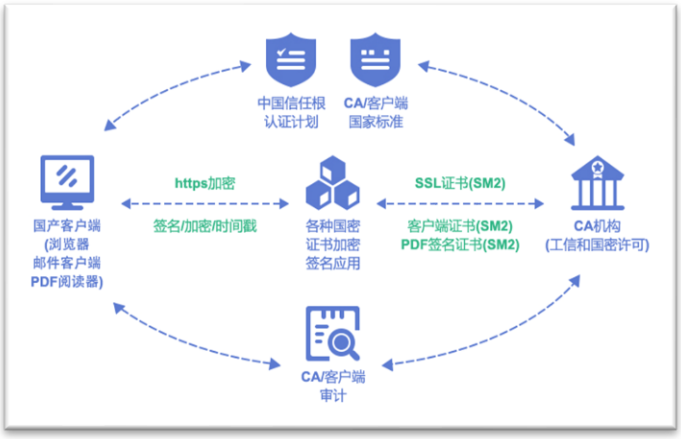
# 普及国密 SSL 证书应用，从普及国密浏览器使用开始

俄乌冲突导致大量俄罗斯政府和银行等重要网站的 SSL 证书被吊销，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，这也充分证明了我国在 2020 年 1 月 1 日正式施行《密码法》的高瞻远瞩，《密码法》第二十七条要求我国关键信息基础设施必须使用商用密码进行保护。但是，至于如何采用商用密码进行保护，则并没有出台实施细则明确，目前只能各个密码产品厂商自圆其说的解释自己的产品的使用和部署能满足《密码法》合规要求，本文就 SSL 证书和 HTTPS 加密的国密合规提供我们的观点和思路。

SSL 证书是互联网安全的底板产品(依据木桶理论)，HTTPS 加密是互联网安全的核心基础技术，互联网在发明和问世时是采用明文传输协议的，不仅广泛使用的 Web 协议-HTTP 协议是明文传输，这是互联网的第一大流量，而且第二大流量的电子邮件 MIME 协议也是明文传输( 包括 SMTP 协议和 IMAP 协议)。这些不安全的明文传输协议被不断完善为加密传输协议，也就是 HTTPS 协议，还有 S/MIME 协议，这些协议名称中的“S”就是“Secure(安全)”的意思。

而目前被广泛使用的 HTTPS 加密协议和 SSL 证书都是采用 RSA 算法和 ECC 算法，这是一个国外的加密算法，为了保障我国的互联网安全和信息系统安全，我国推出了相应的自己的加密算法，那就是 SM2 算法，包括用于消息认证的 SM3 算法和用于加密的 SM4 算法。大家俗称的“国密 SSL 证书”就是指采用 SM2 算法签发的 SSL 证书，对应国密 SSL 证书或 SM2 SSL 证书，我们把采用 RSA 算法签发的 SSL 证书称为“RSA SSL 证书”，把采用 ECC 算法签发的 SSL 证书称为 “ECC SSL 证书”，这实属是无奈之举，国外并没有 RSA SSL 证书和 ECC SSL 证书这个叫法，都称之为“SSL 证书”。

要实现 HTTPS 加密，必须有 CA 签发 SSL 证书，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，这是要建立一个国密证书应用生态。笔者早在由中央网信办网络安全协调局、国家密码管理局指导，中国电子信息产业发展研究院主办的“**2018 网络空间可信峰会**”(2018 年 12 月 17 日-18 日)就提出了“中国网络空间可信生态建设框架”构想，这是一个完整的国密证书应用生态构想，现在看来还是很前瞻的，笔者也很高兴地看到由于《密码法》的实施使得这个生态构想正在我国加速实现中。





这个生态中最重要的应用之一就是国密 HTTPS 加密，而实现国密 HTTPS 加密的首要部件就是国密浏览器，浏览器不支持国密算法和国密 SSL 证书，CA 签发国密 SSL 证书就没有了应用基础。这也就是为何零信技术推出的第一个产品是全面支持国密算法和国密 SSL 证书的零信浏览器，这是一个遵循通用浏览器商业模式的完全免费的国密浏览器，并且在发布时就已经预置信任 8 家 CA 机构的国密根证书和国家国密根证书。

零信浏览器基于开源 Chromium 研发，主要就是增加了支持国密算法和国密 SSL 证书，并特别创新地在地址栏增加了一个国密加密标识 m，点击国密加密标识，会提示“国密合规，密保合规”。这个提示就是提出了我们对《密码法》在 HTTPS 加密保护方面的合规理解与解释，只要网站部署零信浏览器信任的国密 SSL 证书，零信浏览器会优先采用国密算法实现 HTTPS 加密，也就是使用了商用密码进行保护，这就是满足了《密码法》的合规要求，也就是满足了密码保护合规要求，零信浏览器就明确告知网站访问者这个网站是国密合规和密保合规的，一目了然，无需更多的解释，这也是一种创新。


要想普及国密 SSL 证书应用，必须先普及国密浏览器的使用。欢迎读者朋友们免费 下载 使用零信浏览器，体验一下国密加密是什么样的，这里推荐访问 5 个部署了国密 SSL 证书的网站：第 1 个网站是江西省人民政府网站：https://www.jiangxi.gov.cn，第 2 个网站是安徽省人民政府网站：https://www.ah.gov.cn 。第 3 个网站是上海密码管理局官网：https://mgj.sh.gov.cn，

第 4 个网站是信用中国(江西)：https://www.creditjx.gov.cn，这 4 个网站都是部署 SM2/RSA 双 SSL 证书自适应加密，使用零信浏览器访问就是优先采用国密加密，而使用其他浏览器会采用 RSA 加密，看不到国密加密的效果。第 5 个网站是中国银行的网上银行服务：https://ebssec.boc.cn，这是一个仅部署了国密 SSL 证书的网站，如果不是使用支持国密加密的浏览器访问的话，浏览器会提示“意外终止了连接”，请再使用零信浏览器访问，一定能访问，并且在浏览器地址栏会显示国密加密标识。欢迎体验不一样的国密 https 加密！


王高华

2022 年 6 月 17 日于深圳

---

请关注公司公众号，实时推送公司 CEO 精彩博文。