解读《关于加强银行业保险业移动互联网应用程序管理的通知》

国家金融监督管理总局在 9 月 14 日印发了《关于加强银行业保险业移动互联网应用程序管理的通知》(以下简称《通知》)，笔者看到这个《通知》时有似曾相识的感觉，这是继 5 月 22 日网信办、中央编办、工信部和公安部联合发布的《互联网政务应用安全管理规定》(以下简称《规定》)之后的专门针对金融移动互联网应用的安全管理通知，可以理解为是《规定》在金融保险业的落实要求。因为按照《规定》第四十二条要求，银行业保险业的移动应用程序的安全管理参照规定有关内容执行，所以，请广大读者同时参考阅读 解读《互联网政务应用安全管理规定》，笔者不再重复相关内容，仅针对银行业保险业移动应用程序安全做出更加详细的解读和整改指引。

一、 银行业保险业移动应用程序存在哪些安全问题？

《通知》的印发说明了管理部门已经充分认识到目前金融业 APP 存在的诸多问题，笔者仅解读 SSL 证书安全相关的问题，这不仅仅是笔者的专长，也是《通知》的核心关切，《通知》要求金融机构落实移动应用备案、网络安全、数据安全、外包管理、业务连续性及个人信息保护等监管要求，对用户活跃度低、体验差、功能冗余、安全合规风险隐患大的移动应用及时进行优化整合或终止运营。

金融 APP 在网络安全和数据安全方面普遍存在的安全合规风险隐患来自如下四个方面：

1. 金融 APP 的 HTTPS 加密合规方面存在很多安全问题

根据零信技术安全团队对多家银行的网银 APP 的研究，几乎所有金融 APP 都存在如下多个问题：

(1) 金融 APP 在 HTTPS 连接服务端时不验证服务端的 SSL 证书是否可信；

(2) 金融 APP 在 HTTPS 连接服务端时不验证服务端的 SSL 证书绑定的域名是否正确；

(3) 金融 APP 在 HTTPS 连接服务端时不验证服务端的 SSL 证书是否已吊销；

(4) 金融 APP 在 HTTPS 连接服务端时不验证服务端的 SSL 证书是否过期，也不验证 SSL 证书有效期是否合规；

(5) 金融 APP 同服务端 SSL 通信握手时不能选择最安全的加密套件，因为服务器端

部署 SSL 证书时并没有禁用不安全的加密套件；

(6) 金融 APP 不支持国密算法实现 HTTPS 加密，不能优先采用国密算法实现 HTTPS 加密，这个属于非常严重的不合规问题。

这些对网银系统服务器端 SSL 证书的合法性判断缺失的话，就极有可能在用户手机上网环境不安全的情况被 DNS 劫持到一个假冒的网银系统导致泄露用户的银行卡口令和网银系统口令，从而导致用户银行账户的现金被非法转走或取现，给用户带来财产损失。而这种财产损失不仅仅是用户上网环境不安全的责任，更主要的是金融 APP 的不严格验证服务端 SSL 证书而导致的，更大的主要责任在银行，这就是《通知》要求的整改的安全漏洞。而导致这些安全问题的根本原因是 APP 开发者没有做这些额外的证书合法性验证，而只是简单地启用 HTTPS 加密。

2. 金融 APP 采用 HTTPS 安全连接的网银服务端部署的 SSL 证书也存在不少安全问题

要完成一个完整的金融移动应用安全连接，不仅需要确保金融 APP 的安全合规，而且需要金融 APP 连接的服务端部署的 SSL 证书也必须是安全地部署，零信技术安全团队体检了几十个网银系统部署的 SSL 证书，发现有接近一半的网银系统部署的 SSL 证书安全评级为 **F**(非常不安全)，主要有如下三个方面的严重问题：

(1) 没有关闭非常不安全的加密套件(如 RC4、MD5、DES 等)，支持弱密钥交换，这就导致攻击者故意使用弱强度加密套件同网银系统握手通信，进而破解相关的网银系统通信机制而攻击用户账户；

(2) 普遍的没有关闭不安全的 TLS 1.0 和 1.1 协议，甚至有的没有关闭非常不安全的 SSL 3 协议；

(3) 多个安全漏洞没有修复(如 Zombie POODLE 漏洞)、不支持安全协商、前向安全等等。

还有一个非常重要的 SSL 证书部署问题：没有部署完整的 SSL 证书证书链，这使得浏览器和金融 APP 无法正确识别和判断 SSL 证书是否可信，这虽然不属于安全问题，但是非常影响用户体验，也极有可能给假冒网站有了可乘之机，如果要求用户信任浏览器有安全警告的网银网站的话。

3. 使用不安全的国密浏览器访问网银系统存在的安全问题

大家都知道网银系统都必须完成国密改造，包括 HTTPS 加密改造，这就要求有浏览器支持国密算法实现 HTTPS 加密。但是，零信浏览器安全团队发现市场上常用的国密浏览器存在不少安全问题不适合用于网银系统访问，请各个银行保险机构在选用国密浏览器仔细检查所用国密浏览器是否有如下 6 个方面的安全问题：

(1) 浏览器不验证签发国密 SSL 证书的根证书是否可信，不验证是否由拥有 CA 许可证的 CA 机构签发；

(2) 浏览器不验证国密 SSL 证书是否已经吊销；

(3) 浏览器不验证国密 SSL 证书是否过期，也不验收国密 SSL 证书有效期是否超过 1 年；

(4) 浏览器不验证国密 SSL 证书绑定的 IP 地址和域名是否是公网 IP 地址和公网域名；

(5) 浏览器不验证所访问的网址是否同国密 SSL 证书中绑定的域名一致；

(6) 浏览器不能优先采用国密算法实现 HTTPS 加密，即使网银系统部署了国密 SSL 证书仍然使用 RSA 算法实现 HTTPS 加密。

有以上问题的国密浏览器是无法保障用户网银访问安全的，不适合用于网银系统国密改造和网银用户上网银系统办理网上银行业务。

4. 网银系统部署的国密 SSL 证书也存在不少安全问题

最后一个问题是用于网银系统的国密 SSL 证书自身安全问题，具体有如下 3 点：

(1) 国密 SSL 证书有效期超过 1 年，这不仅不合规，而且非常不安全(私钥不安全)。银行机构不能图部署简单而申请和部署了超过 1 年有效期的国密 SSL 证书，规范的国密浏览器会不信任这些超长有效期的国密 SSL 证书。

(2) 国密 SSL 证书不支持证书透明，这意味着 CA 机构可以在银行不知情的情况下任意签发绑定其域名的国密 SSL 证书而不对外公示其签发行为，这是不可信的证书签发行为。银行在选购国密 SSL 证书时一定要同 CA 机构明确要求支持证书透明。

(3) 多家 CA 机构签发的国密 SSL 证书中不含有签发中级根的 AIA 网址，或者即使有也无法访问，这个问题会影响到国密浏览器和网银 APP 正常访问网银系统和正常验证网银系统部署的 SSL 证书。

以上这些问题非常值得银行业保险业 IT 主管们高度重视，必须在选购国密 SSL 证书时向

CA 机构强调不能存在这些问题，并选择向没有这些问题的 CA 机构申请国密 SSL 证书。

二、 如何整改才能满足《通知》和《规定》的要求？

《通知》要求各个银行业保险业主必须及时发现问题和及时整改问题，大家可以对照笔者在上一部分列出的金融 APP、Web 服务器 SSL 证书部署、网银用浏览器和网银用 SSL 证书存在的各种问题一一排查是否存在这些问题，如果存在，则必须一一解决。

1. 金融 APP 的 HTTPS 加密合规方面存在的问题整改方案

金融 APP 普遍存在的这 6 大证书安全问题，需要金融机构同 APP 开发商一一核实并验证问题是否存在，并在整改完成后验证是否已经完成整改。这些问题都必须整改，当然最核心的问题是一定要支持国密算法实现 HTTPS 加密，并且是优先采用国密算法实现，只有这样才是最终达到了国密改造的目的。

2. 金融 APP 采用 HTTPS 安全连接的网银服务端存在的问题整改方案

这是网银 Web 服务器或者网关的 SSL 证书部署问题，对于国际算法 SSL 证书，一定要用 Qualys SSL Labs 的在线体检工具对每一个部署 SSL 证书的网站进行体检，发现问题及时调整服务器配置文件，关闭不安全的加密套件和加密协议。对于其他安全漏洞也要根据体检结果做及时修复，只有体检结果达到 A 级或 A+级才是安全的 SSL 证书部署。

而对于国密 SSL 证书的部署，最常见的问题是没有部署完整的 SSL 证书链，而 SSL 证书又没有可以访问的 AIA 信息，则浏览器是无法正常显示的。目前市场上没有可用的类似于 SSL Labs 一样的国密 HTTPS 加密体检工具，建议在完成部署后使用零信浏览器访问，如果零信浏览器不能正常显示国密加密标识 **m**，则一定是部署有问题，或一定是零信浏览器不信任的国密 SSL 证书。

3. 使用不安全的国密浏览器访问网银系统存在的安全问题整改方案

要想检验正在使用的国密浏览器是否正常验证了部署的国密 SSL 证书，这需要一定的专业知识，最简单的方法是同一个网站同时使用零信浏览器访问，看看零信浏览器是否有安全警告，如果有，会显示具体安全问题。但是如果正在使用的其他国密浏览器却没有警告，则说明这个浏览器并没有严格按照国际标准和国密标准来验证国密 SSL 证书，建议弃用此浏览器。

4. 网银系统用国密 SSL 证书存在的安全问题整改方案

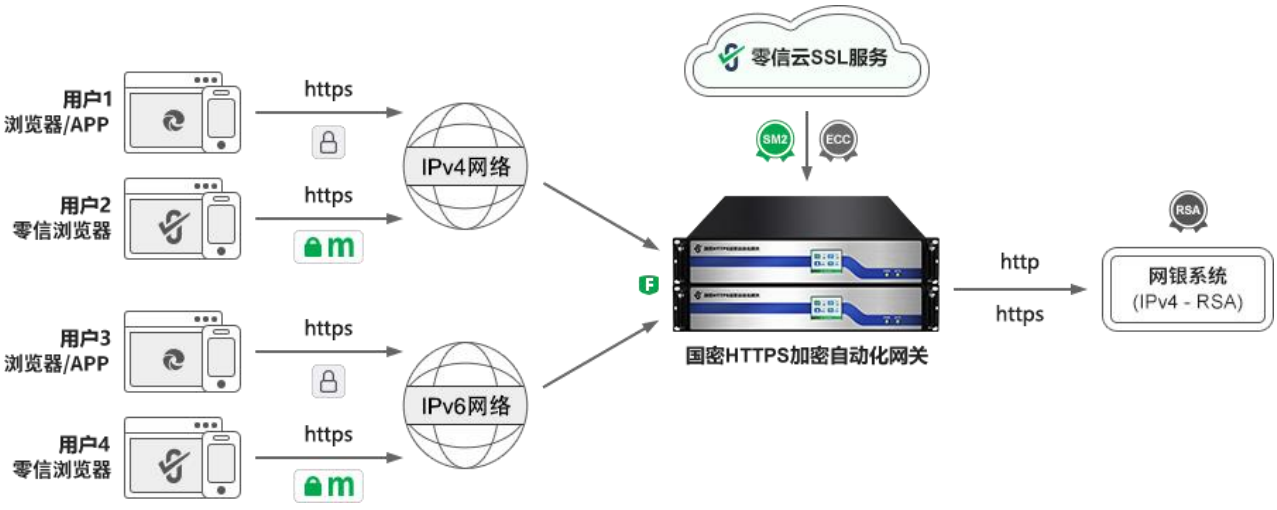
针对上部分指出的国密 SSL 证书常见的三个问题，第一问题很容易发现，大家看看一下你同时申请的国际 SSL 证书有效期一定只有 1 年，但是如果你同时拿到的国密 SSL 证书超过一年，则就是不合格的国密 SSL 证书。

对于国密 SSL 证书是否支持证书透明，大家也可以对比手中的国际 SSL 证书，一定有一个“SCT 列表”字段，如果你手中的国密 SSL 证书中没有这个字段，则就是不支持证书透明，也可以认为是不合格的国密 SSL 证书，因为 CA 在签发这张国密 SSL 证书时没有透明公示其签发行为，这样的国际 SSL 证书谷歌浏览器是不信任的，而零信浏览器目前对于不支持证书透明的国密 SSL 证书只是显示“证书不透明”，计划将来也像谷歌浏览器一样不信任这样的国密 SSL 证书。建议用户选购支持国密证书透明的国密 SSL 证书，保障国密 SSL 证书的自身安全可信。

而对于 AIA 网址，大家可以查看国密 SSL 证书中是否有 AIA 信息，如果有，复制这个网址使用浏览器访问，看看是否可以下载下来查看签发这张国密 SSL 证书的签发 CA 证书，如果正确，则是一个合格的证书。如果没有这个字段或者有这个字段无法访问，则不是一张合格的国密 SSL 证书。

三、 零信技术提供哪些产品助力快速完成整改？

上一部分提出的整改方案并不是最佳方案，有些还需要相当高的专业知识才能发现问题所在。最简单的整改方案是在 Web 服务器之前部署零信国密 HTTPS 加密自动化网关，一个网关自动化搞定网银系统四个方案的升级改造难题，包括国际算法 HTTPS 加密自动化、国密算法 HTTPS 加密自动化、WAF 防护自动化和 IPv6 改造自动化。一个网关能自动化完成上述所有除了金融 APP 的验证问题以外的其他所有问题。



部署零信网关的网站使用 SSL Labs 体检能保证每一个网站体检安全评价都是 A 级，使用完全免费的干净无广告的国密浏览器--零信浏览器访问部署的零信网关的网银系统，一定是采用国密算法实现 HTTPS 加密，并且严格按照国际标准和国密标准来验证 SSL 证书。同时，零信浏览器会在地址栏展示国密加密标识、WAF 防护标识，查看国密 SSL 证书一定会显示国密证书透明信息。

部署零信网关让银行不再需要向 CA 机构申请和人工手动部署双算法 SSL 证书，由零信网关自动化对接零信云 SSL 服务系统自动化完成双证书申请和部署。自动化配置的国际 SSL 证书由全球信任的第二大 CA-Sectigo 签发，国密 SSL 证书由拥有 CA 许可证的贵州 CA 签发，双 SSL 证书都支持证书透明，能满足金融保险业 HTTPS 加密国密改造需要，满足《通知》的整改要求，一键完成整改，一键完成合规。

王高华

2024 年 9 月 25 日于深圳