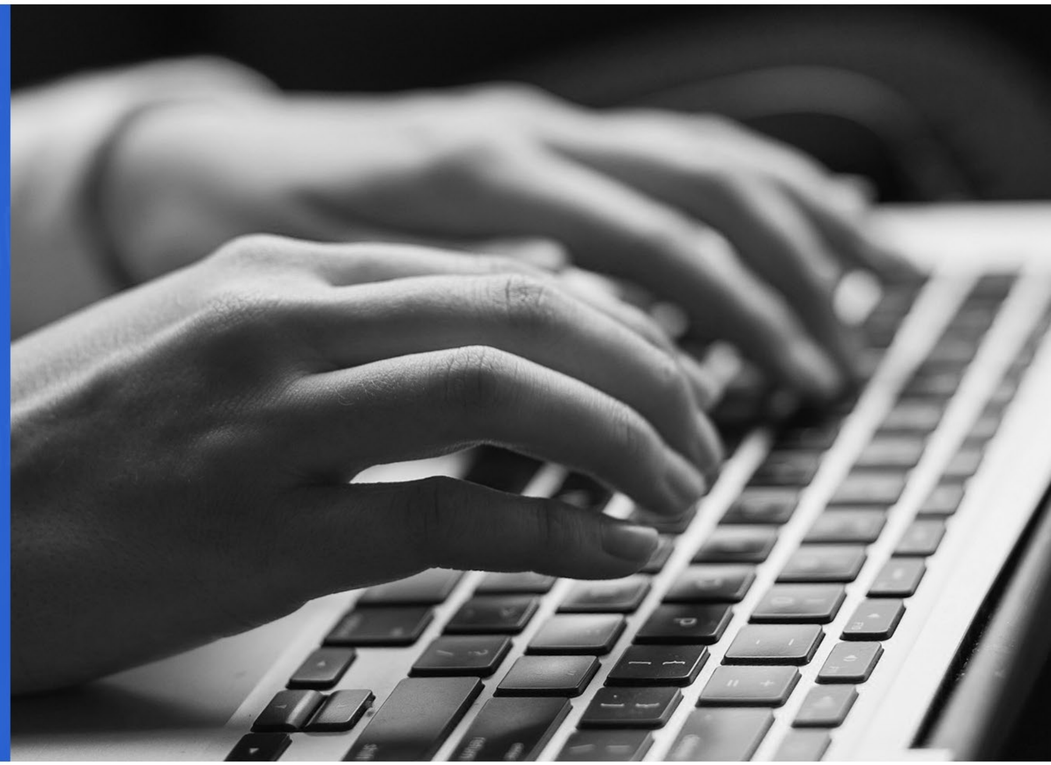
零信®
ZoTrus

网银系统升级改造方案

一个网关搞定四个辣手的网银系统升级改造难题



https://www.zotrus.com

什么是网银系统？就是用户可以通过浏览器或APP完成各种银行业务操作的服务系统。　网银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银行业务的需要，特别是手机APP网银的普及使用，极大地方便了用户使用银行服务。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，用户使用网银的电脑环境和手机环境也非常复杂，无法保证网银APP的使用操作系统环境是安全的，这些都对网银系统的安全防护提出了更高的要求，网银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，网银系统升级改造的核心是国密HTTPS加密和WAF防护。

一、 网银系统升级改造遇到了哪些难题?

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-2023Q3》的统计数据，我国二十大银行的国密HTTPS加密改造工作完成情况并不乐观，究其原因不外乎两个：一是网银前后台系统众多，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；二是多个方面都要求升级改造，大大增加系统投资和维护成本。

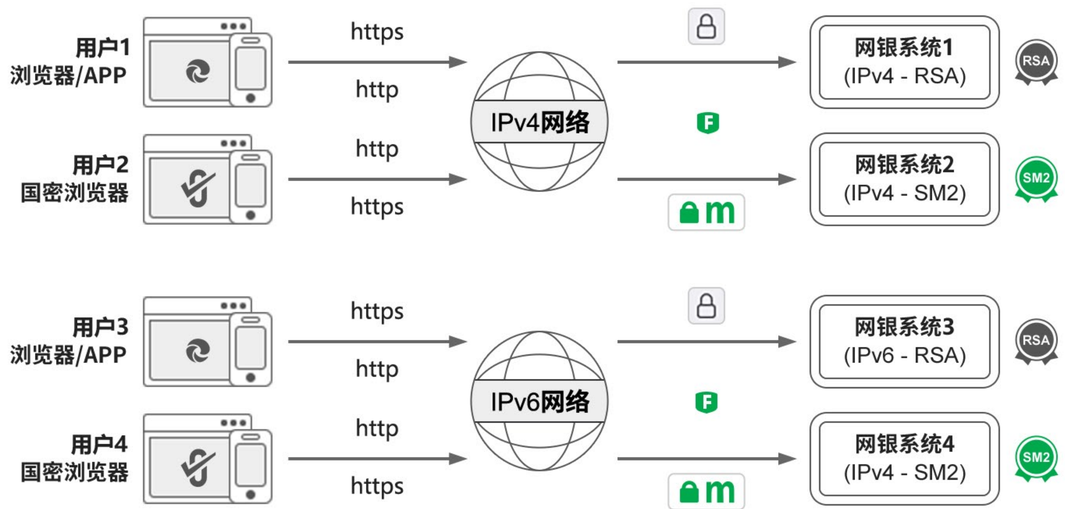
从统计数据展现的SSL证书申请量的数据来看，排名第一位的是工商银行，有672张，这么多张SSL证书所要部署应用的系统一定超过这个数字，可能有上千个网站系统需要人工部署这些证书，这个工作量巨大，带来的运维成本也是巨大的，并且每年必须更新一次。这就是网银系统建设和运维面临的第一个大难题，这就不能理解为何四大银行中还有部分网银服务居然还是以不安全的明文HTTP方式提供，这是不能接受的，这无法保障用户的银行账户安全，也是不合规的做法。

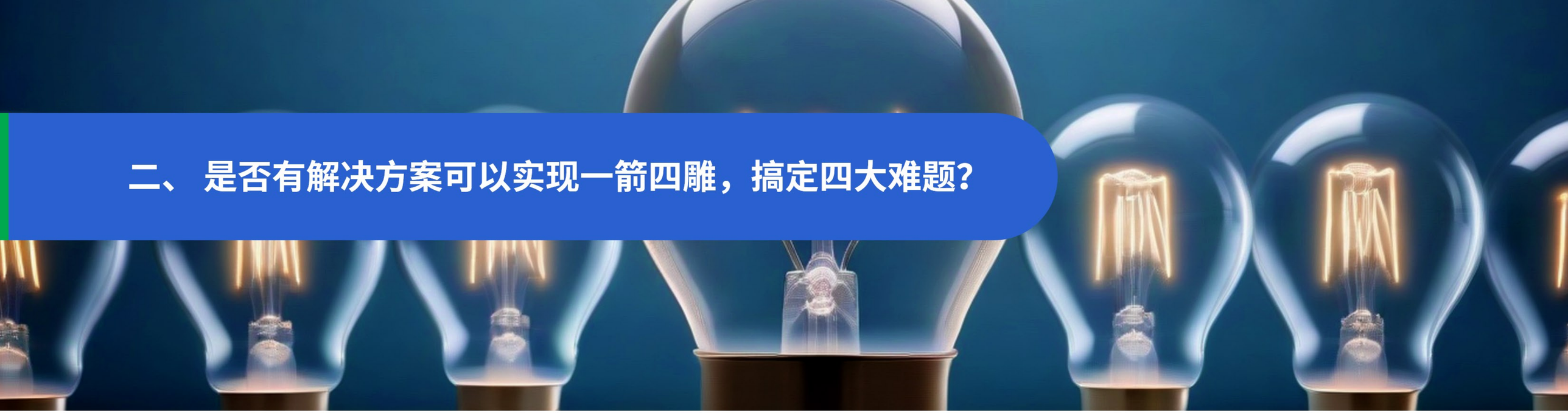
从统计数据还可以看出：20大银行只有7家银行网银系统实现了国密HTTPS加密，只有一家银行的官网可以使用国密HTTPS加密方式访问，其他家要么是RSA算法HTTPS方式访问，要么是不安全的明文HTTP方式访问。这些数据也印证了多个银行IT主管抱怨的国密改造难的问题，因为要想实现国密HTTPS加密，不仅要向CA购买和申请国密SSL证书，而且还要改造Web服务器支持国密算法和国密SSL证书，但是有些银行Web服务器根本是无法改造支持国密算法的。据了解，这些银行只好建设两套网银系统，一套支持RSA算法的老系统，一套支持SM2算法的新系统，两套系统采用不同的域名登录使用，无法做到自适应算法的一套系统登录使用。也就是说：网银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的增加和双倍系统的投资。这是网银系统面临的第二个大难题，这个难题严重影响了各大银行彻底完成国密改造的进度、广度和深度。

网银系统面临的第三个难题就是WAF防护，在各种Web应用攻击不断加剧的形势下，网银系统不仅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。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，必须支持HTTPS加密，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设备不支持国密算法和国密SSL证书，这也严重影响了网银系统普及部署WAF设备来保障网银系统Web应用安全。

网银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，这对于比较老的系统可能无法升级支持，毕竟网银系统有二十多年的发展历史了。所以，目前银行的做法只能再花钱搞两台套支持IPv6的网银系统，这无形之中又增加了网银系统的投资和维护成本。

网银系统为了满足国密改造和IPv6改造的合规要求，建设了4套网银系统来满足要求，这不仅仅是大大增加了网银系统投资的问题，而且大大增加了网银系统的复杂性和维护难度，从而降低了网银系统的可靠性，这绝对不是一个好的解决方案，是一个为了应对合规检查的无奈之举。





二、 是否有解决方案可以实现一箭四雕，搞定四大难题?

目前网银系统普遍采用的建设四套系统的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。所有网银系统的申请和部署SSL证书工作一般都要求多人一同进机房生成证书请求文件(CSR)，拿到SSL证书后又要求多人一同进机房部署证书，这个多人参与的工作一年一次，已经非常繁琐和费力了。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，也即是说，原先一年更新一次的工作量将翻5倍，一年要更新5次，多人同时进出机房10次为几十台、甚至上百台服务器和网站系统更新SSL证书，这将是一个不可能实现的任务，而不仅仅是以上列出的四大难题。这些难题已经严重影响了网银系统普及应用国密算法来保障我国网银系统安全，严重影响了各大银行的国密合规进程。怎么办？是否有更好的解决方案?

大家能想到的只有ACME技术(自动化证书管理环境)，但是，到目前为止，没有一个银行的网银系统启用了国外的自动化部署国际SSL证书实现HTTPS加密，这与网银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，不能实现商密SSL证书的自动化部署，无法实现商密HTTPS加密自动化。另外，网银安全急需的WAF设备基本上都还不支持ACME技术，仍然需要人工申请和部署SSL证书。

要解决网银系统面临的以上四大难题，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网银系统面临的问题，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，但是需要支持商密算法实现商密HTTPS加密，实现商密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访问网银服务。

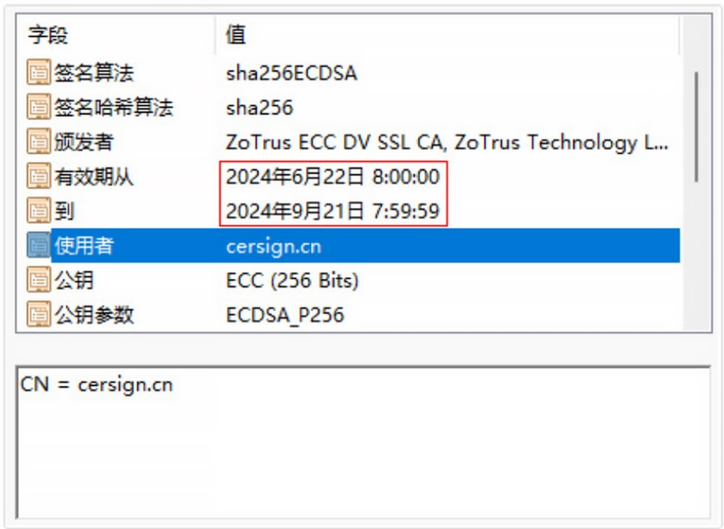
这些都是摆在银行IT主管们面前的现实问题和技术难题，必须寻找一个好的解决方案彻底解决这4个棘手的难题，而不是现在的建设四套不同的系统的临时方案。

三、 零信网关，自动化搞定网银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。

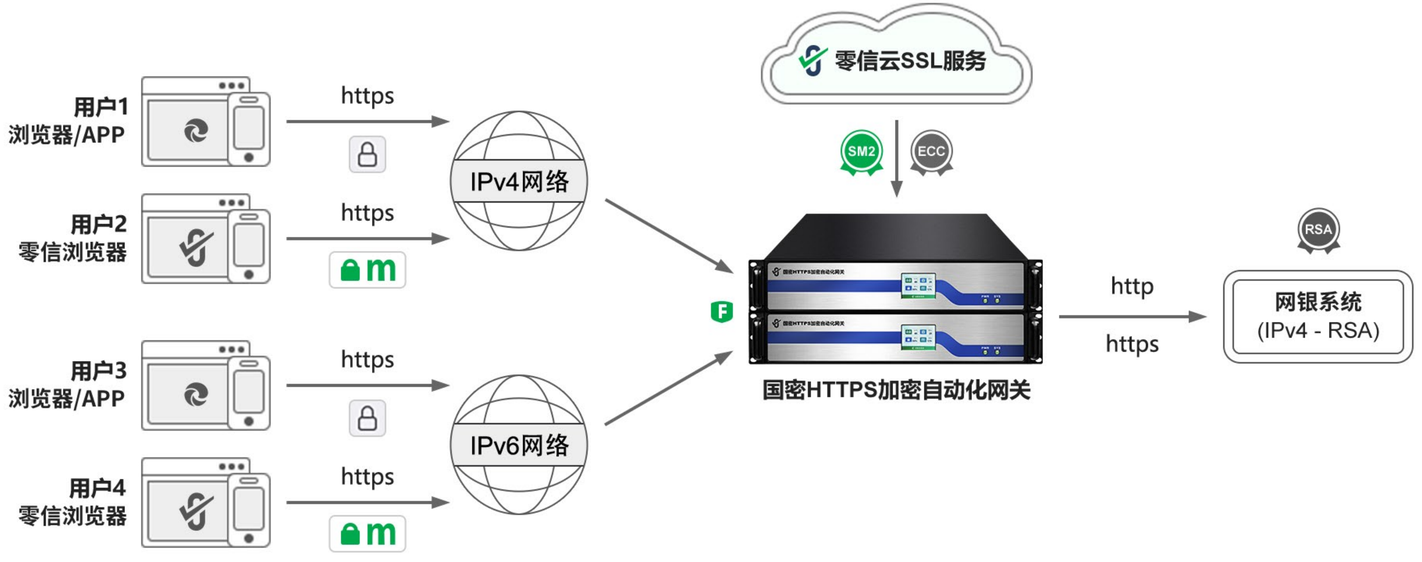
零信国密HTTPS加密自动化网关最大的特点和特色是用户无需向CA申请SSL证书，自动化申请双算法SSL证书(国密OV SSL证书和国际DV SSL证书)、自动化安装双SSL证书，并且已经提前满足将来90天有效期证书政策，自动化实现商密HTTPS加密，自适应加密算法，支持国密算法和国密证书透明的国密浏览器采用SM2算法实现国密HTTPS加密，不支持国密算法和国密证书透明的其他浏览器采用国际ECC算法实现HTTPS加密。这是一个端云一体的创新解决方案，国密HTTPS加密自动化网关内置国密ACME客户端，自动对接零信云SSL系统，自动化完成双算法SSL证书申请、部署和续期，确保业务系统零改造实现HTTPS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

传统方案需要为网银系统建设四套系统来满足四种不同用户使用网银服务的需求，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网络的网银系统零改造，零安装SSL证书，自动化满足四种用户的网银服务需求，如下图所示。



网银系统部署零信国密HTTPS加密自动化网关后，可以实现：

HTTPS加密自动化

原网银系统Web服务器零改造，零安装任何软件，不再需要多人一起去机房生成CSR文件和安装SSL证书，只需部署零信网关，设置网银域名，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网银系统安全运维工作。

国密HTTPS加密自动化

零信网关让原网银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网银系统，只需在现有的网银系统前面部署零信国密HTTPS加密自动化网关即可，自动化配置国密OV SSL证书，自动化实现国密HTTPS加密，原网银系统零改造，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，无需向CA购买和申请国密SSL证书和无需人工安装部署，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，反正都是机器自动化定期申请和安装。

3

WAF防护自动化

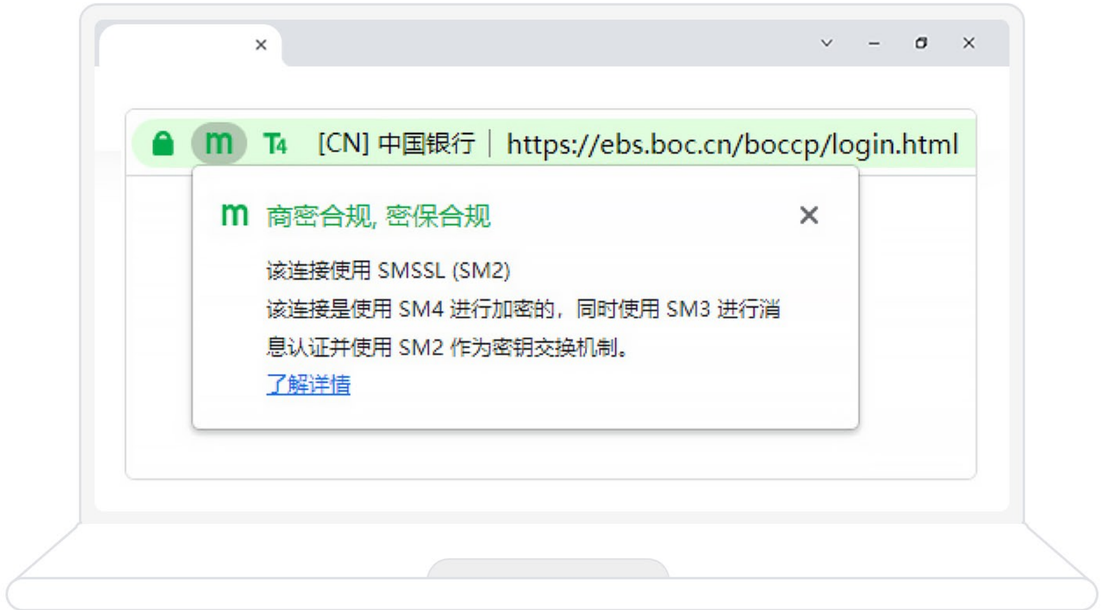
无需另外花钱购置WAF设备，也无需为部署和更新WAF设备所需的SSL证书发愁，只需部署零信国密HTTPS加密自动化网关，就可以自动化实现HTTPS加密方式的WAF防护，WAF防护的检测能力和识别能力都达到A级(最高级别)，防护性能甚至超过售价百万的WAF设备，并且是同时支持国际算法HTTPS加密和国密算法HTTPS加密自动化的WAF防护。

4

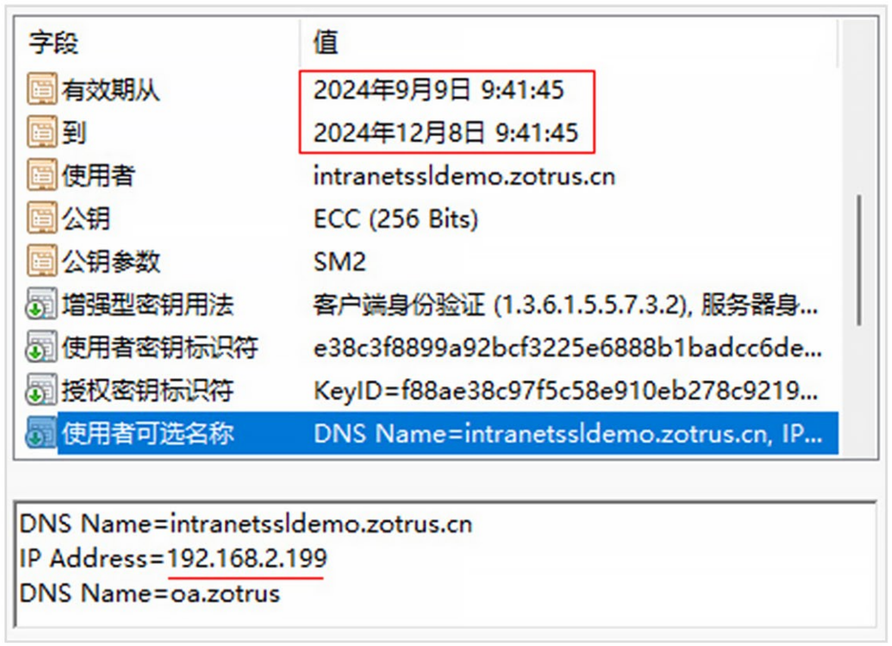
零改造搞定IPv6支持

原网银系统Web服务器和内网无需改造，但网银用户可以使用IPv6访问网银系统，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。

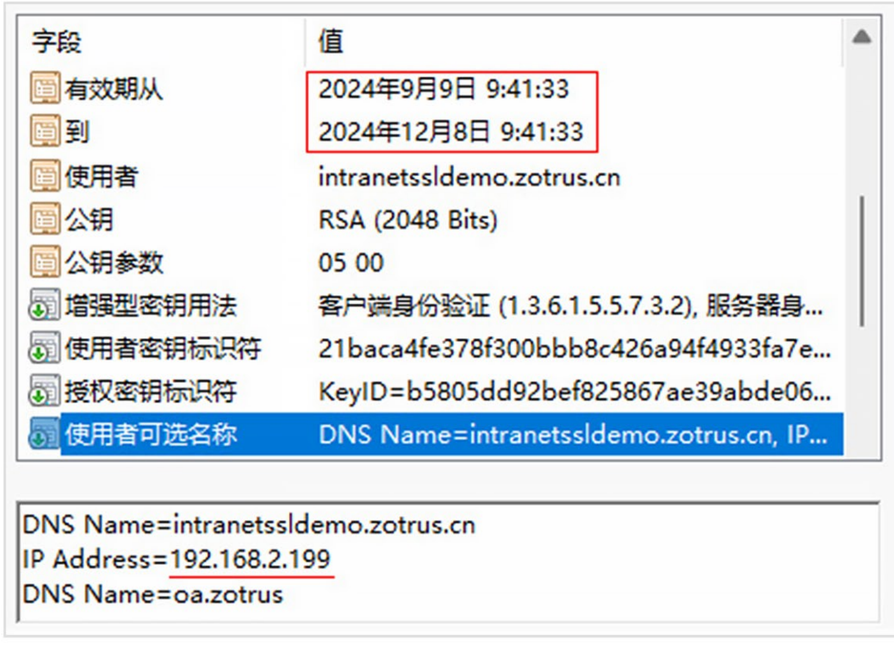
不仅如此，零信技术还提供完全免费不限数量配套的国密浏览器—零信浏览器，优先采用国密算法安全访问网银系统，确保了即使RSA算法SSL证书被非法吊销也不影响用户正常访问网银系统和正常使用网银服务。零信网关还免费赠送零信浏览器网站可信EV认证，让零信浏览器在地址栏绿色显示银行名称，提升网银系统防假冒能力，有力保障网银用户账户安全。



以上解决方案不仅仅适用于位于公网的网银系统、银行官网和业务管理系统，同时适用于位于内网的银行内部业务管理系统，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，以满足银行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

四、 零信方案为银行提供六大超值服务

零信技术提供的自动化证书管理方案，不仅仅用于银行的网银系统，还可以用于银行官网和其他业务管理系统，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/SM2两套网银系统，节省系统重复建设成本100万元；

05 自动化，无需建设IPv4/IPv6两套网银系统，节省系统重复建设成本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；

02 自动化，快速部署国密SSL证书，保障网银系统不会受到地缘政治的SSL证书断供影响；

03 自动化，不会出现人工申请SSL证书的忘了到时续期和部署的严重问题；

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，覆盖银行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，真正实现现有系统零改造，不影响现有业务系统正常运行，无缝升级完成改造。

五、唯有自动化，才能提供不间断的网银优质服务

国家有关部门已经多次发文要求各大银行必须全面完成国密改造，其中最重要的是网银系统国密改造，这是公众使用银行服务的入口，而网银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密码体系的网银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，以满足网银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网银服务。零信网关实现了一个网关搞定网银升级改造4个棘手的难题，是网银系统升级改造的首选产品。

不仅如此，要想保障网银Web系统全程安全，银行还需要改进网银APP的SSL证书验证机制，因为现在用户使用网银APP已经比使用浏览器登录网银系统更普及，这就要求网银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网银系统部署的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网银APP。并且网银APP必须优先采用国密算法实现HTTPS加密，这样才能保证不受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网银服务。