携手合作伙伴，共赢商密市场

今天，零信技术隆重发布了最新的合作伙伴计划，这是零信技术在完成了两个重要的商密 HTTPS 加密应用生态产品研发后的重大行动计划，意在分享零信技术鼎力打造的国密证书透明和国密证书自动化管理两个生态产品的研究成果，携手合作伙伴，共赢巨大的商密 HTTPS 加密应用市场。本文将从以下 4 个方面来解读零信合作伙伴计划：

(1) 商密 HTTPS 加密应用市场到底有多大？

(2) 普及商密 HTTPS 加密应用的技术难度在哪？

(3) 零信技术是如何解决商密 HTTPS 加密应用难题的？

(4) 共享研究成果，携手合作伙伴，共赢商密市场

一、 商密 HTTPS 加密应用市场到底有多大？

这是必须首先告诉合作伙伴的第一重要问题，让合作伙伴了解这个市场到底有多大，是否值得投入到这个市场中来。

HTTPS 加密在我国电商平台、网银系统基本上得到了普及应用，这是因为没有 HTTPS 加密就无法保障用户的机密信息传输安全，无法保障重要的用户数据安全，所以，所有浏览器都对没有部署 SSL 证书实现 https 加密的网站显示为“不安全”，https 加密市场是一个正在快速增长中的市场。

而去年俄乌冲突发生后美国 CA 吊销了几乎所有俄罗斯政府和银行网站的 SSL 证书，并断供不再给这些网站签发新的 SSL 证书，这个严重的由于地缘政治原因导致的恶性互联网安全事件给我国的政府网站和银行网站安全敲响了警钟，因为我国政府网站和银行网站部署的也是美国 CA 签发的 RSA 算法 SSL 证书，也一样存在这样的安全风险，这使得我国自主密码算法的国密 SSL 证书的普及应用提升到了急需普及应用的日程，我国必须居安思危，未雨绸缪，加快普及国密 SSL 证书的部署应用，实现国密 https 加密。

那么，国密 HTTPS 加密应用市场到底有多大？据多个省政务云平台公开披露的信息，省政务云平台已经至少为超过 1 万到 2 万个政府网站提供集约化管理服务，但是这些省申请的 SSL 证书总数只有十几张，有些省甚至只申请了几张 SSL 证书，证书申请量不到网站数量的千分之一。再看看各部委垂直管理的网站从部到省市县也有上万个网站系统，但是部署 SSL 证

书的数量也非常少。还有金融机构、大型关键信息基础设施运营单位、大型企业、电信运营商、云服务提供商等等，都有大量的成百上千甚至上万个网站需要实现国密 HTTPS 加密。

据保守估算，国密 HTTPS 加密应用市场是一个**超百亿**的蓝海市场，是一个一定会落地的真实市场，不仅仅是解决现实存在的证书安全风险的必须市场，而且也是一个合规的刚需市场。《密码法》、《网络安全法》、《数据安全法》、《个人信息保护法》和《关键信息基础设施安全保护条例》、《商用密码管理条例》等法律法规明确要求这些重要的网站系统必须采用商用密码来保障关键信息系统安全和保护关键数据安全。

二、 普及商密 HTTPS 加密应用的技术难度在哪？

虽然我们看到了商密 HTTPS 加密应用市场很大，但是商密 HTTPS 加密应用推进很缓慢，因为目前整个互联网安全保障体系采用的是基于 RSA 算法的密码体系，这个体系已经成功运行了将近 30 年，就像城市自来水管网一样遍布到整个城市的每一个角落，而要改造这个体系为基于商用密码算法的密码体系，就等于要把整个城市的自来水管道都全部换掉，这种大规模的改造谈何容易！这就是为何“国密改造”很难推进的根本原因。

而国密 HTTPS 加密应用则是整个密码体系国密改造中的最重要的一环，因为整个互联网的 https 信息传输加密是基础安全，没有这个基础保障，其他安全保障都是根基不牢的“安全”。实现 HTTPS 加密有三大难题和障碍，具体有：

难题一：人工手动部署 SSL 证书，非常繁琐、费时费力

要实现 https 加密，用户必须向 CA 申请 SSL 证书，完成身份认证后才能拿到证书，再把 SSL 证书安装到 Web 服务器中，才能启用 https 加密，这个过程是非常繁琐的、费时费力费钱的过程。

随着所有网站都必须实现 https 加密，特别是各省市政务网站的集约化集中管理，需要管理多达上万政务网站，使得 SSL 证书的申请和部署成为网管人员的一个最大的工作负担。政务云平台必须投入更多的运维人员才能实现多个网站的 https 加密，否则一旦某个系统的 SSL 证书过期而忘了续期，将严重影响业务系统的正常运行而带来不可估量的损失。

这就能解释为何这么政府网站没有部署 SSL 证书了，太难了！所以，千万不要以为大量的网站没有部署 SSL 证书就一定是 SSL 证书的市场，现实证明不是!这个巨大的市场属于 HTTPS 加密应用市场，用户需要的是 HTTPS 加密，而不是 SSL 证书！

难题二：国密 HTTPS 加密改造，涉及面广、难度很大

等保和密保合规要求之一是“网络与通信传输安全”，也就是 Web 服务器的 HTTPS 加密，这个加密必须采用国密算法实现。这就要求 Web 服务器部署国密 SSL 证书，需要用户向 CA 申请国密 SSL 证书并部署到 Web 服务器上使用，这个难点同**难题一**是一样的。

但是，要启用国密 SSL 证书，不仅仅是安装 SSL 证书，而且还需要对 Web 服务器进行国密改造，以便支持国密算法，同时还要求用户改用支持国密算法的浏览器以实现国密 https 加密访问，这就要求给所有用户电脑更新安装国密浏览器，这也是一个比较大的工程。还有，有些重要的正在使用的 Web 服务器不能动，不能改造，不能影响正在运行的业务系统，并且有些 Web 服务器软件根本就无法改造。

还有，CDN/WAF 服务/WAF 设备也需要改造支持国密算法和国密 SSL 证书，因为大流量网站系统必须上 CDN 和必须上 WAF 防护。

国密 HTTPS 加密改造涉及面非常广，是一个从客户端到云端的全程改造，每一个方面的改造难度都很大，但又必须改！

难题三：SSL 证书有效期即将缩短为 90 天，部署工作量将增加 4 倍

这是一个即将到来的难题，为了保障 https 加密安全，谷歌正在推动 SSL 证书有效期由现在的 1 年缩短为 90 天，意在将 PKI 生态系统具有抗量子算法所需的敏捷性。

这就意味着原先需要每年为网站申请和部署一次 SSL 证书，变成了每年 4 次，**难题一**的巨大工作量又一下子增加了 4 倍！这就把手动申请和部署 SSL 证书变成了不可能了！

这一革命性的技术变化，预计 2024 年一定会到来，所有网站主管都必须提前做好准备，提前实现 SSL 证书自动化申请和部署，实现 HTTPS 加密的自动化管理。

三、 零信技术是如何解决商密 HTTPS 加密应用难题的？

商密 HTTPS 加密应用的三大难题就是压在政务云平台、公共云平台和大型机构等有大量网站需要部署 SSL 证书的网管和运维工程师头上的三座大山，必须有解决方案解决这些难题，才能普及实现 https 加密。零信技术创新地研发了三大解决方案和相关的产品，实现了自动化申请、部署和续期双 SSL 证书，实现了全自动、零改造或一键改造，无需关心证书有效期的不断缩短，彻底完美地解决了国密 HTTPS 加密普及应用的三大难题。

1. 零信 HTTPS 加密自动化管理三大解决方案，彻底完美解决 HTTPS 加密应用三大难题

解决方案一：一次安装，启用零信国密 ACME 客户端软件-SM2cerBot。

此解决方案类似于国际 ACME 解决方案的 ACME 客户端软件：CertBot，不同的是：SM2cerBot 是自动化申请、部署、续期双算法 SSL 证书，一张 90 天有效期的全球信任的国际 SSL 证书和两张 90 天有效期的国密 SSL 证书(签名证书和加密证书)。并且自带国密算法支持模块，自动替换不支持国密算法的 Nginx 为支持国密算法的 Nginx 服务器，自动化一键实现 https 加密，自适应加密算法，并优先采用国密算法实现国密 HTTPS 加密。

此解决方案的缺点是需要卸载原 Nginx 服务器软件，可能对业务系统有影响，适合于新网站部署，实现国密 https 加密自动化管理。

解决方案二：一次部署，启用零信国密 HTTPS 加密自动化网关，原 Web 服务器零改造、零安装 SSL 证书。

此解决方案适合于原 Web 服务器正在运行重要的业务系统和不能改动服务器的应用场景。原 Web 服务器零改造实现国密 https 加密，无需申请和安装 SSL 证书，只需部署 HTTPS 加密自动化网关，把原网站 IP 地址设置到网关即可由网关实现 https 加密、卸载转发到原网站，原 Web 服务器位于内网，不仅更加安全，而且把 https 加密的负担交给了网关，使其能更好地为业务系统服务。此解决方案由网关负责自动化申请、部署和续期双算法 SSL 证书，自动化负责 https 加密，自适应加密算法，并优先采用国密算法实现国密 HTTPS 加密。

零信国密 HTTPS 加密自动化网关推荐双机部署，最多可以为 255 个网站自动化配置双算法 SSL 证书，含 5 年最多 255 张双 SSL 证书，仅 SSL 证书价值高达 113 万元，同时节省工程师人力成本高达 150 万元，是一个非常超值的 https 加密自动化管理解决方案。

解决方案三：一次设置，启用零信国密 HTTPS 加密自动化云服务，原 Web 服务器零改造、零安装 SSL 证书。

此解决方案适合于既不能在 Web 服务器上安装国密 ACME 客户端软件，也不想购买或无法部署硬件网关设备的应用场景。这是一个云服务，只需做域名解析，即可自动化申请、部署和续期双 SSL 证书，原 Web 服务器零改造实现 https 加密，自适应加密算法，并优先采用国密算法实现 HTTPS 加密。

零信国密 HTTPS 加密自动化云服务是一个基于业界领先的阿里云 CDN/WAF 服务打造的集 HTTPS 加密自动化、CDN 高速分发、边缘 WAF 防护、网站可信认证于一体的全方位网站安全防护解决方案，适合于单个网站的安全防护和 https 加密自动化管理，每个网站需要启用一个独立的 HTTPS 加密云服务。

2. 零信国密 HTTPS 加密自动化管理三大配套服务，为三大解决方案提供超值支持

零信 HTTPS 加密自动化管理解决方案完美解决了自动化申请、部署和续期双算法 SSL 证书的难题，但是要想实现国密 HTTPS 加密，还得有浏览器支持国密算法和国密 SSL 证书，自动配置的双 SSL 证书都得支持证书透明来保障 SSL 证书自身安全。为此，零信技术免费提供了三大配套超值服务。

配套服务一：免费提供国密浏览器—零信浏览器

零信浏览器是一个完全免费的、干净无广告的支持国密算法和国密 SSL 证书、支持国密证书透明的国密浏览器，也是一个基于谷歌 Chromium 内核的通用浏览器，从底层加密套件支持国密算法，实现浏览器同 Web 服务器握手时自动快速协商加密算法，同时支持 RSA / ECC / SM2 三种密码算法加密套件，实现自适应算法 https 加密。

配套服务二：免费配套签发双算法 SSL 证书

零信云 SSL 服务系统和零信国密 ACME 服务系统免费配套为零信 HTTPS 加密自动化管理解决方案提供自动化签发双算法双 SSL 证书服务，用户无需另外向 CA 申请 SSL 证书，无需另外花钱购买 SSL 证书，三个解决方案都已包含 https 加密服务所需的双 SSL 证书，国际 SSL 证书全球信任和支持所有浏览器，国密 SSL 证书国密合规和支持所有国密浏览器。

特别超值的是：HTTPS 加密自动化网关最多为 255 个网站域名和长达 5 年的配套提供多达 3825 张一年期 SSL 证书，完全免费提供，非常超值！

配套服务三：免费提供国密证书透明日志服务

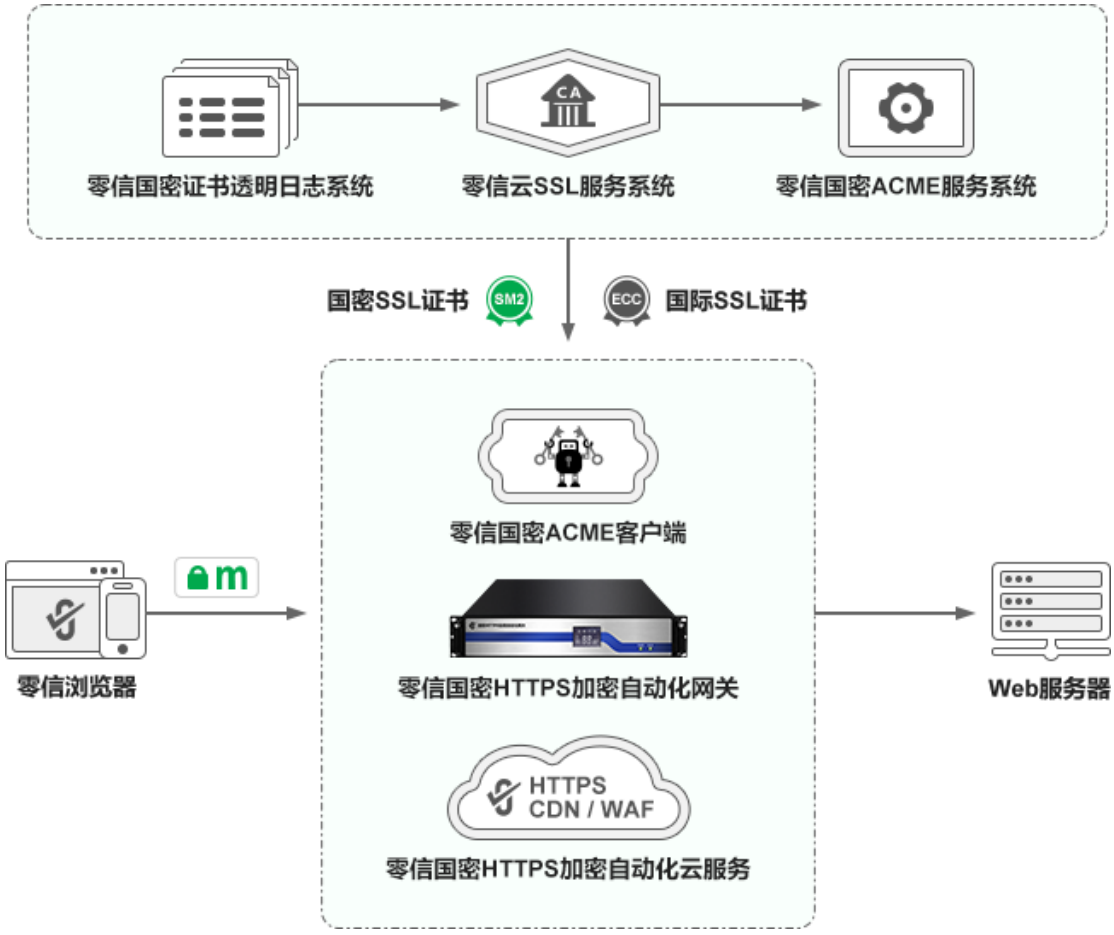
为了保障为零信 HTTPS 加密自动化管理解决方案配套签发的国密 SSL 证书的自身安全，全球独家为所有国密 SSL 证书提供国密证书透明日志服务，每一张配套提供的国密 SSL 证书都像国际 SSL 证书一样都有证书透明安全保障，有力保障用户的合法权益和网站安全。

四、 共享研究成果，携手合作伙伴，共赢商密市场

零信技术投入巨大研发力量历时两年研发了国密证书透明生态产品和国密证书自动化管理生态产品，形成了一个可以实现全自动国密 https 加密的应用生态，彻底解决了国密 HTTPS 加密应用遇到的三大难题，彻底扫除了普及国密 HTTPS 加密应用的三大障碍，非常适合于大规模实施普及国密 HTTPS 加密应用，只有普及了国密 HTTPS 加密应用，才能解除我国互联网

面临的随时遭遇 SSL 证书吊销和断供的安全威胁，才能真正实现采用商用密码来保障我国互联网安全可信。为此，零信技术适时发布了合作伙伴计划，让更多的有志和有智之士加入到国密 HTTPS 加密这个蓝海市场中来，共同赢得商用密码 HTTPS 加密应用市场。

零信国密 HTTPS 加密自动化管理三大解决方案和三大配套服务由零信国密证书透明日志系统、零信云 SSL 服务系统、零信国密 ACME 服务系统、零信国密 SSL 证书和国际 SSL 证书、零信浏览器、零信国密 ACME 客户端、零信国密 HTTPS 加密自动化网关和零信国密 HTTPS 加密自动化云服务等八大系统提供相关产品和服务，让用户网站系统和物联网设备能全自动实现 https 加密，自适应加密算法，满足不同用户的国密合规和全球信任的 HTTPS 加密应用需求。



俗话说“独木不成林”，“众人拾柴火焰高”，零信技术愿全面开放所有自研生态产品，同合作伙伴共享研究成果，共同打造国密 HTTPS 加密自动化应用生态，让这些优秀的研究成果能迅速得到普及应用，从而快速普及应用国密 HTTPS 加密，快速实现用商用密码来保障我国网络空间安全。

零信技术为合作伙伴提供三种不同的合作计划：分销伙伴、OEM 伙伴和生态伙伴，欢迎

合作伙伴根据自己的业务发展规划和业务特点选择合适的计划，携手共同拓展商用密码应用蓝海大市场。零信技术坚持合作伙伴优先，与合作伙伴紧密合作，共同为客户提供更完备的密码产品和更完善的服务。

王高华

2023 年 7 月 26 日于深圳

请关注公司公众号，实时推送公司 CEO 精彩博文。