国密证书透明是保障国密 HTTPS 加密安全的必须

所有浏览器都对 HTTP 网站显示为“不安全”，因为 HTTP 是明文传输协议，从浏览器到服务器(云端)之间的信息传输是明文，非常容易被非法窃取和非法篡改。唯一可行的技术措施是 HTTPS 加密传输，在服务器部署 SSL 证书实现 HTTPS 加密，这是网站安全的基础和必须。而为了保障 SSL 证书本身的安全，国际标准保障措施是每一张用于 HTTPS 加密的 SSL 证书都必须在签发之前到指定的证书透明日志服务系统去做签发备案，并把备案签名数据写入 SSL 证书中，只有这样，浏览器才会信任这张 SSL 证书，才可以用这张 SSL 证书实现 HTTPS 加密。证书透明机制就是为了保障 SSL 证书本身的安全，这是互联网安全的基础。

国际证书透明机制已经累计成功保障了 74 亿多张的全球信任的国际 SSL 证书的安全可信，我国正在大力推广国密 SSL 证书实现国密 HTTPS 加密的普及应用，以应对目前非常不确定的国际环境对我国互联网带来的安全威胁。我国也必须有自己的国密证书透明机制来保障国密 SSL 证书的安全，从而保障国密 HTTPS 加密的安全，进而可靠地保障我国网站和互联网安全。

国密 HTTPS 加密安全的前提是国密证书透明，即采用国密算法实现的证书透明日志系统，只有每一张国密 SSL 证书都国密证书透明了，才能保障国密 SSL 证书本身的安全。国密 HTTPS 加密、国密证书透明机制，连同我国目前已经实施的网站备案机制、域名注册实名制一道形成一个从域名注册(网站诞生)到网站运营再到网站安全(加密)的完整的网站安全保障体系，将真正有力保障我国网站和互联网的安全可控，各个环节缺一不可。

国密证书透明机制的主要技术和管理优势有如下三点：

(1) 保证每一张国密 SSL 证书的签发行为的公开透明披露，及时发现各种疏忽错误签发和恶意攻击签发，切实保障用户网站安全权益；

(2) 为国家密码主管部门提供一个实时准确的国密 SSL 证书签发情况统计数据，为政府决策提供可靠的参考数据；

(3) 为国密 SSL 证书和国密 HTTPS 加密产业相关方提供一个可靠的市场分析数据，从而为

产业发展提供可靠的数据支持。

目前，只有零信技术成功研发并可靠地运行了 3 个国密证书透明日志系统，也只有零信浏览器支持国密证书透明安全机制检查，也只有证签技术和零信技术签发的国密 SSL 证书已经内置证书透明签名数据(SCT)，这是远远不够的！笔者呼吁国家密码主管部门尽快建立一个国家级的国密证书透明日志系统，从国家安全高度来重视和建设运维国家级国密证书透明系统。同时，呼吁各大国密浏览器支持国密证书透明机制，呼吁各个有能力签发国密 SSL 证书的 CA 机构尽快把签发的每一张国密 SSL 证书都实现国密证书透明。只有这样，才能建立起一个强大的国密证书透明机制生态系统，才能真正让国密证书透明发挥更大的安全保障作用，从而真正切实保障我国互联网安全。

王高华

2022 年 9 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。