岁末钜献 | 网安市场的新蓝海是 HTTPS 加密自动化

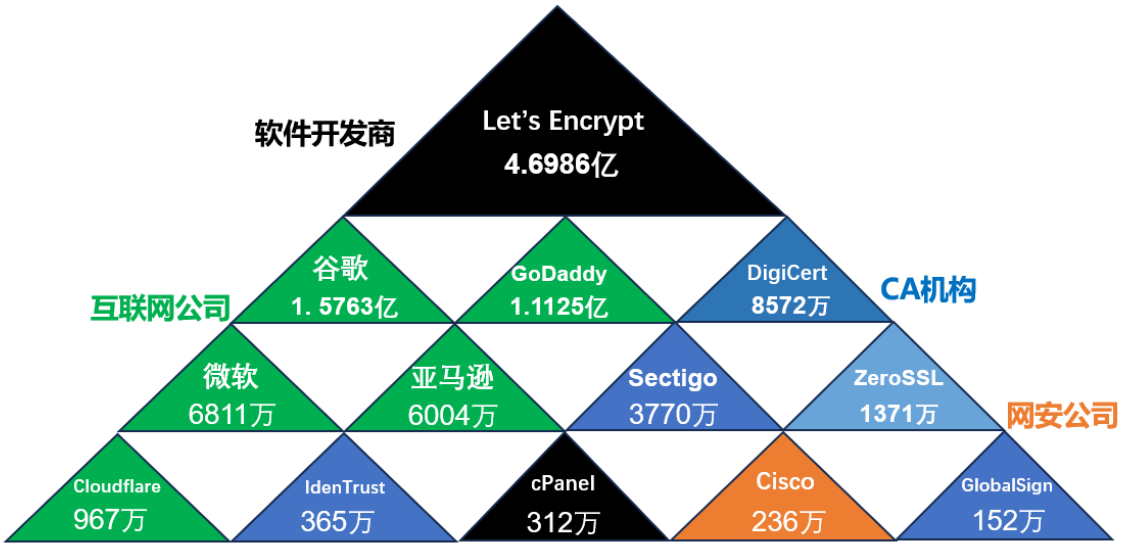
2024 年马上就要过去了，最近同几家头部网安企业高管交流，都说网安市场现在很难。笔者也算是一个老网安人，特在岁末写篇文章，给网安企业支个新招，助力网安企业早点抓住国密 HTTPS 加密自动化大市场，所有市场机会都是早起的鸟儿有虫吃。

一、 “木桶理论”的底板是什么？如果底板不牢怎么办？

网安业界人士一定都知道“木桶理论”：一只木桶的盛水量取决于桶壁上最短的那一块。也就是说：一个信息系统的安全水平取决于最薄弱的环节，必须查找和弥补安全防护措施中的“短板”，提升整体安全防护水平。这也是大家常说的“补齐短板“的由来。

网安市场中的每个产品都是为了补齐安全防护中的某一个短板，但是，不知道大家是否想过这个问题：谁是木桶的底板呢？如果底板不牢，木桶还能用吗？底板比任何一块壁板都重要，网络安全的底板是密码体系。目前，全球网络安全的底板是 RSA 密码体系，这个底板的核心部分就是 HTTPS 加密，核心产品是 SSL 证书。俄乌冲突发生后，俄罗斯网安市场的这块核心底板被人撤了，所有政府网站和银行网站 HTTPS 加密所需的 SSL 证书被断供，已部署使用的 SSL 证书被吊销，导致这些关键信息基础设施都不可访问了，或不能安全地访问了。网络安全防护的底板都没有了，其他安全防护措施也就失去了其价值。

这就是为何全球互联网巨头都已经深度融入 HTTPS 加密自动化市场，甚至直接作为顶级根 CA 为用户免费自动化提供 SSL 证书，以快速取得市场领先地位，因为这是网络安全的底板市场，必须牢牢抓住。前十三大 SSL 证书提供商有：软件开发商 2 个，互联网公司 5 个，CA 机构 5 个，网安公司 1 个，笔者已在多篇文章解读过其他类型的公司，本文特别解读一下网安公司，为何网安公司也必须深度参与 HTTPS 加密自动化市场呢？还是因为这是木桶的底板！网络安全的底座！



全球前十三大SSL证书提供商排名和证书签发量(2024.12.30统计)

二、 全球十大网安公司都在深度融入 HTTPS 加密自动化

全球十大网安公司中排名第一的是 Cisco(思科)公司，从上面的统计图表可以看出，思科在全球 SSL 证书提供商中排名第 12 位，SSL 证书签发量为 236 万张，这些 SSL 证书都是为各种思科网络设备和物联网设备自动化配置的，自动化实现各种网络设备和物联网设备的 HTTPS 加密数据传输和安全管理。不仅如此，思科还有自己的可信根认证计划，是国际标准组织—CA/浏览器论坛的证书消费类成员单位，其他同类成员单位是浏览器厂商(谷歌、微软、苹果等)。思科既是第一大网安公司，也是第 12 大 SSL 证书提供商，同时也是一个证书消费者，自动化为其网络设备配置 SSL 证书实现了三种身份的统一。

排名第 2 位的是 Palo Alto Networks，第 3 是 Fortinet，第 4 是 Check Point，第 5 是 Juniper Networks，第 6 是 Zscaler，第 7 是 Symantec(赛门铁克)，第 8 是 Trend Micro(趋势科技)，第 9 是 IBM Security，第 10 是 F5，其中 Fortinet 已为各种网络设备签发了 18 亿张自签 SSL 证书(绑定设备 IP 地址)。这些网安公司的网络设备，如负载均衡设备、WAF 设备、SSL VPN 设备等，都已经支持国际标准 ACME 协议的 SSL 证书自动化，有些厂商的 OS 都已经集成了 ACME 服务，方便用户只需配置域名就可以自动化免费实现 HTTPS 加密。这也就能解释为何 Let's Encrypt 和谷歌 GTS 的免费 SSL 证书签发量分别高达 4.69 亿张和 1.57 亿张，因为大量的网安设备正在使用其完全免费的 SSL 证书自动化服务。

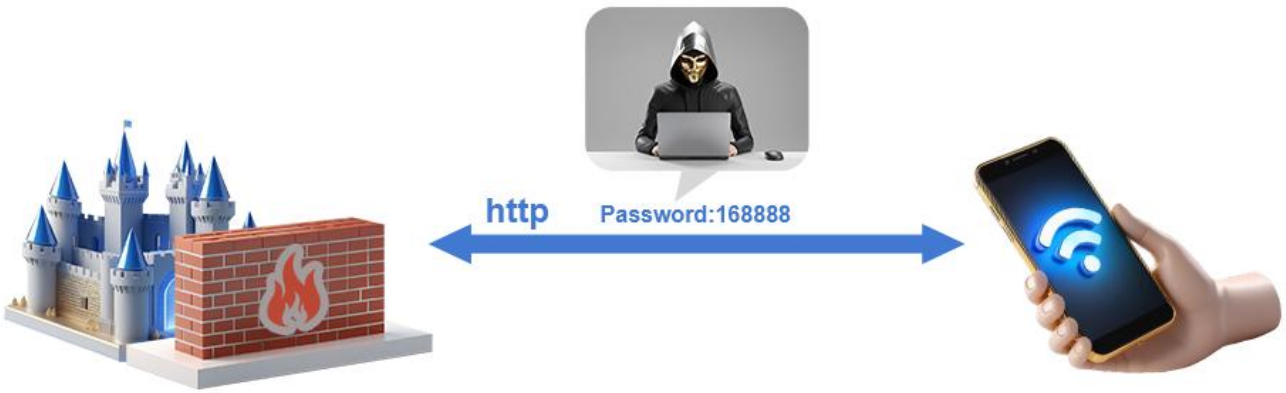
这十大网安公司除了思科是从全球信任根 CA-DigiCert 定制 Cisco 品牌中级根证书为其网络设备自动化签发自己品牌的 SSL 证书外，其他厂商都是直接使用其他 ACME SSL 证书提供商自动化签发的免费 90 天 SSL 证书，都是全球信任的 SSL 证书，这是因为许多网安设备需要

浏览器登录管理，部署浏览器信任的 SSL 证书不会有安全警告，比自签证书更安全。而 Fortinet 大量签发的自签 SSL 证书都是绑定内网 IP 地址的 SSL 证书，这是全球信任的 SSL 证书不支持的证书类型，只能自己签发。另外，赛门铁克曾投巨资收购了当时全球最大的 CA—VeriSign，趋势科技也曾收购了 CA 公司 Affirmtrust，直接拥有顶级根 CA，意在深度融合 CA 数字证书到其各种网络安全产品和服务中，这也值得已经收购了 CA 公司的国内网安公司和互联网公司重新思考应该如何深度融合 HTTPS 加密自动化业务。

三、 国密 HTTPS 加密自动化是我国网安市场的新蓝海

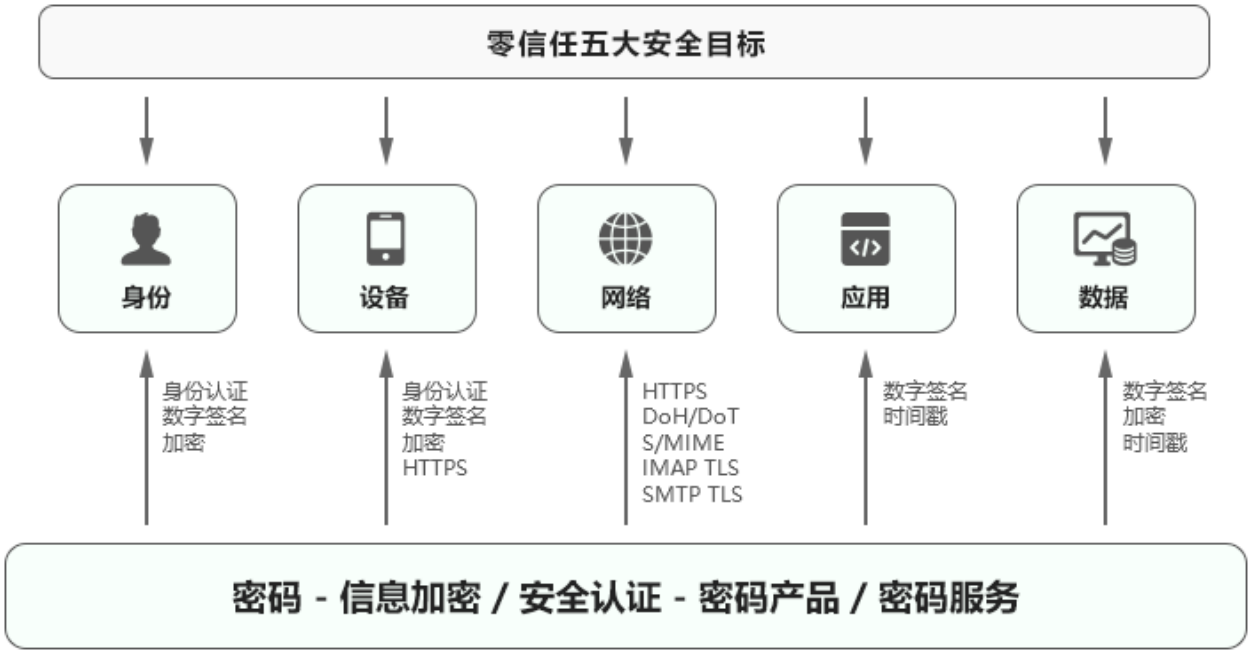
网安企业在过去的三十年得到了长足发展，为保障我国网络安全做出了应有的积极的贡献，并且培养了一大批能打胜仗的市场营销队伍和技术过硬的研发队伍。但是，在网络安全产品如：杀毒软件、防火墙、IPS/IDS、SSL VPN、上网行为管理等市场已经充分竞争和充分饱和的今天，网安产品销售精英们都不知道再给客户推销什么了，该买的都买了。所以，所有网安企业是时候认认真真地寻找真正的新蓝海市场了。

那么，什么才是真正的新蓝海市场呢？要回答这个问题，聪明的读者应该已经猜到了，那就是向全球十大网安公司学习，学习他们深度融入 HTTPS 加密自动化。HTTPS 加密为何如此重要呢？因为这是木桶的底板，网络安全的底座。在数据为王和万物互联的时代，如果数据流动和数据交易不采用 HTTPS 加密方式传输，那其他任何安全防护都等于零！传统的网安产品用于堡垒式防护，但是现在的网络攻击，不再去攻击堡垒，攻不动，攻击者就懒得去攻了，直接守候在数据流通的通道上，直接把没有加密的 HTTP 流量轻松拿走，根本不用费力去攻击堡垒就可获得所需数据！这就是网络安全的现状，网安企业必须针对这个现状，在保持传统网安产品满足堡垒防护的基础上，为用户提供保障数据传输安全的网安产品和解决方案。



保障数据传输安全的成熟技术是 HTTPS 加密技术，网安企业需要深度融合密码技术，拥抱密码技术，提升网络产品的核心竞争力，把网络安全产品覆盖到七层网络协议的所有层。特别是要抓住目前我国高度重视国产商用密码的普及应用这个重点和热点，因为全球网络安全的底座是 RSA 密码体系，而为了保障我国网空安全，必须把这个底座再增加一个底板-国产密码体系，这是一个全产业链的升级改造，仅密码企业是完不成的，因为这个任务太重了，市场太大了，急需有实力的网安企业深度参与和深度融合。

如何深度融合？可以参考美国《联邦政府零信任战略》提出的五大安全目标：身份安全、设备安全、网络安全、应用安全和数据安全，这五大安全目标中的网络安全部分除了强调零信任架构外，重点强调了 3 个密码应用：加密 HTTP 流量(HTTPS)、加密 DNS 流量(DoH/DoT)、加密电子邮件流量(TLS IMAP/SMTP, S/MIME)，这三大流量的加密都离不开 HTTPS 加密，其他四个安全目标也都离不开密码应用—数字签名、加密和时间戳。而依据我国《密码法》第二条对密码的定义，就是需要应用各种商用密码产品和密码服务来实现加密保护和安全认证，这是强制要求，这就是我国的零信任战略，只信任采用商用密码保护的系统。密码是零信任安全(包括网络安全)的底座，商用密码是我国零信任安全(包括网络安全)的底座。



实现零信任安全的五大目标的核心是实现 HTTPS 加密，而要普及实现 HTTPS 加密，只有自动化一条路！因为传统的手动申请 SSL 证书和部署 SSL 证书实现 HTTPS 加密的方案是无法普及应用的，必须通过自动化方式才能实现，全球信任的有效的 SSL 证书签发量已经超过了 10 亿张，这是传统的人工申请和部署 SSL 证书时代所无法想象和无法达到的数量，也只有自

动化才能做到普惠 HTTPS 加密来保障全球互联网和万物互联的安全。

我国网安企业必须借鉴国际网安企业的成功经验，抓紧切入 HTTPS 加密自动化市场。但是，又不能完全照搬，因为国际 HTTPS 加密自动化只能实现 RSA 密码体系的自动化，不支持国产密码体系的自动化，所有 Web 服务器也不支持国密算法，这就需要有适合我国国情的 HTTPS 加密自动化解决方案，普及实现国密 HTTPS 加密自动化，只有实现了这个目标才能真正保障我国网络空间安全，这是重任只能落在网安企业身上，当然也是网安企业的新的市场机会，一个巨大的新蓝海市场机会，一个千亿级甚至万亿级的市场机会，抓住了就继续上升，如果抓不住就会被市场淘汰出局，因为现在是数据时代。

四、 网安企业应该如何切入 HTTPS 加密自动化蓝海市场？

通过上面的分析，相信有识之士已经跃跃欲试了。现在正是规划 2025 年业务发展计划的时候，笔者不能只提出问题，告诉大家这是一个巨大市场机会，而不告诉大家该怎么干。本部分就详细讲讲该如何干才能快速切入这个新蓝海市场。

1. 必须改变观念，不死守老三样，积极拥抱新形势和新市场

现在是数据为王和移动互联网时代，时代变了，市场也就变了，用户需求变了，传统的网安产品虽然在传统堡垒防护方面仍然有效，但是现在的市场是必须解决移动互联网和万物互联时代的数据流通传输安全问题，这是一个目前还没有解决的难题，因为现在的人工申请和部署 SSL 证书解决不了这个难题，以至于 31 个省市自治区政府官网只有 17 个实现了 RSA 算法 HTTPS 加密，只有 1 个湖南省实现了国密算法 HTTPS 加密，但还不是强制 HTTPS 加密，这个 HTTPS 加密市场需要自动化才能解决数据传输安全难题。

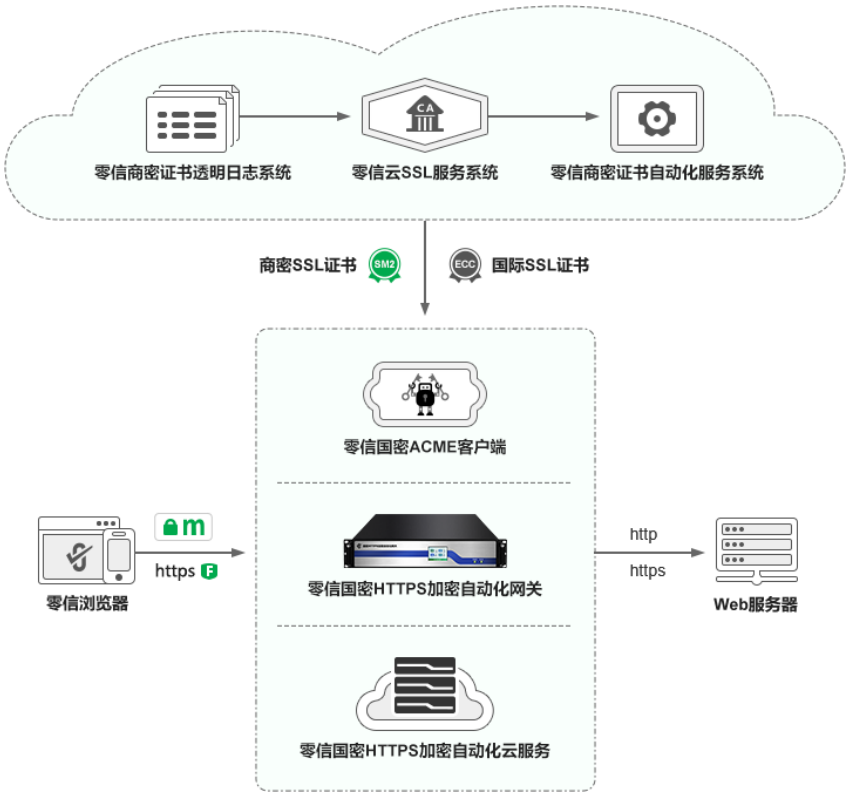
网安企业必须改变观念，不要以为这个市场是 CA 的市场或密码企业的市场，不要以为这是一个简单的销售一张几百元的 SSL 证书给用户的小生意，是一个销售国密 HTTPS 加密自动化解决方案给用户的大生意，订单至少是上百万、上千万、甚至上亿元的大单。这些大单只有网安企业深度切入这个市场才能落地，因为网安企业既有技术实力，又有专业的营销能力和市场能力，这些需要实现 HTTPS 加密自动化的政企用户和金融用户本来就是网安企业的用户，是传统网安设备的用户，只需把 HTTPS 加密自动化能力集成到传统网安设备中去，就可以帮助用户实现国密 HTTPS 加密自动化，也就能普及应用商用密码来保障我国关键信息基础设施安全，真正满足用户的等保合规和密评合规需求。这是一个三赢的市场，政企用户和金融用户

能真正轻松完成各种法律法规所要求的国密 HTTPS 加密改造和普及应用，密码企业的相关产品也得到了应用，网安企业赢得了新的市场机会。

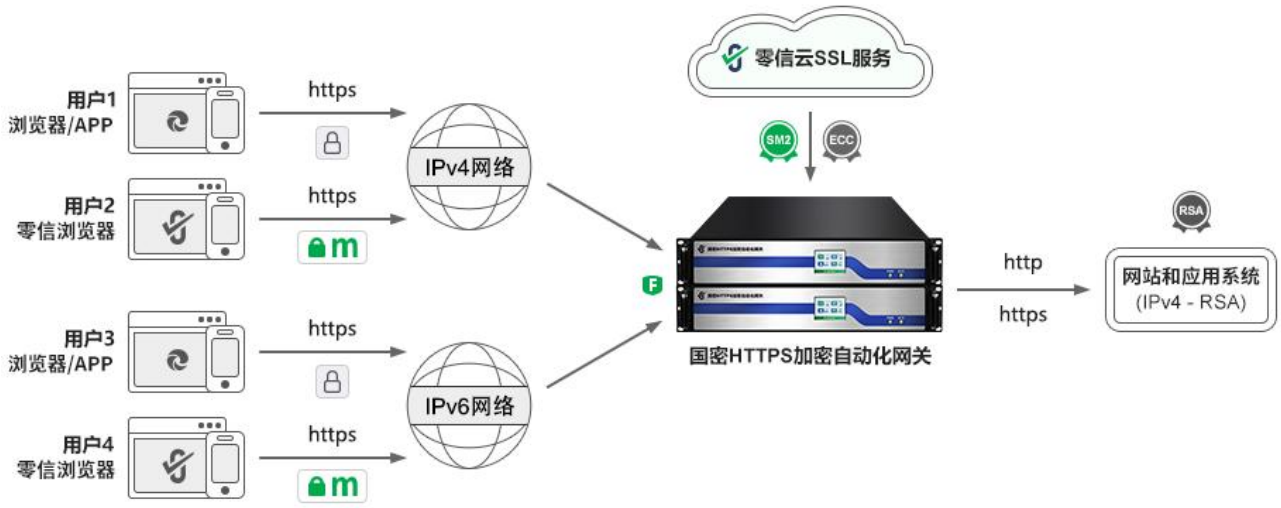
2. 做好充分技术准备，尽快具备双密码能力

网安企业由于不了解 HTTPS 加密市场，可能会认为这个市场有高不可攀的技术壁垒和政策壁垒，这就是笔者为何先讲国际网安巨头是如何切入这个市场的原因，让大家看到榜样的力量。但是，国外网安企业的经验仅供参考，我国网安企业必须同时具备国产密码能力和 RSA 密码能力，必须具备双算法 SSL 证书的可靠生产能力和自动化部署能力，简称为双密码能力。

零信技术历时 3 年研发，已经成功研发了国密证书透明生态和国密证书自动化管理生态所需的全系列密码产品，实现了端云一体的国密 HTTPS 加密自动化，能为网安企业提供双密码能力建设所需的所有产品和相关服务，让网安企业能在**两个月内**为其所有网安产品自动化配置自己品牌的双算法 SSL 证书，为用户提供国密 HTTPS 加密自动化解决方案，具备拿下国密 HTTPS 加密大市场的双密码能力。为什么需要双算法 SSL 证书呢？这是现阶段的实际应用需求—互联网公共服务不宜强制要求用户必须使用国密浏览器上网，必须同时支持 RSA 算法和 SM2 算法实现 HTTPS 加密。也就是说，必须保留木桶的现有底板不变，同时在下面增加一块兜底的国密底板，以备现有底板可能会被抽走，双底板双保险，就不怕 RSA 底板突然被非法抽走。



零信技术端云一体创新解决方案使得原先的传统方案需要投资建设四套系统来满足四种不同用户使用互联网服务的需求变成了只需建设一套系统，直接在已经建成的系统之前增加部署零信国密 HTTPS 加密自动化网关即可，原 Web 服务器零安装 SSL 证书，零改造，自动化满足用户 HTTPS 加密、WAF 防护、国密改造、IPv6 改造等各种合规应用需求。端云一体，更合理，更省事，更省钱，大大提升了系统可靠性，降低了系统管理难度。



也就是说，只要网安企业真想快速切入和拿下国密 HTTPS 加密自动化市场，零信技术就能帮助网安企业具备双算法 SSL 证书的可靠生产能力和自动化部署能力，只有具备了这两个密码能力，再加上已具备的市场营销能力，就能赢得国密 HTTPS 加密自动化大市场。

对于第一个密码能力，双算法 SSL 证书的可靠生产能力，必须像思科那样从全球信任的国际根 CA 定制 RSA 算法 SSL 中级根证书，同时还必须从拥有工信部和国密局 CA 许可证的 CA 机构的国密根证书定制 SM2 算法 SSL 中级根证书，实现自动化签发网安企业自己品牌的全球信任的国际 SSL 证书和国密合规的国密 SSL 证书，这就具备了双算法 SSL 证书的可靠生产能力。

第二个密码能力是双算法 SSL 证书的自动化部署能力，这就要参考 ACME 国际标准，遵循《自动化证书管理规范》国密标准草案，为所有与 HTTPS 加密相关的网安产品自动化配置自己品牌的双算法 SSL 证书，自动化实现双算法 HTTPS 加密。

第二个能力目前所有国际网安巨头都已经具备(RSA 算法 SSL 证书)，第一个密码能力不是目的，是基础，能提升核心竞争力，推荐网安企业自己直接具备这个能力，否则由于第一能力受制于人而有可能影响市场拓展。第二个密码能力才是真正能变现的能力，是能发挥网安企业的现有市场优势的能力。

如何具备第二个密码能力呢？我国网安企业无法照搬国外网安企业的经验，因为 RSA 密

码体系已经嵌入到所有系统和所有设备中，只需能自动化完成 SSL 证书申请、验证和取回部署即可。但是，目前所有系统和所有设备都不支持国产密码体系，这就有一个国密改造的难题，需要所有系统和所有设备支持国密算法，这是一个全生态产品升级改造的大工程。

也正是由于这个原因，急需已经具有各种网安产品线的网安企业的深度参与，直接让各种网安产品底层支持国产密码算法，只有像国际网安巨头那样在产品 OS 中支持 SSL 证书自动化管理，再加上支持国产密码算法，才能实现国密 HTTPS 加密自动化。如已经在政府网站广泛使用的 WAF 设备，只需增加支持国密算法，支持双算法 SSL 证书的自动化申请和部署就可以实现国密 HTTPS 加密自动化，就可以轻松帮助政府用户完成国密 HTTPS 加密改造。

3. 网安企业只要充分发挥已有市场优势，就能拿下国密 HTTPS 加密自动化大市场

HTTPS 加密自动化是网安企业保障网络通信数据传输安全的新业务，也可以理解为是网安产品的升级换代业务，比如说 SSL VPN 产品，现在是需要用户自己去向 CA 申请 SSL 证书，拿到证书后手动配置到 SSL VPN 设备中去使用，而升级换代后，销售给用户的 SSL VPN 产品只需用户设置好网址，就可以自动化配置网安厂商自己品牌的全球信任的国际 SSL 证书和国密合规的国密 SSL 证书，所有浏览器都信任的双 SSL 证书，自动化实现 HTTPS 加密，自动化完成了国密改造，这一定大受用户欢迎。

再比如说 WAF 设备和云 WAF 服务，现在是需要用户向 CA 申请 SSL 证书并手动配置到 WAF 中使用，而升级改造后，用户只需在 WAF 设备上配置好网站域名就可以自动配置网安厂商自己品牌的双算法 SSL 证书，自动启用国密 HTTPS 加密和 WAF 防护，自动化完成了国密改造，这也一定会大受用户欢迎。零信国密 HTTPS 加密自动化网关正是由于内置了 WAF 防护功能而接到了多个原计划采购传统 WAF 设备的订单，用户看中的是 HTTPS 加密自动化功能，一站式搞定 HTTPS 加密、WAF 防护、国密改造、IPv6 改造等多个网站安全防护应用需求和合规需求。

网安企业有现成的客户资源和良好的服务口碑，只需增加双密码能力，就可以为用户创新提供国密 HTTPS 加密自动化解决方案，解决用户急需完成国密 HTTPS 加密改造之所需。由四个部委联合发布的今年 7 月 1 日施行的《互联网政务应用安全管理规定》，要求所有政府官网、所有互联网政务服务系统都必须实现国密 HTTPS 加密安全连接访问，对于没有实现的单位将依规依纪追究当事人和有关领导的责任。但目前只有一个省政府官网、一个部委官网实现了国密 HTTPS 加密，这是给了网安企业一个非常大的市场机会，一个亿级市场机会，就看谁能抓住这个机会了。

由七个部委于今年 11 月 21 日联合发布的《推动数字金融高质量发展行动方案》，要求所有金融机构都必须采用商用密码来保障金融数据安全和网络安全，这也是要求银行官网、网银系统和银行业务系统必须实现国密 HTTPS 加密。而目前只有一个银行官网实现了国密 HTTPS 加密，还有大量的网银系统没有实现国密 HTTPS 加密，还有大量金融机构的官网都没有启用 HTTPS 加密，这也是给了网安企业一个非常大的市场机会，一个百亿级的市场机会，就看谁能抓住这个机会了。

还有非常火的人工智能大模型，所依赖的原始数据如果在数据采集和传输过程中不采用 HTTPS 加密，各种数据就极有可能被非法篡改而失去了价值，甚至会误导 AI 产生非常严重的错误结果而酿成巨大的安全事故。这个数据传输安全风险也同样存在于智慧城市建设的大数据采集上，同样存在于工业互联网的数据采集和自动控制中，同样存在于智能车联网的数据采集和自动控制中。数据的价值在于流通，所以，必须保障数据在流通通道上的安全，这就需要 HTTPS 加密，需要 HTTPS 加密自动化，需要国密 HTTPS 加密自动化。这是一个千亿级甚至万亿级的市场机会，就看谁能抓住这个机会了。

除了合规要求和实际应用场景需求外，还有密码管理部门的执法检查，这个对拿下这些市场机会非常有利。7 月 19 日国家密码管理局根据《中华人民共和国密码法》、《商用密码管理条例》及相关商用密码管理规章发布了《国家密码管理局商用密码随机抽查事项清单(2024 年版)》，这是一个非常高明的执法检查手段，既能解决执法部门执法人力不足的难题，又能体现被检查对象的公平性，还能达到法律具备足够的威慑力的效果。列入抽查对象的所有单位为了应对这个随时会落下的执法宝剑，只有自动化这一条康庄大道可走，只有自动化实现商密 HTTPS 加密和 WAF 防护，才能从容应对随时随地的各种合规执法检查，才能真正普及应用商用密码来保证我国关键信息基础设施的安全可靠运行。

列入密码执法检查的所有单位都是网安市场的用户，不仅有随时被随机抽查的压力，而且还有一个即将落下的技术压力，那就是国际标准即将落地的 SSL 证书有效期缩短为 90 天或者 45 天，这是为了保障 SSL 证书密钥安全和 HTTPS 加密安全的有力措施，同时也是为了应对量子计算对传统密码算法的安全威胁。这个技术宝剑一旦落下，传统的手动申请和部署 SSL 证书已经成为不可能，用户不可能对几百个、几千个甚至上万个网站每年手动申请和安装 5 次或 10 次 SSL 证书，只有自动化一条路可走，部署 HTTPS 加密自动化解决方案成为必选之方案，这也是将近到来的巨大市场机会的有力技术证明。

也正是由于我国需要普及国密 HTTPS 加密自动化，需要同国际上的 HTTPS 加密自动化不一样的解决方案，这就给了我国网安企业一个得天独厚的巨大市场机会，网安企业必须尽快具备双密码能力，才能抓住这个巨大的市场机会。笔者坚信：经历过几十年风雨洗礼的我国网

安企业一定能抓住这个难得的市场机会，继续为保障我国网络空间安全做出新的贡献，取得新的辉煌。

王高华

2024 年 12 月 30 日于深圳

欢迎关注零信技术公众号，实时推送每篇精彩 CEO 博客文章。
已累计发表中文 198 篇(共 57 万 2 千多字)和英文 84 篇(10 万 9 千多单词)。