90 天 SSL 证书对策二：企业篇

90 天 SSL 证书的倒计时开始了，我国做好准备了？该如何应对国际标准将把 SSL 证书有效期从目前的 1 年缩短到 90 天，笔者将针对四个不同的行业提出相应的对策，分四篇：政务篇、企业篇、云平台篇和 CA 篇，政务篇已于 10 月 19 日发表，今天写企业篇，企业数据是企业生存的关键资产，不仅需要保护其在服务器中的安全(在岸安全)，还需要保护其在流通中的安全(在途安全)，这就需要 HTTPS 加密。

一、 企业对保护数据普遍重视不够

相信企业 IT 主管们一定不会认为笔者这个提法，认为自己非常重视自己企业的数据保护。各类大小规模的企业无论是商贸企业还是生产企业一般都建设了各种信息管理系统，管理着企业赖以正常运作的各种重要数据，有些还是关系民生的数据，如航班信息。但是这些产生和管理重要用户数据的系统有许多都是 HTTP 明文传输系统，非常容易在数据流动过程中被非法窃取和非法篡改，请不认可笔者的提法的企业 IT 主管们检查一下自己的业务系统是否全部实现了 HTTPS 加密，相信仍然有许多系统并没有实现 HTTPS 加密，这是因为企业往往只重视传统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防护转化到云计算时代的数据保护上来。

笔者发现许多为政府和大型企业提供数据安全产品和服务的科技企业的官网也没有部署 SSL 证书，这是不可接受的，这样的企业提供的数据安全产品和服务也是不可信的，尽管获得了各种各样的奖项。因为 HTTPS 加密是数据安全的核心技术，数据是不可能不流动的，流动就需要 HTTPS 加密，如果该企业官网都没有部署 SSL 证书，极有可能给用户的解决方案也是没有采用 HTTPS 加密技术来保护用户系统的数据安全的，这样的解决方案就不可能是安全的方案。

也就是说，大家都想保护自己的数据，但是很多企业还是传统的保护理念，认为保护数据服务器的安全即可，或者做好数据使用的权限管理即可，或者把数据加密处理保存在数据库即可，这些都是传统的城堡安全思维。数据是需要流通的，只有流通才能产生价值，而流通就需要用户可以通过浏览器/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。

二、 保护企业数据从 HTTPS 加密开始

在目前的云计算和移动互联网时代，数据是在不断流动的，是全国范围设置全球范围的基于互联网的流动，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移动 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。

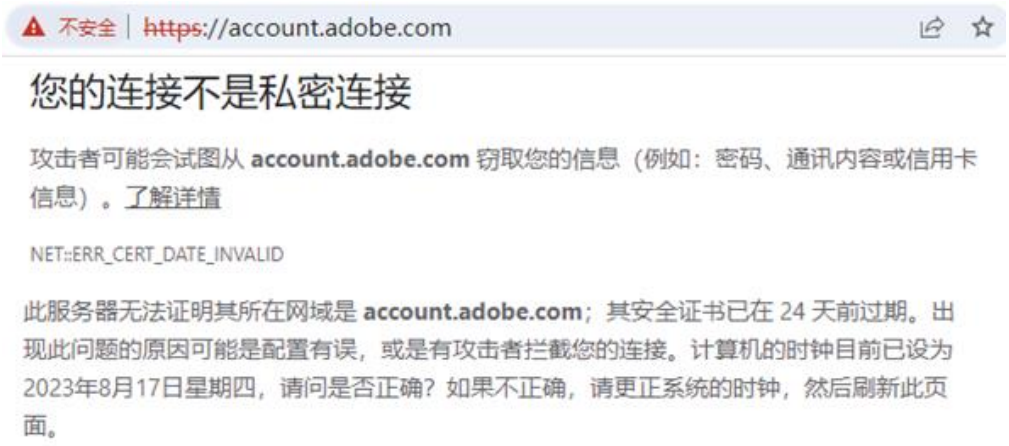
笔者从国际证书透明日志系统检索了如下八家央企域名的 SSL 证书申请量：国家电网(sgcc.com.cn)：139 张、中国烟草(tobacco.gov.cn)：13 张、中国石化(Sinopec.com): 138 张，中国石油(petrochina.com.cn)：22 张、中国铁路(12306)：173 张、中国移动(10086.cn)：888 张、国家电投(spic.com.cn)：20 张、中国船舶(cssc.net.cn)：2 张。从 SSL 证书的申请量就能看出各个企业对 HTTPS 加密的重视程度，因为大企业一定有许多业务系统，证书申请量少只能说明还要大量的业务系统没有实现 HTTPS 加密。从日志数据可以看出：中国移动排名第一位，这说明其对业务系统的数据安全保护工作的高度重视，而中国船舶仅申请了两张证书，也许是其业务系统没有用官网域名，但如果不是这种情况的话，则说明该集团很不重视企业数据保护，急需改进。

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 **1612** 张，这是我国申请证书最多的航空公司-国航的 28 张的 57 倍多，是国企中申请证书最多的中国移动的两倍，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。所以，保护企业数据安全，必须尽快为所有业务系统无论是在内网还是外网都必须全部实现 HTTPS 加密，只有这样才能保障重要的企业数据的“在岸”安全和“在途”安全，也就是全业务流程的全程安全。

而要实现 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，但是如果要管理像中国移动那样有 888 张 SSL 证书在上千台服务器上去使用，这个人工处理的工作量是巨大的，笔者的经验是超过 20 个网站就需要专门的工程师来运维了。这是大型企业面临的困境，知道必须部署 SSL 证书来实现 HTTPS 加密来保护数据传输，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。而笔者前段时间访问 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。



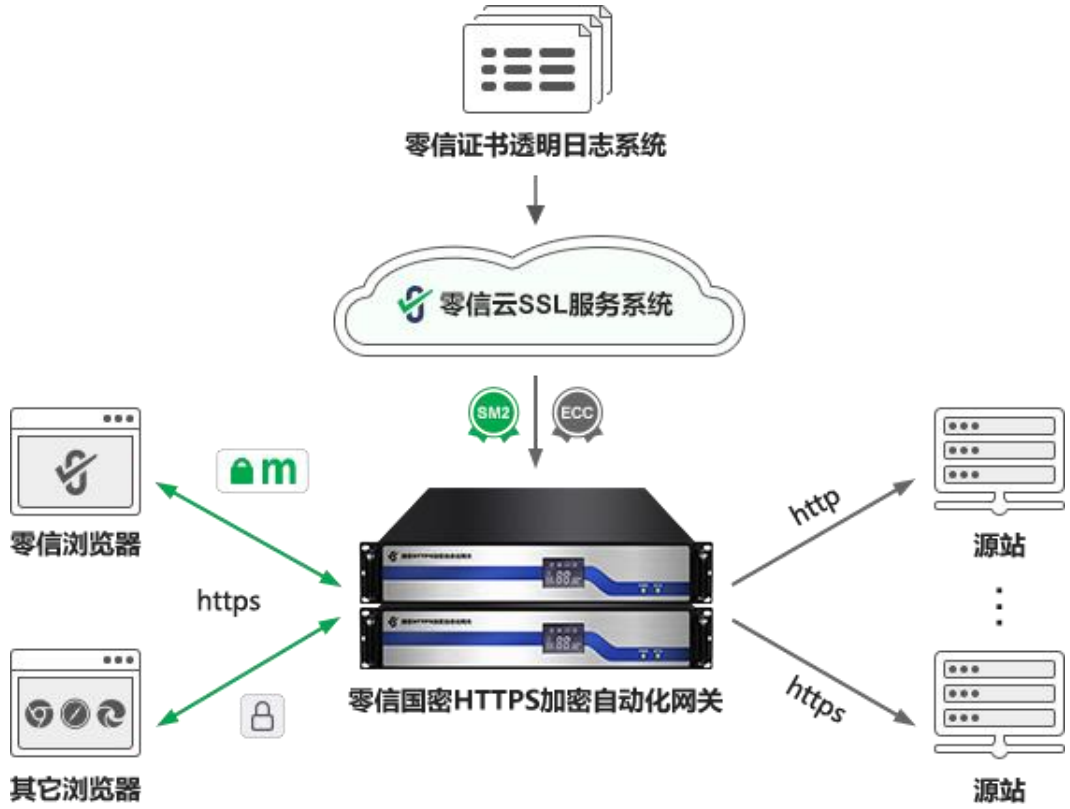
也就是说，在所有系统都必须普及实现 HTTPS 加密的时代，手工部署 SSL 证书来实现 HTTPS 已经力不从心，即使是大公司也如此。更加严峻的考验还在后头，谷歌正在推动缩短 SSL 证书有效期为 90 天，这意味着原先一年才申请和安装一次 SSL 证书的行为需要改为一年 5 次！连一年一次都会遗漏，更不用提一年 5 次了，这意味着手动申请和部署 SSL 证书已经不可能。怎么办？

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？

三、 全面实现 HTTPS 加密的唯一可行方案是部署国密 HTTPS 加密自动化网关

上面讨论了企业在全面实现所有网站系统 HTTPS 加密中遇到的三大难题，是否有一个解

决方案能帮助企业彻底解决这些难题？当然有，这就是零信技术全球独家推出的国密 HTTPS 加密自动化管理解决方案。用户无需向 CA 申请国际 SSL 证书和国密 SSL 证书，无需在原 Web 服务器上安装 SSL 证书，原 Web 服务器无需升级改造支持国密算法，也无需在服务器上安装 ACME 客户端软件，什么也不用动，不改动目前的业务系统服务器，只需在原服务器之前部署国密 HTTPS 加密自动化网关即可，直接一步到位自动化实现 HTTPS 加密，而且是自适应加密算法的 HTTPS 加密，支持国密算法的浏览器使用国密算法实现国密 HTTPS 加密，不支持国密算法的浏览器使用国际算法实现 HTTPS 加密，并且都是自动化实现。



这是突破了“国密改造”传统思路的解决方案，国密改造很难，那就不改造，保留现有的基于国际密码体系的用户端系统和服务端业务系统，由网关来自动化对接零信云 SSL 服务系统，自动化为网站域名配置双算法双 SSL 证书，双证书全部支持证书透明，由网关来实现国密加密算法到国际加密算法和明文 HTTP 的协议和算法转换，提供类似于 CDN 或 WAF 的 HTTPS 加密卸载转发服务。

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，让企业数据从产生就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 125 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 275 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“多”(好处)、“快”速实施、“好”用、“省”证书费用和人力成本的最佳解决方案。

有诗为证：

企业数据要保护，在岸防护还不够。

在途保护更重要，传输加密是关键。

部署网关最划算，多快好省自动化。

数据资产保护好，企业才有大发展。

王高华

2023 年 10 月 30 日于深圳

请关注公司公众号，实时推送公司 CEO 精彩博文。