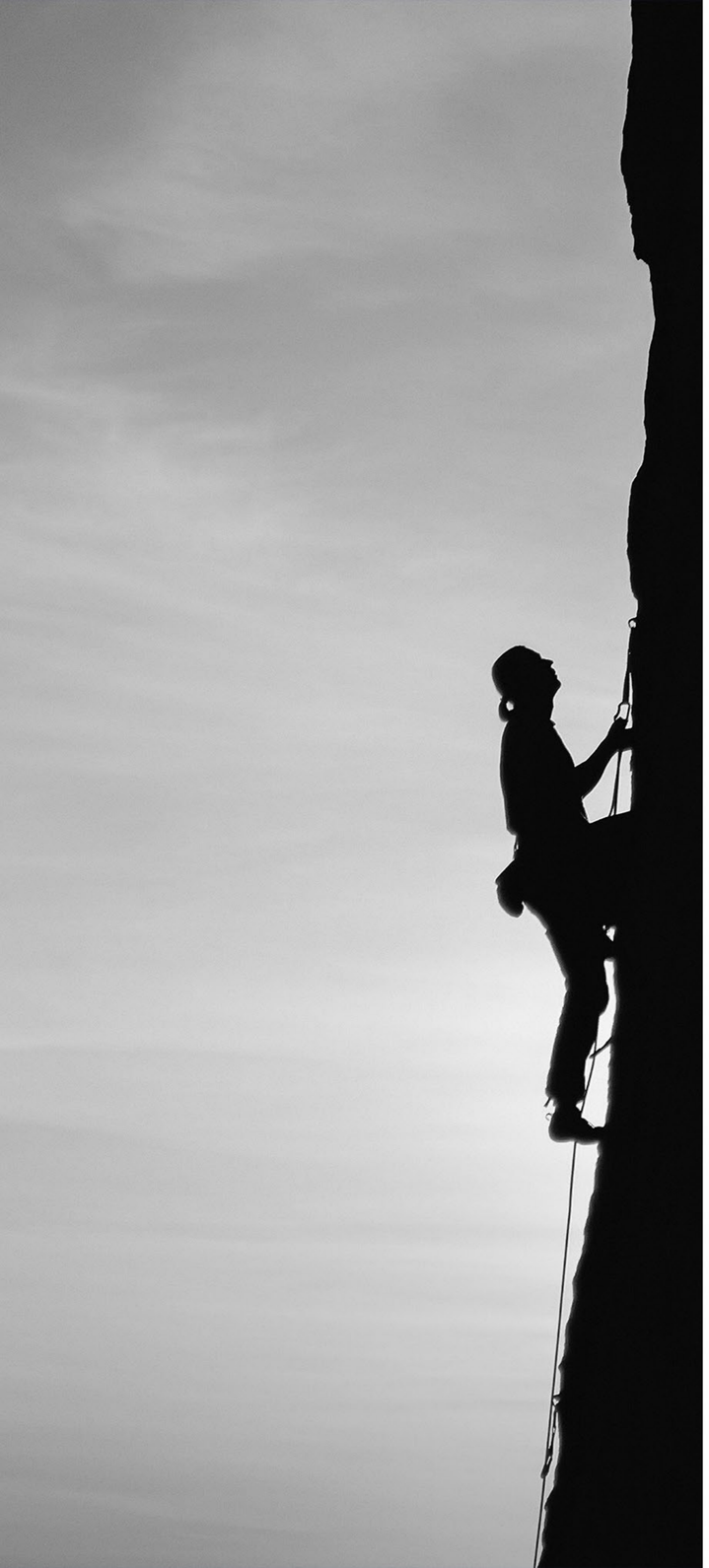
零信®
ZoTrus

零信技术HTTPS加密自动化管理解决方案

零信技术（深圳）有限公司
ZoTrus Technology Limited
www.zotrus.com
2024.01



目录 ZOTRUS

01 实施HTTPS加密的挑战

02 手动安装SSL证书实现HTTPS加密并非用户所需

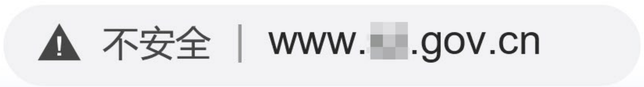
03 ACME，HTTPS加密终极解决方案!

04 HTTPS加密自动化解决方案，彻底完美解决三大难题

05 零信国密HTTPS加密自动化三大配套服务

06 权威认证和客户案例

1 实施HTTPS加密的挑战



为何明明知道浏览器提示“不安全”，却不部署SSL证书?

为何明明知道密码合规要求，却不部署国密SSL证书?

为何省政府网站部署了这么少的SSL证书?

用户知道需要部署SSL证书，所以个别政务网站部署证书了！

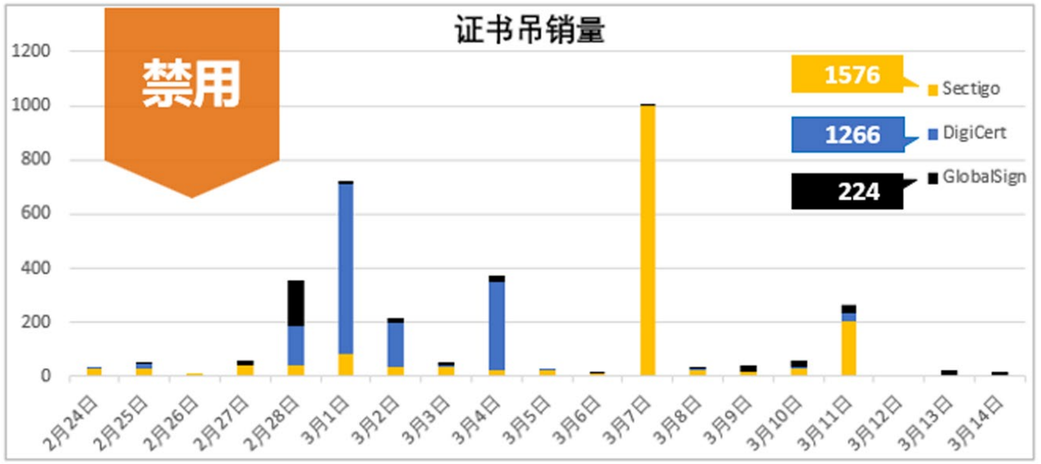
为何其他大量的政务网站不部署？是缺钱?

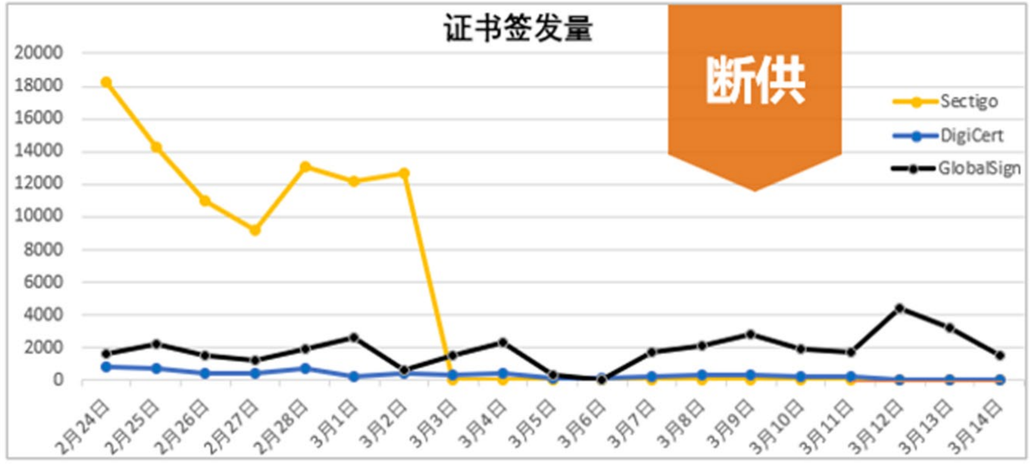
国密 https

RSA https

RSA https + WAF

2022年俄乌冲突后.ru/.by/.su SSL证书吊销和签发情况





这意味什么？ 全球互联网还需要RSA密码体系以外的体系实现HTTPS加密，那就是SM2体系！

实现HTTPS加密的三大难题

难题一

人工手动部署SSL证书，非常繁琐、费时费力

如何实现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，以及企业在各个不同的公共云服务商申请多个Web服务器，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。

政务云和企业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重新部署SSL证书将严重影响业务系统的正常运行而带来不可估量的损失。

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。其难题在于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，国密改造涉及面太广，难度很大，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5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生态系统具有到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5次，难题一的巨大工作量又一下子增加了5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证书自动化管理。

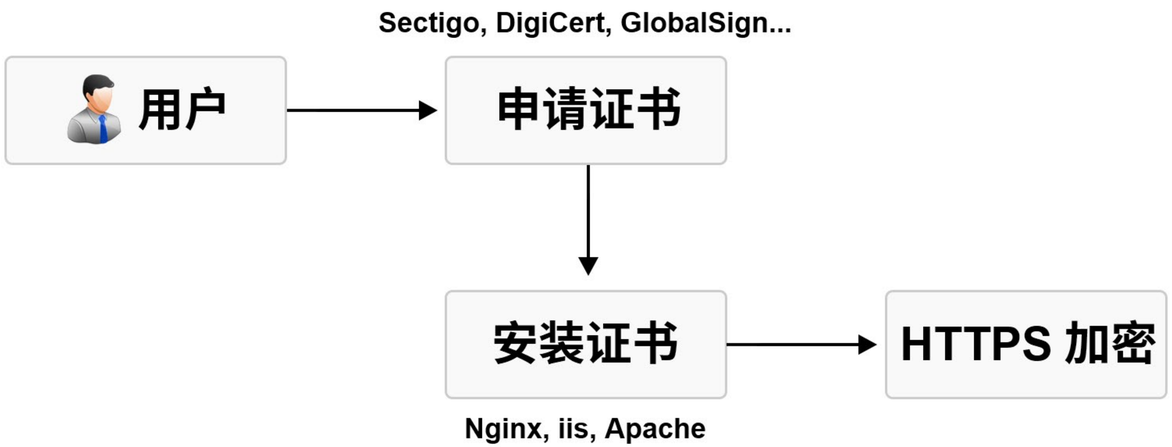
ZOTRUS

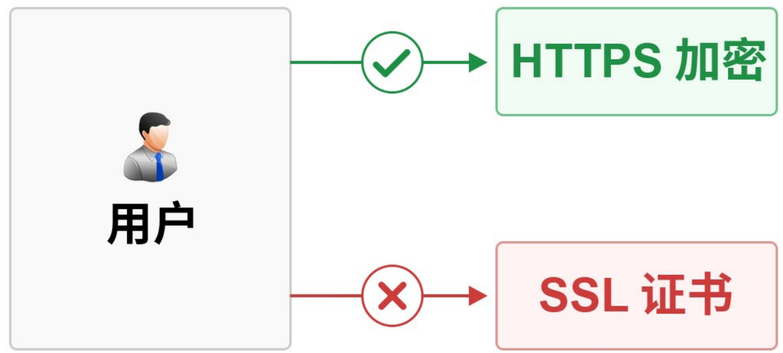
有解？当然有！自动化配置双算法SSL证书实现HTTPS加密！

- 三大难题就是压在网管和运维头上的三座大山，必须有解决方案解决这些难题。
- 零信技术创新地研发了三大解决方案和相关的产品，实现自动化申请、部署和续期双算法SSL证书，全自动、零改造，无需关心证书有效期，彻底完美地解决了以上三大难题和一大挑战。

2 手动安装SSL证书实现HTTPS加密并非用户所需

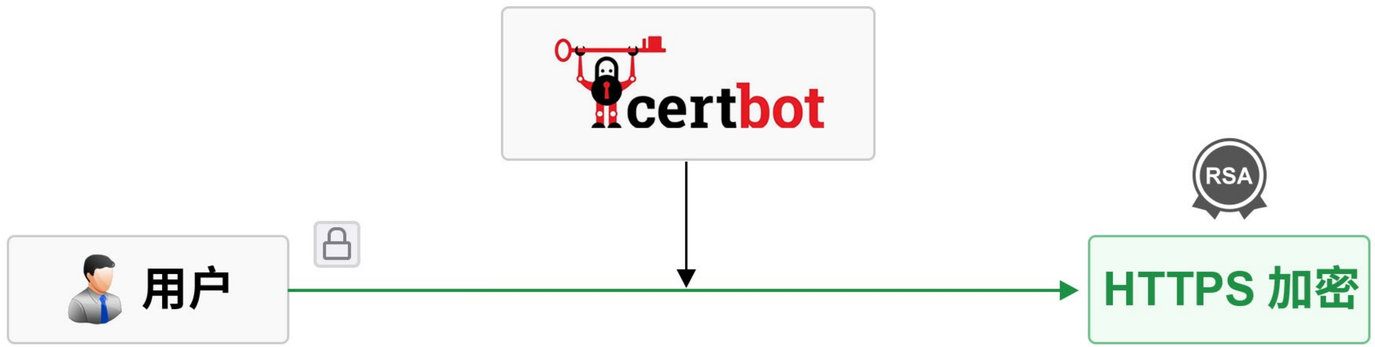
- 用户需要的是HTTPS加密，需要的是消除浏览器的“不安全”警告，需要的是国密合规！不是SSL证书！
- 我们应该为用户提供HTTPS加密解决方案，而不是用户实际不需要的SSL证书！





3 ACME，HTTPS加密终极解决方案！

ZOTRUS



acme

英 /ˈækmi/

n. 顶点；顶峰；

国际解决方案

ACME：自动化证书管理环境，RFC8555，给用户所需要的产品-HTTPS加密，而不是SSL证书！ Let's Encrypt大获成功！密，而不是SSL证书！

国密解决方案

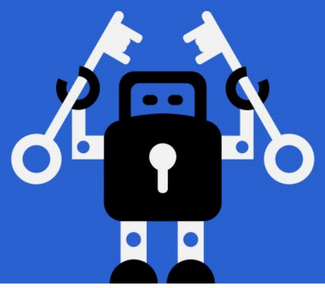
国密ACME，国密HTTPS加密终极解决方案！

要想普及应用国密SSL证书，只有自动化申请和部署管理一条道！

但是，国际ACME不是我们的道

因为不支持国密SSL证书，

Web服务器软件也不支持国密算法！

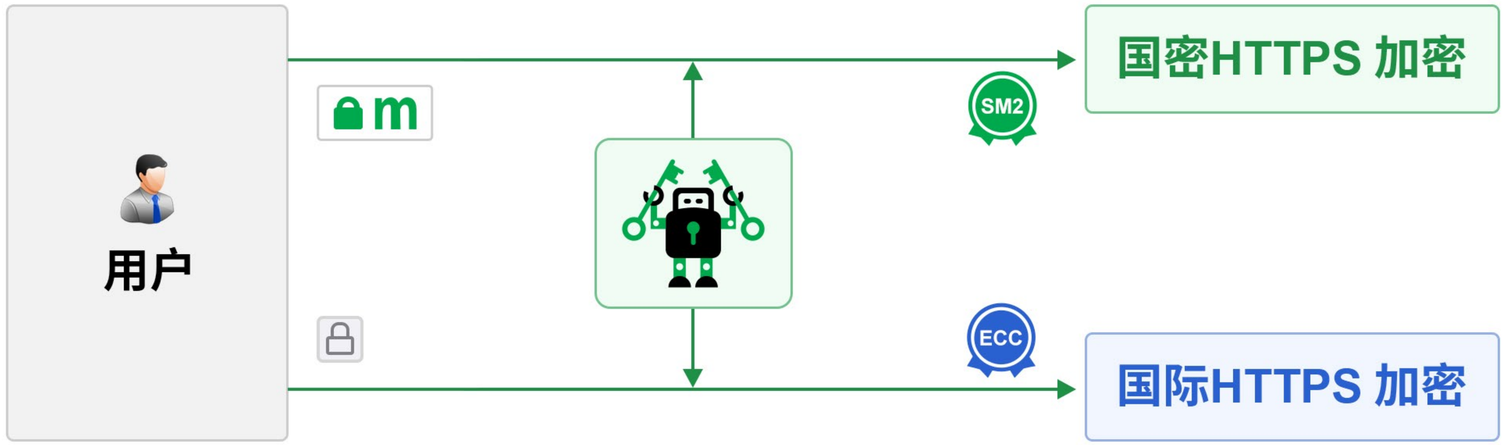


中国的道是：国密ACME = 国际ACME + 国密SSL证书 + 国密算法模块

零信技术鼎力打造，国密HTTPS加密终极解决方案！

国密解决方案

国密ACME，国密HTTPS加密终极解决方案！



国际SSL证书

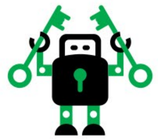
国密ACME = 国际ACME + 国密SSL证书 + 国密算法模块

零信技术打造国密证书自动化管理生态(SM2 ACME)

4 零信技术HTTPS加密自动化解决方案，彻底完美解决三大难题

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125万元，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。

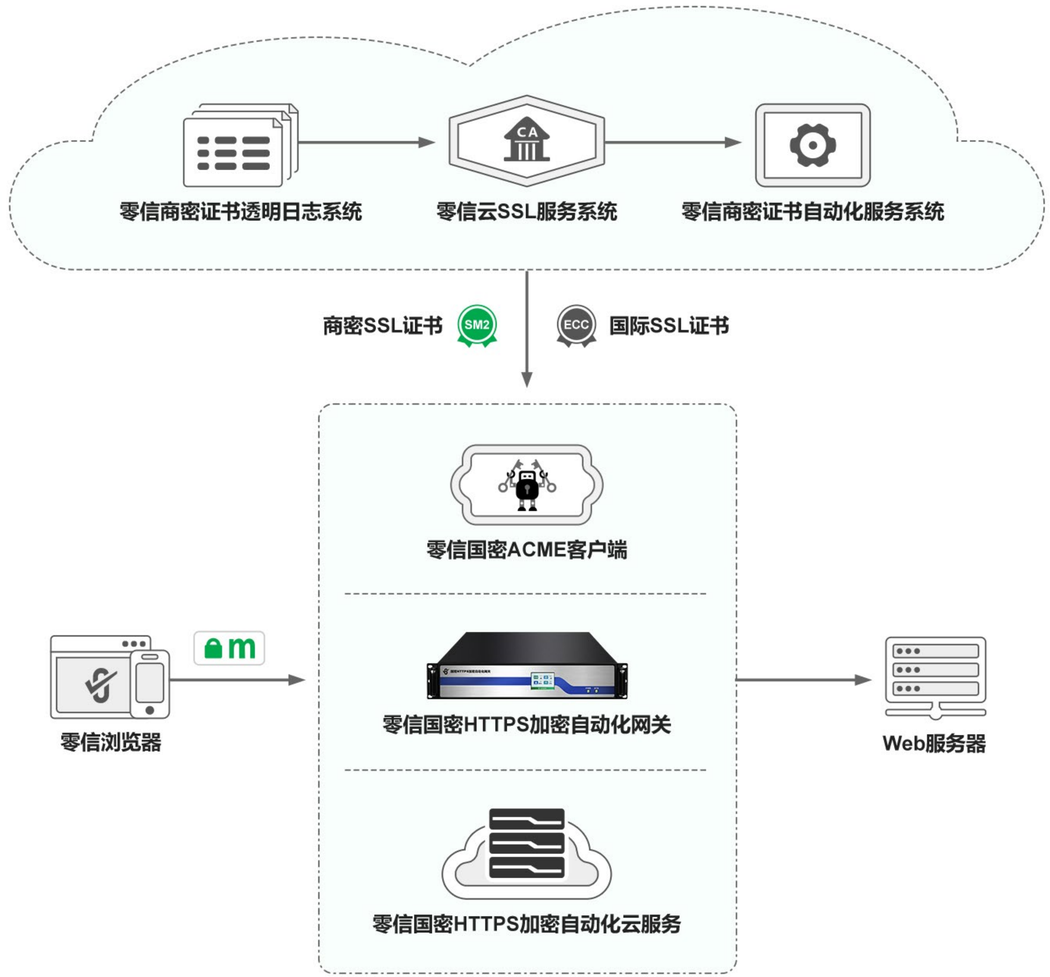
零信国密HTTPS加密自动化云服务是一个基于业界领先的阿里云CDN/WAF服务打造的集HTTPS加密自动化、CDN高速分发、边缘WAF防护、网站可信认证于一体的全方位网站安全防护解决方案，适合于单个网站的安全防护和HTTPS加密自动化管理，每个网站需要启用一个独立的HTTPS加密云服务。

零信技术HTTPS加密自动化管理三大解决方案对比表

	解决方案一 零信国密ACME客户端软件	解决方案二 零信国密HTTPS加密自动化网关	解决方案三 零信国密HTTPS加密自动化云服务
一次操作	安装软件	部署设备	解析域名
自动申请和部署双SSL证书	90天有效期ECC DV SSL证书 90天有效期SM2 DV SSL证书	1年期ECC DV SSL证书 1年期SM2 OV SSL证书	1年期ECC DV SSL证书 1年期SM2 OV SSL证书
自动续期双SSL证书	是的，每90天	是的，每365天	是的，每365天
支持网站数量	不限	50/100/150/255个	1个，可选购多个
服务年限	不限	5年	1年，可选购多年
费用	0元	19.8万元-99.8万元	4888元-98888元
可选配其他证书类型	可选购1年期DV / OV / EV证书	可选ECC OV / EV 和 SM2 EV	可选ECC OV/EV 和 SM2 EV
原Web服务器零改造	否	是	是
含WAF防护	不	含	含
含CDN服务	不	不	含
含网站可信EV认证	不	含	含
浏览器支持	国际SSL证书: 所有浏览器 国密SSL证书: 零信浏览器	国际SSL证书: 所有浏览器 国密SSL证书: 所有国密浏览器	国际SSL证书: 所有浏览器 国密SSL证书: 所有国密浏览器
适用场景	新建网站	有多个网站系统需要自动化部署SSL证书，独立自主管理	1个或几个网站系统需要自动化部署SSL证书，无需采购硬件
不足之处	需要重装Nginx和安装客户端软件	无	依赖云服务

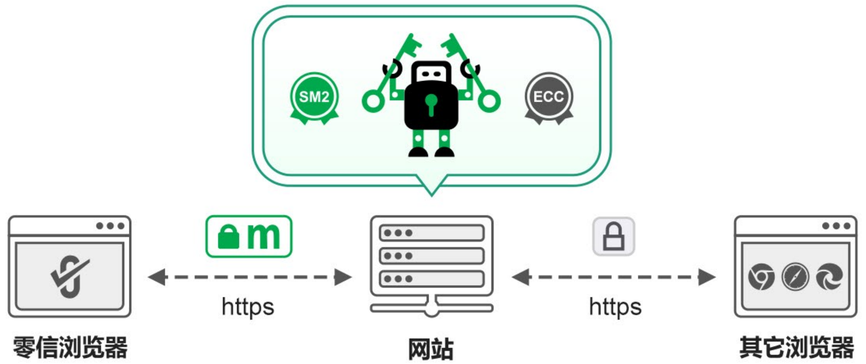
鼎力打造国密HTTPS加密自动化管理八大核心产品

零信技术已经成功打造国密证书透明生态产品和国密证书自动化管理生态产品的八大核心产品，包括：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。

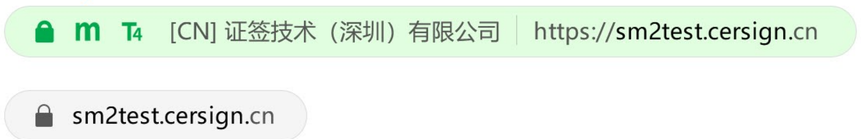


方案一　一次安装、永久自动实现国密HTTPS加密

- 只需在服务器上一键安装国密ACME客户端软件-SM2cerBot
- 自动申请和部署90天国密 DV SSL证书
- 自动申请和部署90天国际DV SSL证书
- 双证书到期自动续期
- 双证书部署，自适应算法HTTPS加密
- 零信浏览器国密算法加密，其他浏览器国际算法加密，实现国密合规和全球信任



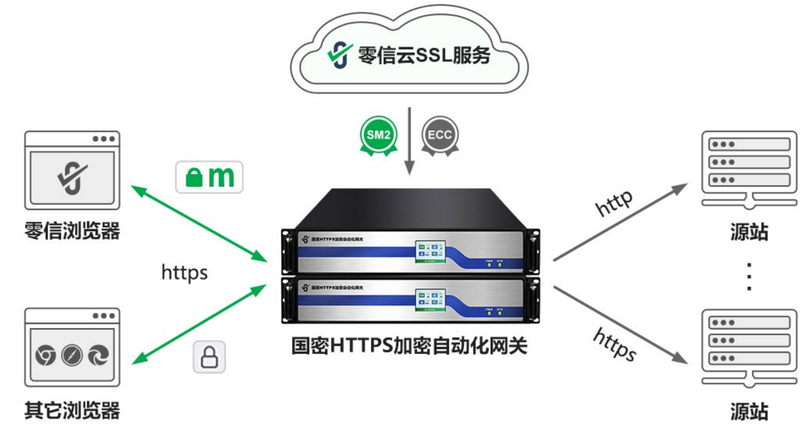
实施后效果



不能满足重要系统服务器不能动的需求，仅适用于新建网站！

方案二　一次部署、自动实现国密HTTPS加密和WAF防护

- 只需部署国密HTTPS网关，高速HTTPS加密响应、快速HTTPS卸载
- 原服务器零改动、零改造
- 自动申请和部署国密SSL证书
- 自动申请和部署国际SSL证书
- 双证书到期自动续期
- 双证书部署，自适应HTTPS加密、WAF防护、网站可信认证
- 零信浏览器国密算法加密，其他浏览器国际算法加密，实现国密合规和全球信任

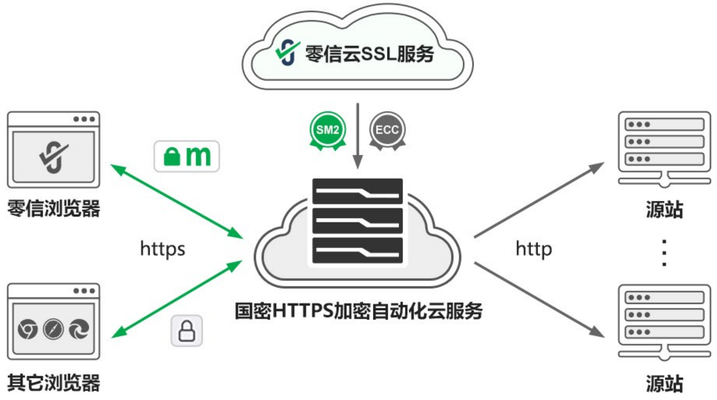


实施后效果

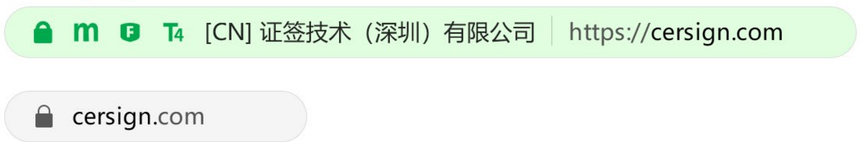
能满足重要系统Web服务器不能动需求，最多支持255个网站

方案三　一次设置、自动实现国密HTTPS加密和云WAF防护

- 只需做一次域名解析设置
- 原服务器零改动、零改造
- 自动申请和部署国密SSL证书
- 自动申请和部署国际SSL证书
- 双证书到期自动续期
- 双证书部署，自适应HTTPS加密、云WAF防护、CDN分发、可信认证
- 零信浏览器国密算法加密，其他浏览器国际算法加密，实现国密合规和全球信任



实施后效果



能满足重要系统Web服务器不能动需求，但依赖第三方云服务

5 零信国密HTTPS加密自动化三大配套服务

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。

6 权威认证和客户案例

商用密码产品认证证书

证书编号：GM004410620230847

委托人名称及所在地

零信技术(深圳)有限公司
深圳市南山区粤海街道滨海社区高新南十道87、89、91号深圳市软件产业基地2栋C301C

生产者（制造商）名称及所在地

零信技术(深圳)有限公司
深圳市南山区粤海街道滨海社区高新南十道87、89、91号深圳市软件产业基地2栋C301C

生产企业名称及所在地

零信技术(深圳)有限公司
北京市朝阳区朝外大街19号华普国际大厦714

产品名称和型号、版本

国密 HTTPS 加密自动化网关
SM2-HTTPS-Auto-Gateway-MG V1.0

产品标准和技术要求

GM/T 0025《SSL VPN 网关产品规范》
GM/T 0028《密码模块安全技术要求》第二级要求

上述产品符合商用密码产品认证规则的要求，特此发证。

颁发日期：2023 年 9 月 27 日　　有效期至：2028 年 9 月 26 日

证书有效期内本证书的有效性依据发证机构的定期监督获得维持。

牛路宏

国家密码管理局商用密码检测中心

中国·北京·万丰路300号　www.scctc.org.cn 证书通过此网站查询

《商用密码产品认证证书》

2023年9月23日，零信国密HTTPS加密自动化网关通过国家密码局商用密码检测中心的安全二级商用密码产品认证。

第二十五届中国国际高新技术成果交易会
CHINA HI-TECH FAIR 2023

优秀产品奖证书

获奖单位：零信技术(深圳)有限公司

获奖项目：零信国密HTTPS加密自动化网关

中国国际高新技术成果交易会组委会

二〇二三年十一月

优秀产品奖

第二十五届(2023)中国国际高新技术成果交易会组委会颁发给零信国密HTTPS加密自动化网关。

大客户案例

遵循《自动化证书管理规范》和《证书透明规范》商密标准草案

密码行业标准化技术委员会

密标委发〔2023〕9号

关于下达2023年度密码行业标准制修订任务（商用密码领域）的通知

2023年度密码行业标准制修订任务（商用密码领域）

牵头承担单位：零信技术（深圳）有限公司

序号	项目名称	类型	时间安排	工作组
1	证书透明规范	制定	2025.12 完成标准报批稿	基础工作组
2	自动化证书管理规范	制定	2025.12 完成标准报批稿	基础工作组

- 零信技术牵头立项制定商密标准《证书透明规范》和《自动化证书管理规范》
- 零信浏览器和零信国密HTTPS加密自动化网关率先遵循两个标准草案

参考阅读

ZOTRUS

什么是国密ACME？国密HTTPS终极解决方案

ACME实现了国际SSL证书的自动化管理(申请和部署)，国密ACME则实现了国密SSL证书和国际SSL证书的双证书自动化管理，同时实现了Web服务器的国密算法支持，这是国密HTTPS加密的终极解决方案！

国密HTTPS加密自动化网关，HTTPS国密改造首选

这是一个内置国密ACME客户端，支持国密算法和国密SSL证书的升级版硬件安全网关，满足了政务网站零改造实现国密HTTPS加密的需求。终极解决方案，政务网站HTTPS加密国密改造首选!

SSL证书自动化部署，保障业务系统https加密不间断

国密ACME服务是目前唯一一个能不间断地自动化申请和配置国密SSL证书和国际SSL证书的创新云服务，保障HTTPS加密不中断必选。

零信®
ZoTrus

欢迎选用零信HTTPS加密自动化解决方案

尽享无忧HTTPS加密，自动持续保障业务系统安全！

客服微信

公众号

欢迎联系我们：0755-26604080，微信：CerSignZoTrus，Email: help@zotrus.com