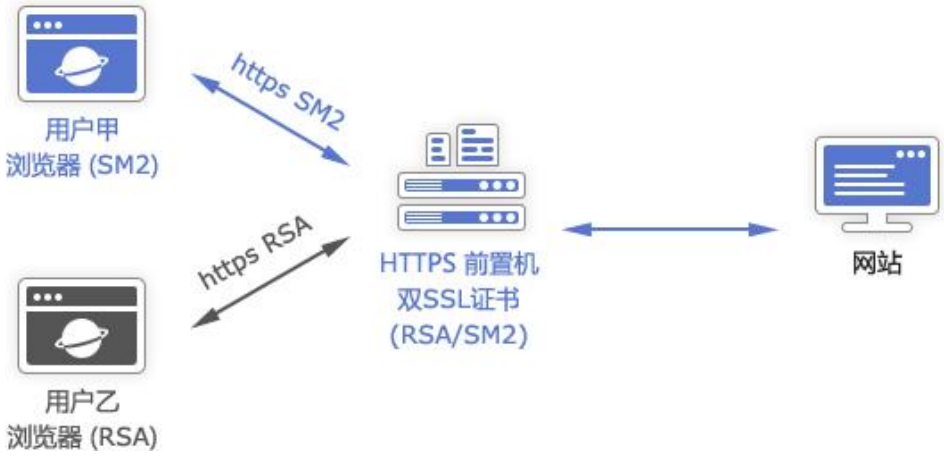
零信浏览器是一个免费的国密浏览器

网站没有部署 SSL 证书，所有浏览器都会显示为“不安全”，这是对 http 明文传输的零信任。而网站如果部署了国密 SM2 SSL 证书，国外浏览器是不支持的，会提示：“协议不受支持，客户端和服务器不支持 SSL 协议版本或加密套件”。虽然 SM2/SM3/SM4 算法已于 2018 年和 2021 年先后成为了 ISO/IEC 国际标准，但是离落地成为全球 CA 遵循的 CA 相关国际标准和得到所有浏览器的支持还有很长的路要走。可喜的是，国产浏览器已经行动起来了，已经有多个品牌的国产浏览器支持 SM2 SSL 证书，满足了我国政务用户的《密码法》合规应用需求。

但笔者认为：目前国产浏览器的国密算法和国密 SM2 SSL 证书的支持，还有很多做得不到位的地方，这里就不具体评述了。国密算法和国密 SM2 SSL 证书的支持是零信技术的首发产品—零信浏览器的第一个亮点，不仅支持国密 SSL 证书和遵循《GM/T 0024 SSLVPN 技术规范》和《GB/T38636-2020 信息安全技术传输层密码协议(TLCP)》等密码标准规范，而且我们在用户界面上增强显示部署了国密 SSL 证书的网站，如下图所示，在安全锁标识后面增加一个 m 标识来突显此网站已经部署了国密 SSL 证书，实现了国密算法加密。

一个 m 标识让所有使用零信浏览器访问政府网站时用户一眼就知道这个网站是否是采用国密算法保护的，也让网站主办单位无需出具什么合规证明，直接让监督检查单位用零信浏览器访问试试就知道是否已经合规。不仅如此，零信浏览器优先采用国密算法同 Web 服务器握手通信，如果网站部署了国密 SSL 证书，支持国密算法，则优先采用 SM2 算法实现密钥交换，采用 SM3 算法实现消息认证和采用 SM4 算法实现数据传输加密。如果没有部署国密 SSL 证书，则优先选用 ECC 算法，因为 ECC 算法比 RSA 算法更快，能给用户更好的体验。如果网站没有部署任何 SSL 证书，则浏览器会显示此网站“不安全”。

零信浏览器基于开源项目 Chromium **97** 版本开发，浏览功能这块已经非常先进了，无需做任何改动。我们首先增加的第一功能就是支持国密算法(SM2/SM3/SM4)和国密 SSL 证书，并设计为优先使用国密算法，如果网站部署了双 SSL 证书的话。说起双 SSL 证书，这也是笔者很是骄傲的事情，这是笔者首次在 2018 年的“**网络可信峰会**”上演讲时提出的，如下图所示，很高兴的地看到这个双证书自适应机制现在已经成为了所有部署了国密 SSL 证书网站的标配，大家在访问某个政府网站时可能看到的是部署了 RSA SSL 证书，实际上是你使用的浏览器不支持国密算法而没有采用国密 SSL 证书来实现 https 加密，推荐大家再用零信浏览器访问试试，看看是否能在地址栏看到一个 m 标识。



零信浏览器已经预置信任国家 SM2 根证书和几家 CA 的 SM2 根证书，欢迎各个有 SM2 根证书并能签发 SM2 SSL 证书的 CA 联系我们，预置信任你们的 SM2 根证书，共同打造一个完整闭环的国密算法 https 加密应用生态圈，让国密算法和国密 SSL 证书发挥更大的作用来保障我国电子政务系统安全和全球互联网的安全。

王高华

2022 年 4 月 20 日于深圳
2022 年 4 月 24 日更新

请关注公司公众号，实时推送公司 CEO 精彩博文。