江南天安SSL加速方案简介

随着安全意识的提高，越来越多的网站转向了https的部署方案。有得必有失，增加安全的同时增加了CPU加解密运算的的繁重负担。为了达到更好的性能，不得不采购更加昂贵的CPU来应对。但CPU作为一个通用类型的处理器，虽然样样都会，但却样样不精。这可怎么办？

国密算法是具有中国特色的加解密算法，国密SSL通讯是中国特色的链路加密，具有计算量小，安全性高等优点，但是使用起来相对复杂，专业技术要求相对高，作为普通开发者想用上国密，如何破解？

随着《密码法》的颁布，国家越来越重视信息安全，作为重要系统的关键安全保障，如何才能使得密钥更安全，密钥使用更合规，如何使用物理硬件设备来更加安全合规的保障通信的安全？

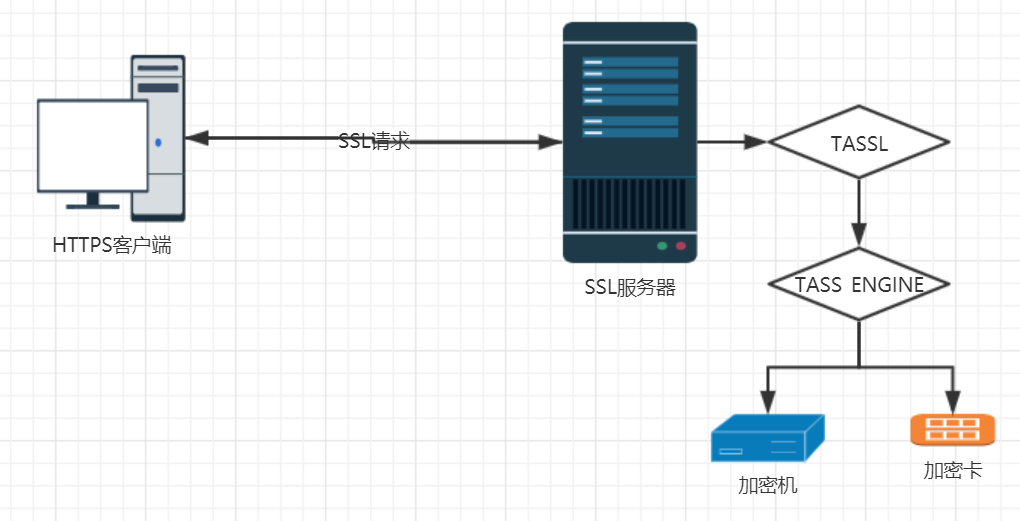
针对以上问题，江南天安推出了基于自有安全设备的SSL加速解决方案。

# SSL加速方案主要特点介绍

* 采用引擎机制，部署更加简单，使用更加方便，升级维护更加容易。

使用openssl原生支持的引擎机制，不需要额外的API接口调用，只需要调用原生的openssl引擎接口进行加载调用即可。如果要进行引擎库的升级，用户调用无需改动，只需要替换引擎库即可。对于没有调用过加密机的用户，只需要很少量的代码的修改即可调用起来加密机。加密机的调用同加密卡调用一致，用户在使用加密机时想切换成加密卡，只需要修改引擎加载的名字即可，无需其他改动，让调用硬件设备更加统一。

**调用示意图：**



* 高可用性

对于调用密码机的方案，内部通过更加成熟的nginx高可用代理方案，引擎内部与nginx代理后的服务端口进行通讯，而不是真正的加密机服务端口。通过nginx可以代理多台加密机，而实现引擎的高可用与故障隔离。

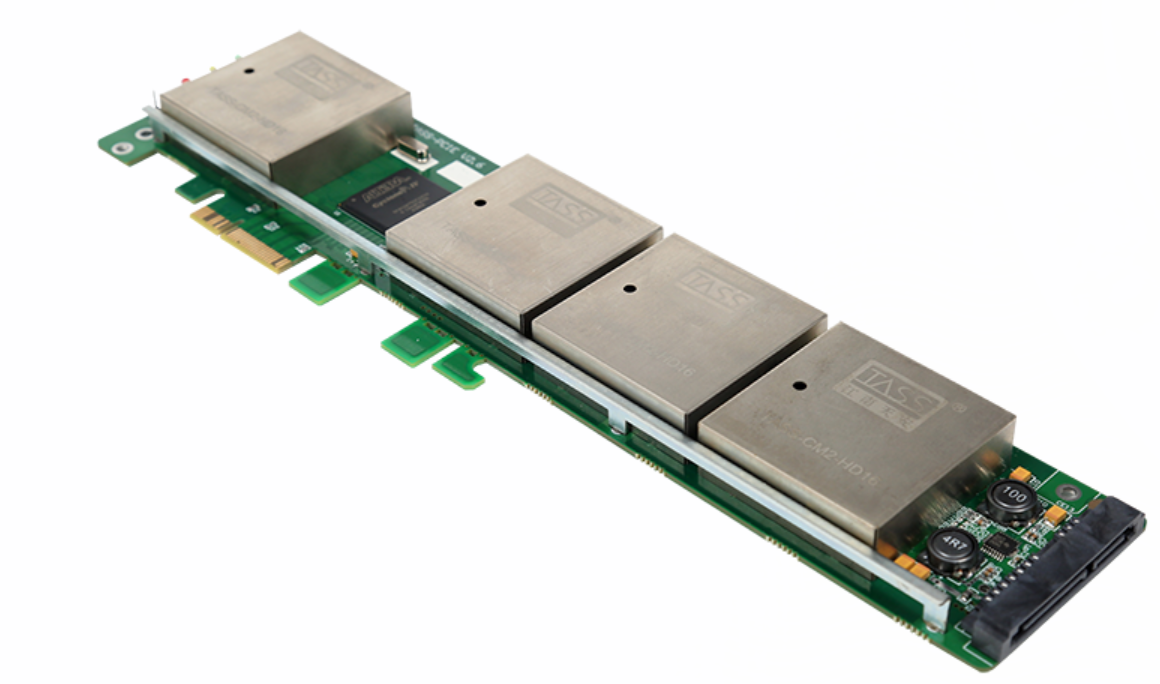
* 实现更加快速的ssl卸载，减少CPU压力和成本

通过引擎通过调用PCIe接口的加密卡，提供了更大的带宽和更小的时延。加密卡提供了更快速的加密解密运算，在新建连接数大并发和要求低时延等苛刻环境下，会提供有力的支持。让加解密此类的运算繁重的任务通过加密卡来运算, 专卡专用，提升性能，会很大程度的减轻CPU的压力，让CPU有余力处理更多的其他业务类的运算，而不必花更高成本采购更高性能的CPU来应对业务的激增的压力。

* 合规性

江南天安SSL加速方案使用的加密机为：SJJ1310/EVSM金融数据密码机，是江南天安依据国密局、人民银行等主管单位的相关标准规范，自主研发的新一代金融数据产品，具有完全独立知识产权并获得多项专利证书，满足PBOC1.0/2.0/3.0、GP、TSM、EMV等行业应用规范。使用的密码卡为：SJK1322 SJK1557密码卡，是江南天安依据国密局、工信部、公安部等主管单位的相关标准规范，自主研发的新一代密码产品，具有完全独立知识产权并获得多项专利证书。目前支持的国密SSL套件为：ECC-SM4-SM3和ECDHE-SM4-SM3，均符合GMT 0024-2014《SSL VPN技术规范》。加密机的SSL加速方案也同时支持RSA算法的加速。





# 国密SSL加速卸载性能指标

* EVSM虚机版本 ：2000QPS
* 标准版本1310 ：7000QPS
* 高性能版本1310：14000QPS
* 加密卡版本 ：18000QPS

# 关于天安 了解更多

地址：北京市海淀区马甸东路17号金澳国际大厦11层1110室

邮编：100088

电话：010-82326383

传真：010-82328039

邮箱：tassl@tass.com.cn

网址：www.tass.com.cn