的国际 SSL 证书和国密合规的国密 SSL 证书，进一步提升自己产品的含金量、品牌影响力和自主可控能力。

王高华

2024 年 9 月 9 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 177 篇(共 50 万 2 千多字)和英文 68 篇(8 万 4 千多单词)。。