一个网关搞定四个棘手的网银系统升级改造难题

笔者最近同多家银行 IT 主管和某省人行科技处领导交流网银系统国密改造方案，通过同这些主管们的沟通大致了解了银行的网上银行系统在国密改造中遇到的难题，也了解了银行在 IPv6 网络升级改造中遇到的难题，同时也了解了网银系统 Web 应用安全防护问题。通过交流，大家还是很认可零信技术自动化证书管理解决方案的。

这位人行科技处领导还说：怎么以前没有听说过有这么好的自动化解决方案呢？各个银行费了好大的力气才算勉强完成国密改造的任务，如果早知道有自动化的方案，那早就完成改造了。现在都基本完成改造，你的方案还需要吗？笔者告诉这位领导：当然仍然需要！即使完成了改造，也仍然是人工申请和部署双 SSL 证书的方案，而我们的方案是自动化一劳永逸的解决方案。我如果还在 CA 的位置上，一定仍然是推荐买国密 SSL 证书、改造 Web 服务器和部署国密 SSL 证书的方案。现在我已经跳出了 CA 思维，才能想到银行实际需要的不是 SSL 证书，是要实现 HTTPS 加密，实现国密 HTTPS 加密，是要完成国密改造。所以才有了我们的创新方案—零改造实现国密 HTTPS 加密。当然，这也是借鉴国际流行的普遍采用的 ACME 技术，本文将详细讲述我们的解决方案，让银行 IT 主管们能详细了解零信网关的创新之处，了解如何采用零信网关搞定 4 个棘手的网银系统升级改造难题。

一、 网银系统为何需要升级改造？有哪些需要改造的？

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。

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，这是 2023 年 Q3 的数据，一年后的今天的最新的数据是 802 张证书，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，这是笔者不能接受的，这无法保障用户的银行账户安全，也是不合规的做法。

排名	银行名称	检索域名	证书数	DigiCert(美)	中金认证(中)	其他CA	国外CA%	国密证书	全站HTTPS
1	工商银行	icbc.com.cn	672	652	16	4	97.62%	有	是
2	建设银行	ccb.com	562	266	222	74	60.50%	无	不是
3	农业银行	abchina.com	81	78		3	100.00%	有	是
4	中国银行	boc.cn	224	221		3	100.00%	有	是
5	交通银行	bankcomm.com	75	11	1	63	98.67%	无	不是
6	招商银行	cmbchina.com	338	330		8	100.00%	无	是
7	邮储银行	psbc.com	124	25	81	18	34.68%	有	不是
8	兴业银行	cib.com.cn	271	271			100.00%	是	是
9	浦发银行	spdb.com.cn	82	45	36	1	56.10%	无	是
10	中信银行	ecitic.com	139	138		1	100.00%	无	不是
11	民生银行	cmbc.com.cn	28			28	100.00%	无	不是
12	光大银行	cebbank.com	78	39	27	12	65.38%	无	不是
13	平安银行	pingan.com.cn	161	145		16	100.00%	无	不是
14	华夏银行	hxb.com.cn	121	23	69	29	42.98%	无	是
15	北京银行	bankofbeijing.com.cn	108	62	19	27	82.41%	有	是
16	广发银行	cgbchina.com.cn	17	15		2	100.00%	无	不是
17	上海银行	bankofshanghai.com	5	3	1	1	80.00%	无	是
18	江苏银行	jsbchina.cn	9	4		5	100.00%	无	不是
19	宁波银行	nbcb.com.cn	14	8		6	100.00%	无	不是
20	浙商银行	czbank.com	49	49			100.00%	有	不是
合计			**3,158**	**2,385**	**472**	**301**	**85.05%**	**7**	**9**

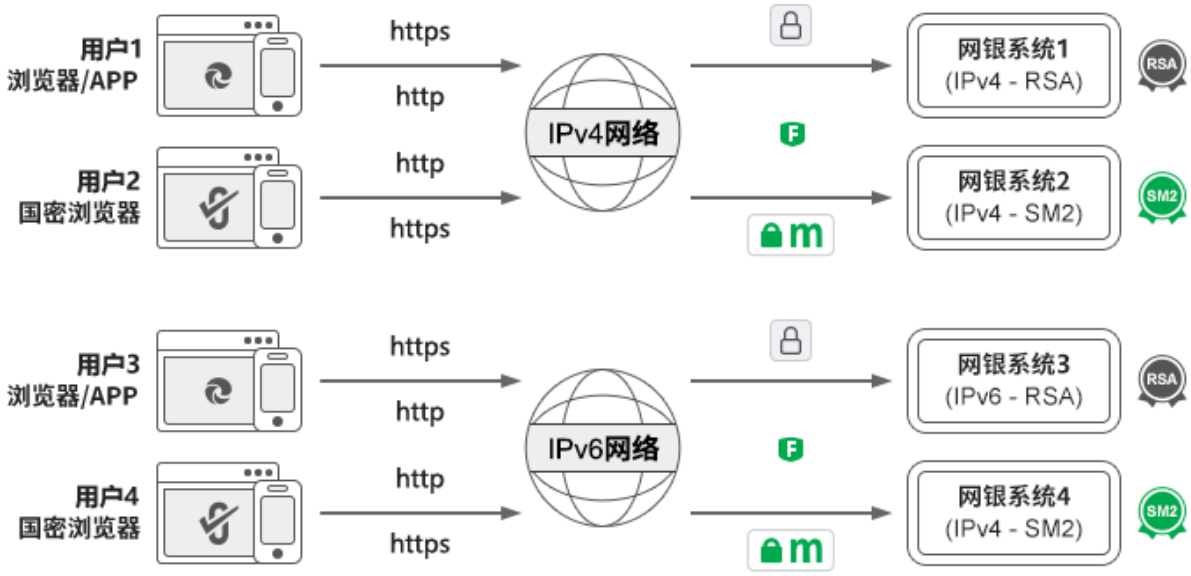
从上面的统计数据还可以看出：20 大银行只要 7 家银行网银系统实现了国密 HTTPS 加密，只有一家银行的官网可以使用国密 HTTPS 加密方式访问，其他家要么是 RSA 算法 HTTPS 方式访问，要么是不安全的明文 HTTP 方式访问。这些数据也印证了多个银行 IT 主管抱怨的国密改造难的问题，因为要想实现国密 HTTPS 加密，不仅要向 CA 购买和申请国密 SSL 证书，而且还要改造 Web 服务器支持国密算法和国密 SSL 证书，但是有些银行 Web 服务器根本是无法改造支持国密算法的。据了解，这些银行只好建设两套网银系统，一套支持 RSA 算法的老系统，一套支持 SM2 算法的新系统，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。

大家可以看出，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？

大家可能会想到 ACME 技术(自动化证书管理环境)，但是，到目前为止，笔者并没有发现哪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，这应该是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。还有，市场上的 WAF 设备都还不支持 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：

(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，但是需要支持商密算法实现商密 HTTPS 加密，实现商密 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 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。

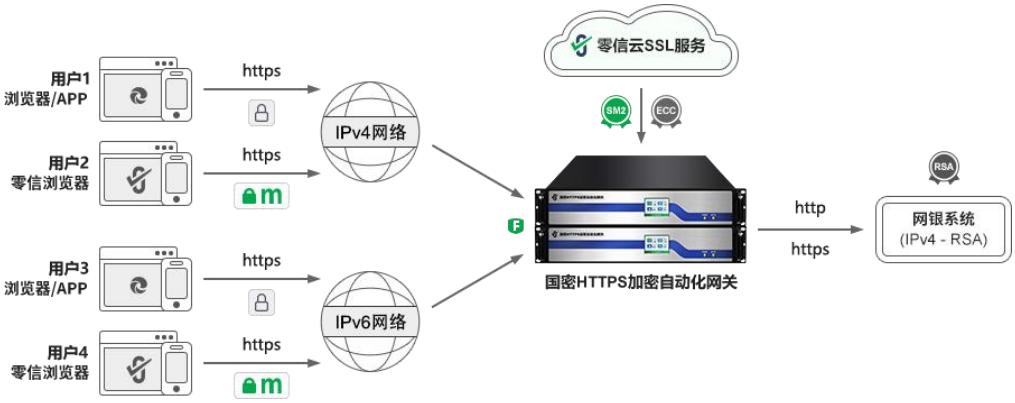
三、 零信网关，自动化搞定网银系统升级改造四大难题

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自动化申请双算法 SSL 证书、自动化安装双 SSL 证书、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。

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：

(1) **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，不用多人一起去机房生成 CSR 文件和安装 SSL 证书，只需一次配置网银域名，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(自动配置的双算法 SSL 证书价值高达 623 万元)，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。

(2) **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。

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。

有诗为证：

网银系统改造，商密应用最是关键。
部署零信网关，一机搞定四大难题。
自动化，多快好省，完成四大改造。
自动化，保网银系统持续可靠运行。

王高华

2024 年 8 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 175 篇(共 48 万 4 千多字)和英文 68 篇(8 万 4 千多单词)。。