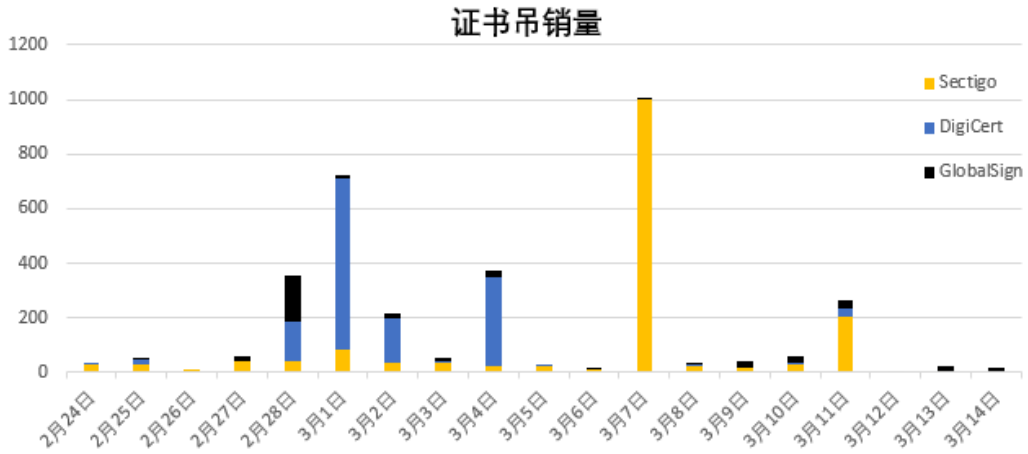
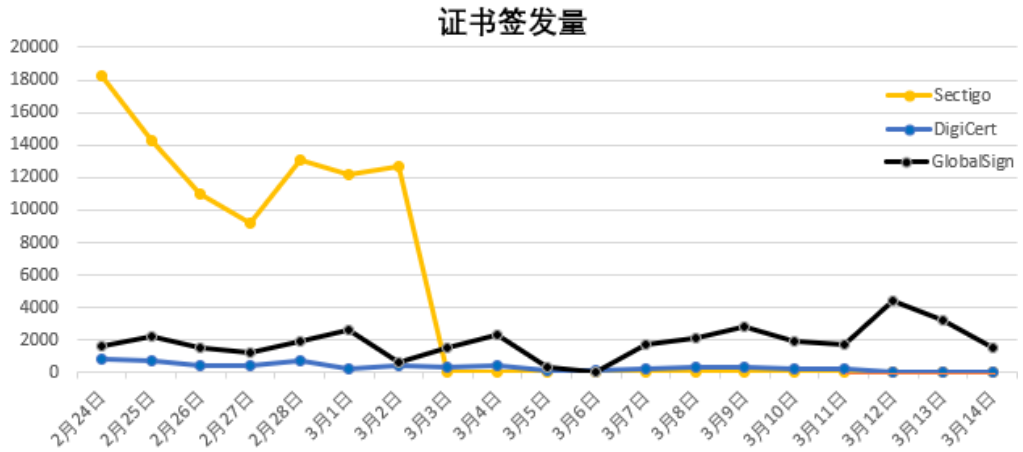
我国做好 SSL 证书“断供”的准备了吗？

今年 2 月 24 日发生了俄乌冲突，大量俄罗斯政府网站和银行网站的 RSA 算法 SSL 证书被吊销或断供。3 月 3 日 Sectigo 停止签发证书，3 月 12 日 DigiCert 停止签发证书，其他 CA 也纷纷停止签发证书，停止签发证书就是“断供”，就是网站无法实现 https 加密了！同时，从 2 月 27 日开始，Sectigo 开始吊销已经签发的 SSL 证书，13 天内共吊销 1576 张证书，DigiCert 2 月 28 日开始，共吊销了 1266 张证书。吊销证书就是禁用！以前已经签发给你的证书禁止使用！断供只是不再供货，而吊销则是即使供了货也不让用！





下图为笔者在 2019 年 8 月 20 日的第七届互联网安全大会的演讲的一页，当时笔者就提出了我国必须做好 SSL 证书“断供”的准备的观点。当时就有人说这不可能发生，但是现在真实地发生在俄罗斯！这不得不值得我们深思和警醒！

俄乌冲突给我国的安全启示是方方面面的，而在互联网安全特别是网站安全方面，RSA 算法 SSL 证书被吊销或断供，这给我国互联网安全，特别是关键信息基础设施安全敲响了警钟，我国必须快速进入国密 HTTPS 加密时代，以应对非常不确定的国际形势，保障我国互联网安全。

普及国密 HTTPS 加密不仅仅是应对国际形势的需要，而且也是《密码法》和《网站安全法》合规的需要，也许有读者认为现在的网站安全国密应用生态还不成熟，无法满足普及国密 HTTPS 加密的应用需求，本文就专门讲一讲这个错误认识问题。

要实现 HTTPS 加密，必须有 CA 签发 SSL 证书，并且必须支持证书透明，必须有浏览器信任签发 SSL 证书的根证书，有 Web 服务器支持签发这张 SSL 证书采用的加密算法，还必须有支持这种加密算法的浏览器可以用 HTTPS 加密协议实现安全的网页访问。也就是说，只有浏览器(包括移动 App)、SSL 证书和 Web 服务器都支持国密算法，才能实现国密 HTTPS 加密。当然，还需要 CDN 和云 WAF 服务提供商也支持国密 SSL 证书和国密算法。必须是整个 Web 生态都支持国密算法。笔者明确地告诉大家，这个国密 https 加密生态现在已经成熟了，是时候普及国密 HTTPS 加密了！

请大家看看笔者列出的支持国密 SSL 证书和国密算法的各个生态产品厂商清单，相信广大读者应该能明智地认为我的观点是正确的--国密 https 加密生态已经成熟了，是时候普及国密 HTTPS 加密了！

能签发国密 SSL 证书的厂商：证签技术、零信技术、数安时代、亚数信息、上海 CA、中金认证、天威诚信、沃通 CA、陕西 CA、网证通、贵州 CA、四川 CA 等。

支持国密算法和国密 SSL 证书的浏览器：零信浏览器、密信浏览器、奇安信浏览器、360 浏览器、红莲花浏览器等。推荐大家使用完全免费的零信浏览器。

支持国密算法和国密 SSL 证书的 Web 服务器：Nginx +国密模块，对于采用其他服务器软件的网站，可以部署 Nginx 作为前置代理机实现支持国密 HTTPS 加密。零信技术免费提供 Nginx 国密支持模块，一键重新编译即可。

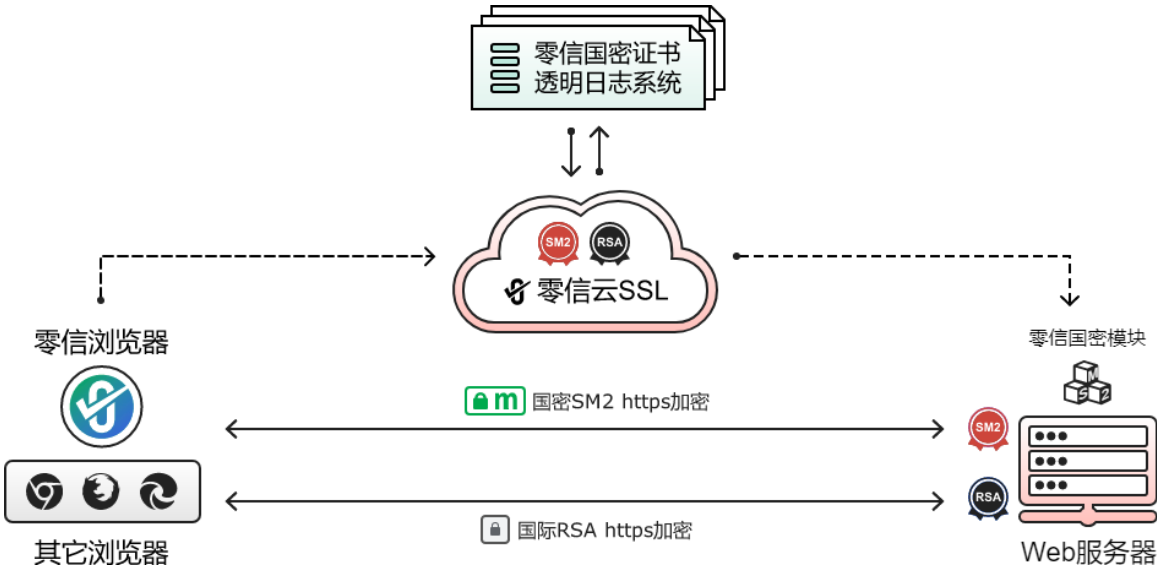
支持国密算法和国密 SSL 证书的证书透明日志系统：零信国密证书透明日志系统，此日志系统已经预置零信浏览器，实时检查每张国密 SSL 证书是否已经证书透明。

支持国密算法和国密 SSL 证书的 CDN 和 WAF 服务：阿里云、网宿

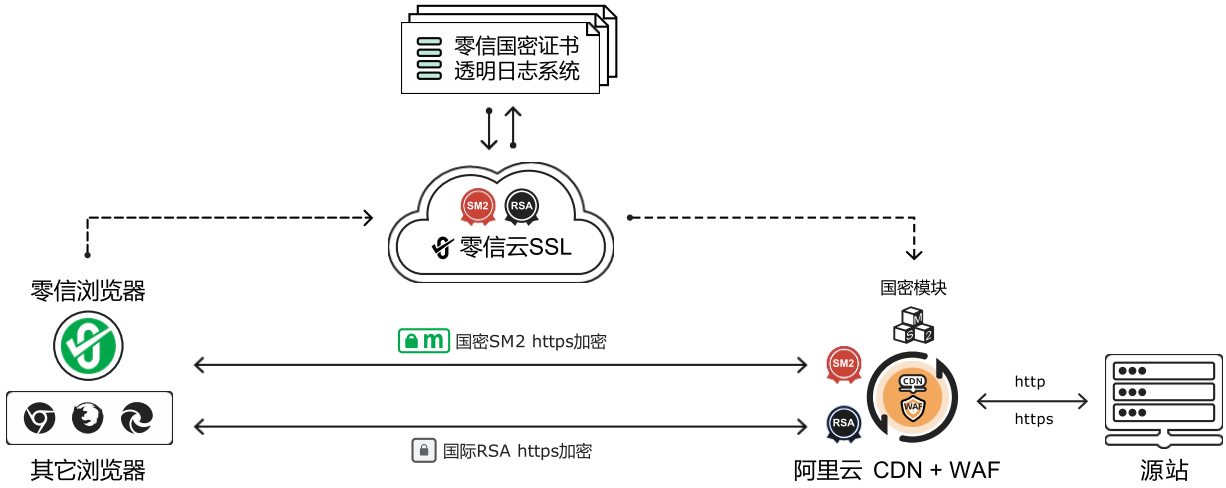
支持国密算法和国密 SSL 证书的移动 App 国密通信组件：中金认证

其他支持国密算法的产品和厂商还有许多，不再一一列举。。。。。

对于国密 https 加密，考虑到用户体验，网站不能要求用户指定使用国密浏览器来访问，所以，最佳方案是网站部署双 SSL 证书(一张国密 SSL 证书和一张国际 SSL 证书)，目前市场上的国密浏览器都是支持双证书自适应加密的，零信浏览器优先采用国密算法实现 HTTPS 加密，只有在网站没有部署国密 SSL 证书的情况下才使用 RSA 算法实现 HTTPS 加密。 为了让大家能体验双 SSL 证书部署是什么效果，我们部署了测试网站：https://sm2test.cersign.cn，请读者分别使用零信浏览器和其他浏览器访问这个国密 https 加密测试网站，会看到零信浏览器优先使用国密加密，并在地址栏显示国密加密标识 m。用户可以在此网站下载完全免费的 Nginx 国密模块，只需重新编译 Nginx 就可以支持国密 SSL 证书和国密算法。同时，读者还可以申请完全免费的 90 天有效期的免费国密 SSL 证书用于体验双证书部署的奥妙！



鉴于国密改造涉及面非常广和难度大，零信技术联合阿里云创新打造了零改造的国密 https 加密云服务--零信网站安全云服务，无需向 CA 申请国密 SSL 证书和国际 SSL 证书，无需在服务器上安装 SSL 证书，无需改造 web 服务器，只需做 3 次域名解析，把原网站变成 CDN 的源站就可以 10 分钟内实现国密 HTTPS 加密，而提供 CDN+WAF 服务的是业界领先的阿里云，零信技术基于阿里云 CDN 提供的 API 为用户全自动配置国密 SSL 证书和国际 SSL 证书到阿里云 CDN 中，快速实现 HTTPS 加密的国密合规和全球信任，快速实现网站云 WAF 防护，快速实现高速内容分发。



请读者分别使用零信浏览器和其他浏览器访问零信官网：https://www.zotrus.com，该网站就是一个零信网站安全云服务实现的国密 https 加密真实案例，用户使用零信浏览器访问会优先使用国密算法实现国密 https 加密，并在地址栏显示国密加密标识 **m**，还会看到地址栏有一个 **F** 标识，表示此网站已经启用了云 WAF 防护，如下左图所示。如果用户使用其他不支持国密算法和国密证书透明的浏览器访问，则会采用 ECC 算法实现 https 加密，如下右图所示。

相信大家从以上的国密生态厂商列表和零信技术的 https 加密解决方案可以看出，我国在国密 https 加密的技术和产品上已经准备好了！万事俱备，就差用户马上行动这一步了，必须马上行动起来，以确保所有网站在目前不确定的国际环境中的 HTTPS 加密安全可控，特别是政府网站和金融网站，确保即使国际 SSL 证书被“断供”或被“吊销”也不会影响用户正常访问网站系统。

最后，请大家看看两个真实部署的国密 https 加密案例，一个是省级政府官网，一个是中国银行的网银系统。

王高华

2022 年 11 月 4 日于深圳

请关注公司公众号，实时推送公司 CEO 精彩博文。