

# 网安市场的新蓝海是 HTTPS加密自动化

---

王高华 Richard Wang

2024.12.30



# 目录

一

“木桶理论”的底板是什么？如果底板不牢怎么办？

---

二

全球十大网安公司都在深度融合HTTPS加密自动化

---

三

国密HTTPS加密自动化是我国网安市场的新蓝海

---

四

网安企业应该如何切入HTTPS加密自动化蓝海市场？

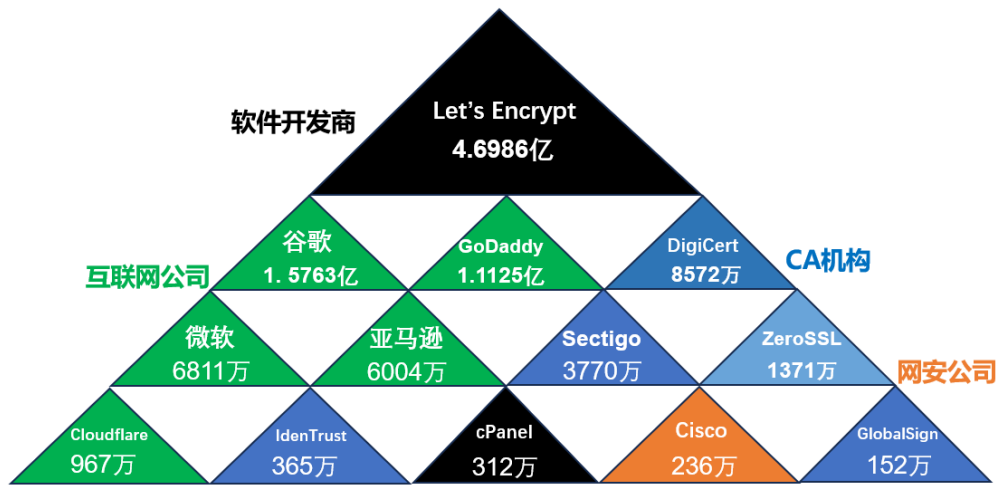
1. 必须改变观念，不死守老三样，积极拥抱新形势和新市场
2. 做好充分技术准备，尽快具备双密码能力
3. 网安企业只要充分发挥已有市场优势，就能拿下国密HTTPS加密自动化大市场

# 一、“木桶理论”的底板是什么？如果底板不牢怎么办？



- 一只木桶的盛水量取决于桶壁上最短的那一块。
- 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”。
- 网络安全的底板是密码体系，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，政府网站和银行网站的SSL证书被断供和已有SSL证书被吊销。
- 网络安全防护的底板都没有了，也就失去了其他安全防护的价值。

# 一、“木桶理论”的底板是什么？如果底板不牢怎么办？



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)

- 全球互联网巨头都已经深度融入HTTPS加密自动化市场，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13大SSL证书提供商中只有1家网安公司-Cisco，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！

## 二、全球十大网安公司都已深度融入HTTPS加密自动化

1. Cisco
2. Palo Alto
3. Fortinet
4. Check Point
5. Juniper
6. Zscaler
7. Symantec
8. Trend Micro
9. IBM Security
10. F5

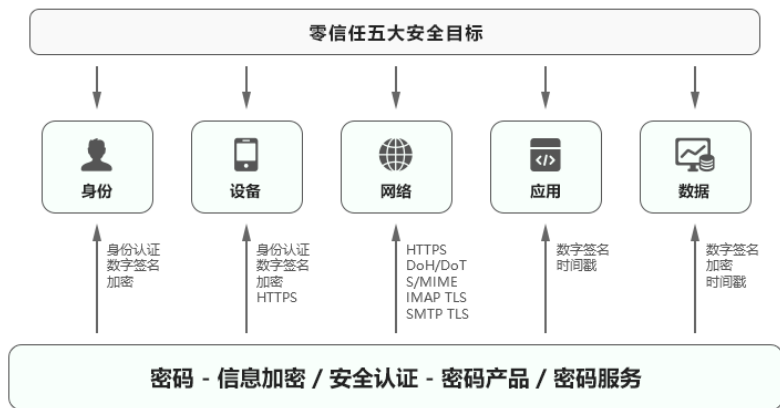
- 思科既是第一大网安公司，也是第12大SSL证书提供商，同时也是一个证书消费者，自动化为其网络设备配置SSL证书实现了三种身份的统一。
- 所有国际网安巨头的网络设备都已经支持国际标准ACME协议的SSL证书自动化，方便用户只需配置域名就可以自动化免费实现HTTPS加密。
- 思科从全球信任根CA-DigiCert定制Cisco品牌中级根证书用于为其网络设备自动签发SSL证书。
- 其他厂商直接使用 Let's Encrypt 和 Google Trust 免费提供的ACME SSL证书自动化服务，为其网络设备自动配置SSL证书。
- Fortinet已为其网络设备签发了18亿张内网SSL证书。
- 赛门铁克曾投巨资收购了当时全球最大的CA-VeriSign，趋势科技曾收购了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。

### 三、国密HTTPS加密自动化是我国网安市场的新蓝海



- 数据为王和万物互联时代，网络安全的重点是保障数据流通的传输安全，攻击者不再攻击已经全副武装的服务端，而是直接在数据传输通道上窃取HTTP明文传输数据。
- 传统堡垒防护市场已经严重饱和，并且不再是防护重点，重点是HTTPS加密传输，保障数据传输安全！
- 网安企业必须提供保障网络安全底座安全的产品和服务，网安企业必须深度融合密码。
- 也只有网安企业深度参与才能完成完成国密改造重任，特别是HTTPS加密国密改造！

### 三、国密HTTPS加密自动化是我国网安市场的新蓝海



- 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，其中网络安全部分只有3个：加密HTTP流量、加密DNS流量、加密电子邮件流量，都离不开HTTPS加密，我国则是必须实现国密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。
- 实现零信任安全五大目标需要各种密码产品和密码服务来实现加密保护和安全认证。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。这是一个千亿级甚至万亿级的市场机会，网安企业必须抓住！

## 四、网安企业应该如何切入HTTPS加密自动化蓝海市场？

### 1 必须改变观念，不死守老三样，积极拥抱新形势和新市场

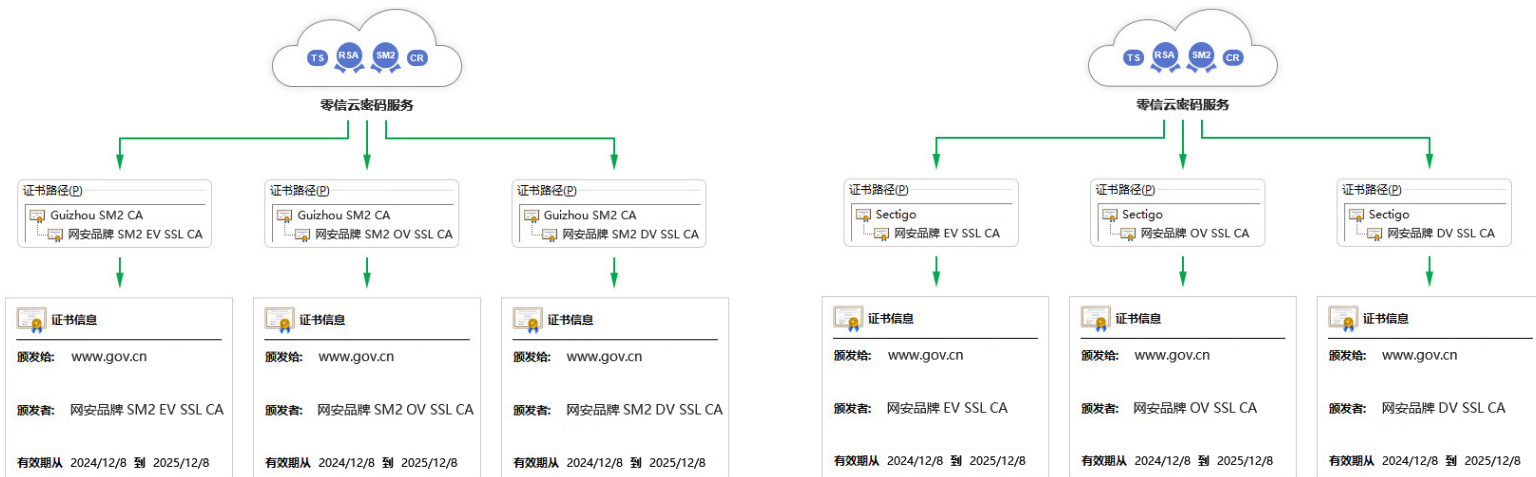
- 现在是数据为王和移动互联时代，时代变了，市场也就变了，用户需求变了，传统的网安产品虽然在传统堡垒防护方面仍然有效，但是现在的市场是必须解决移动互联和万物互联时代的数据流通传输安全问题，这是一个目前还没有解决的难题。
- 网安企业必须改变观念，不要以为这个市场是CA的市场或密码企业的市场，HTTPS加密自动化市场是销售一套国密HTTPS加密自动化解决方案给用户的大生意，订单至少是上百万、上千万、甚至上亿元的大单。这些大单只有网安企业切入这个市场才能落地，因为网安企业既有技术实力，又有专业的营销能力和市场能力。
- 这是一个三赢的市场，政企用户、金融用户能真正轻松完成各种法律法规所要求的国密HTTPS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。



## 四、网安企业应该如何切入HTTPS加密自动化蓝海市场？

### 2 做好充分技术准备，尽快具备双密码能力

**第一个密码能力** 是双算法SSL证书的可靠生产能力，定制RSA算法和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。

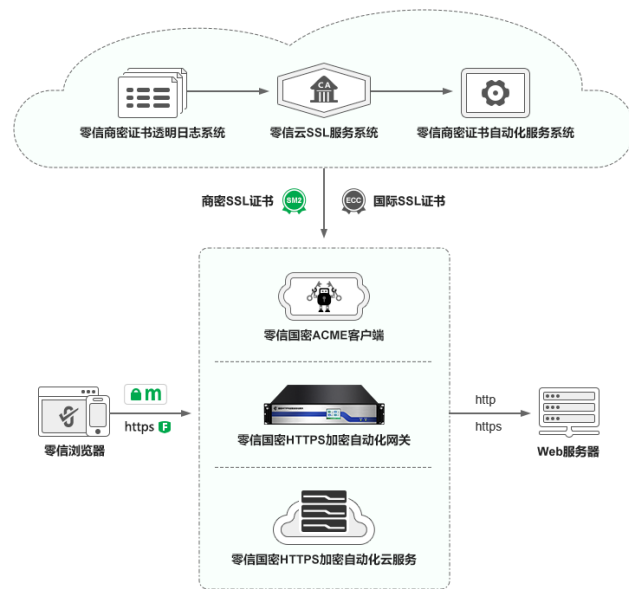


## 四、网安企业应该如何切入HTTPS加密自动化蓝海市场？

### 2 做好充分技术准备，尽快具备双密码能力

**第二个密码能力**是双算法SSL证书的自动化部署能力，为所有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。

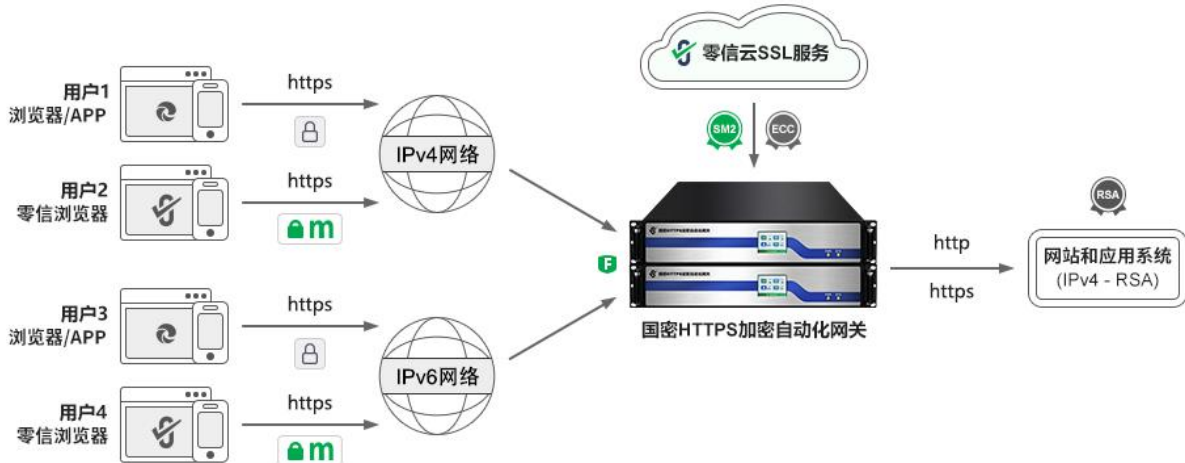
零信技术历时三年研发，已经成功研发了国密证书透明生态和国密证书自动化管理生态所需的全系列商用密码产品，实现了端云一体的国密HTTPS加密自动化，能为网安企业提供双密码能力建设所需的所有产品和服务，让网安企业能**两个月内**为其所有网安产品自动化配置自己品牌的双算法SSL证书，为用户提供国密HTTPS加密自动化解决方案，具备拿下国密HTTPS加密大市场的**双密码能力**。



## 四、网安企业应该如何切入HTTPS加密自动化蓝海市场？

### 2 做好充分技术准备，尽快具备双密码能力

零信创新解决方案让用户只建一套系统，部署一套网关，就能满足RSA/SM2和IPv4/IPv6的HTTPS加密、WAF防护、国密改造、IPv6改造等合规需求。端云一体，更合理，更省事，更省钱，提升了系统可靠性，降低了系统管理难度！



## 四、网安企业应该如何切入HTTPS加密自动化蓝海市场？

### 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，只需现有网安产品集成HTTPS加密自动化能力即可。
- 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，这是一个亿级市场机会。
- 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，也就是必须实现国密HTTPS加密，这是一个百亿级市场机会。
- AI大模型、智慧城市、工业互联网、智能网联汽车等等重要数据传输安全都需要HTTPS加密自动化，这是一个百亿级甚至千亿级的市场机会。
- 国家密码管理局发布的《[国家密码管理局商用密码随机抽查事项清单\(2024年版\)](#)》，则是一把助力国密HTTPS加密自动化市场落地的利器，而即将实施的缩短SSL证书有效期为90天或45天则是一个技术利器。
- 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！