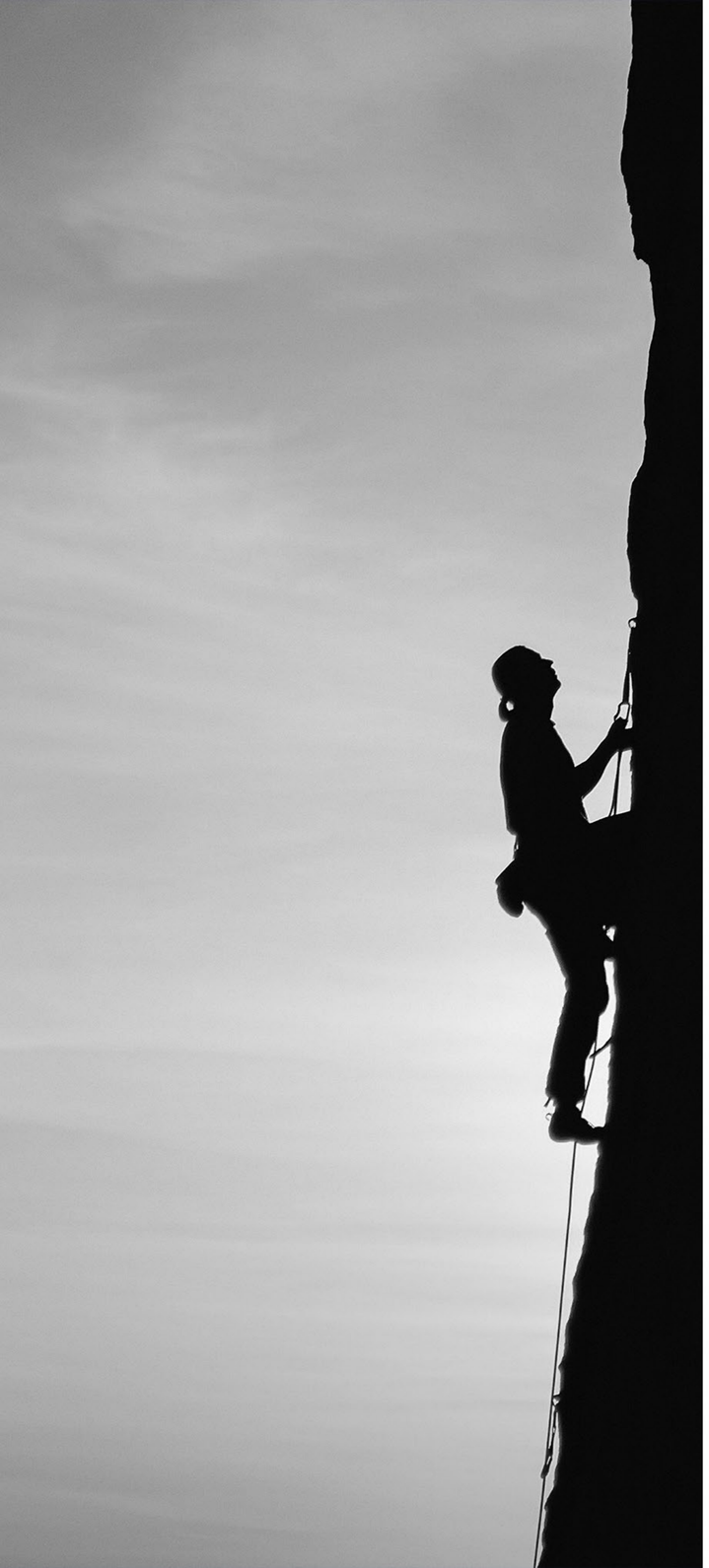
ZoTrus®

ZoTrus
HTTPS Automation Management Solution

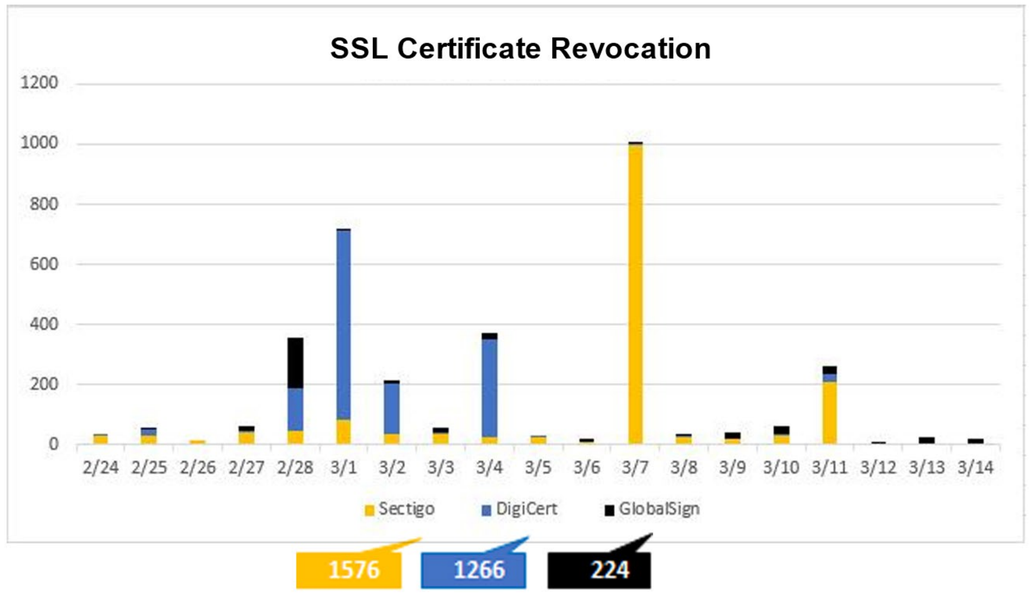
ZoTrus Technology Limited
www.zotrus.com
2024.01

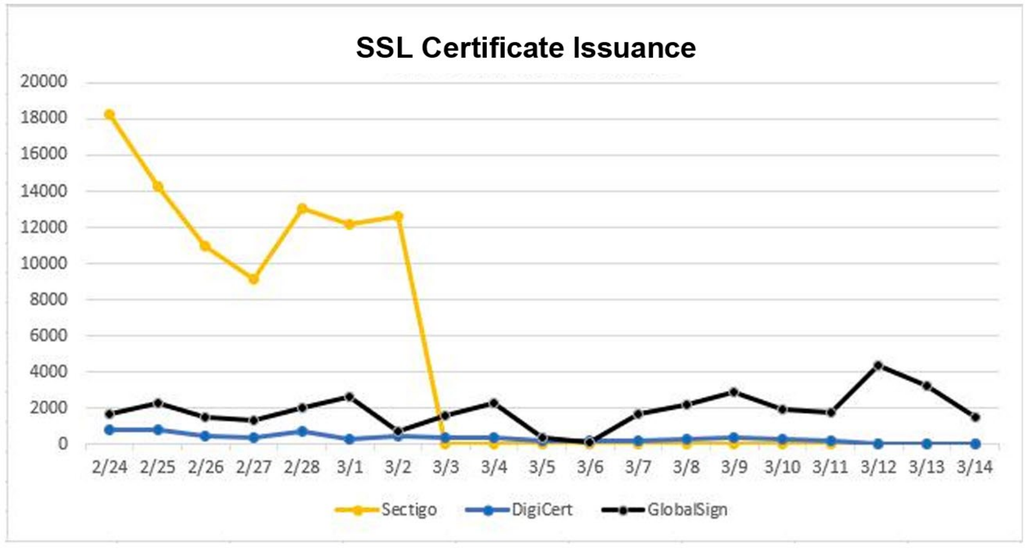


CONTENTS ZOTRUS

1 The challenges in implementing HTTPS encryption

Revocation and dis-supply of SSL certificates for domain .ru/.by/.su after the Russia-Ukraine conflict in 2022 (government and bank websites)





What this means?

The global Internet need a system other than RSA system for HTTPS encryption, the SM2 system is another choice!

Another 3 problems in implementing HTTPS encryption

Problem One:

Manually deploying SSL certificates is an impossible task.

To implement https encryption, the user must apply for an SSL certificate from the CA, get the certificate after completing identity validation, and then install the SSL certificate on the web server to enable https encryption. This process is very cumbersome, time-consuming, and labor-intensive. For tens of thousands of websites management, this is a big workload for IT administrators, they must invest more operation and maintenance personnel to realize https encryption for multiple websites. Otherwise, once the SSL certificate of a system expires and forgets to renew and redeploy the SSL certificate, it will seriously affect the normal operation of the business system and cause immeasurable losses.

Problem Two:

It is difficult to implement SM2 HTTPS encryption.

One of the compliance requirements of the Cyber Security Protection and Cryptography Security Protection is "network and communication transmission security", that is, the HTTPS encryption of the web server, which must be implemented using the SM2 algorithm. This requires the web server to deploy a SM2 SSL certificate, the user needs to apply for SM2 SSL certificate from the CA and deploy it to the web server for https, this step's difficulty is the same as Problem One.

However, to enable the SM2 SSL certificate, it is not only necessary to install the SSL certificate, but also to modify the web server to support SM2 algorithm, and users are required to use a browser that supports SM2 algorithm to implement the SM2 https encryption. The problem is that some important web servers in use cannot be changed, modified, cannot affect the running business system, and some web server software cannot be modified at all.

Problem Three:

SSL certificate period will be shortened to 90 days.

This is an upcoming problem. In order to ensure the security of https encryption, Google is promoting the shortening of the validity period of SSL certificates from the current 1 year to 90 days, with the intention of making the PKI ecosystem have the agility to resist quantum algorithms. This means that the original need to apply for and deploy an SSL certificate for the website once a year has become 5 times a year, and the huge workload of Problem One has increased by 5 times! This makes manual application and deployment of SSL certificates impossible!

This revolutionary technological change is expected to come in 2024, and all website administrators must prepare in advance to realize the automatic management of SSL certificates in advance.

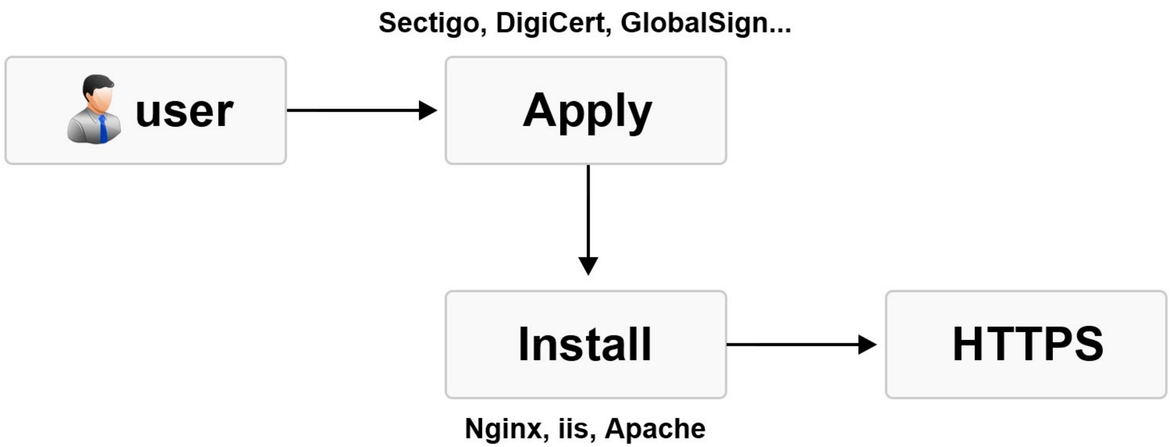
Solution: automatically configure a dual-algorithm SSL certificate to achieve HTTPS encryption

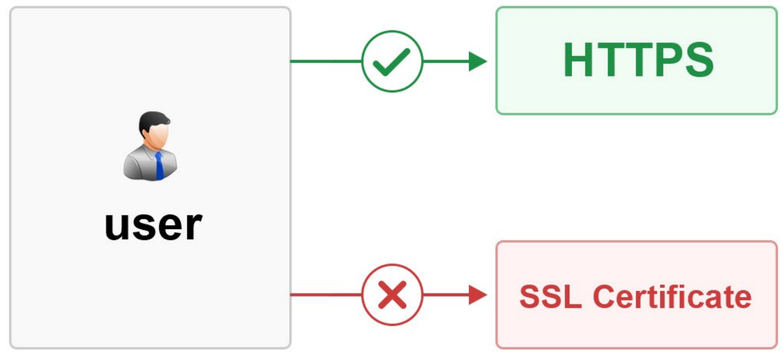
- The above three problems are the three big mountains that weigh on the Web server administrator, and there must be solutions to solve these problems.
- ZoTrus Technology has innovatively developed three solutions and related products to realize automatic application, deployment and renewal of dual-algorithm SSL certificates, fully automatic, zero reconstruction, and no need to care about the validity period of SSL certificates, completely and perfectly solving the above three problems and one big challenge.

2 Manually installing SSL certificate to implement HTTPS encryption is not what you need

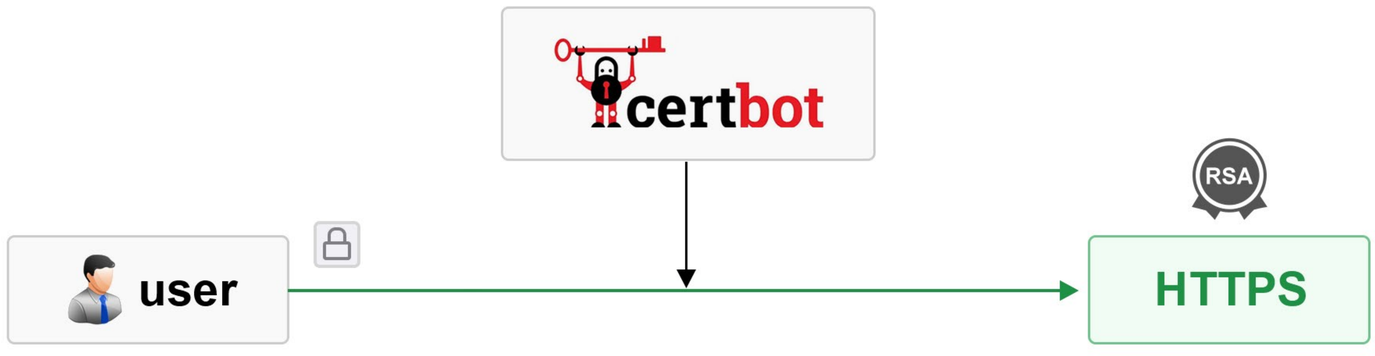
ZOTRUS

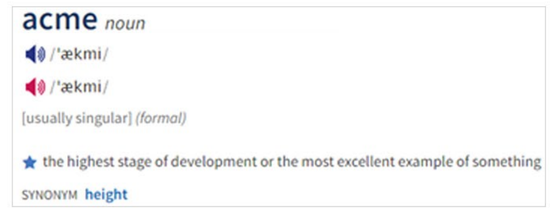
- What you need is HTTPS encryption, what they need is to eliminate the "insecure" warning of the browser, and what they need is China Cryptography Law compliance. Not an SSL certificate!
- We should provide HTTPS encryption solutions, not SSL certificates that users don't actually need!





3 ACME, the ultimate solution for HTTPS encryption





International Solution

ACME: Automatic Certificate Management Environment, RFC8555, give users the product they need - HTTPS encryption instead of SSL certificate! Let's Encrypt is a big success!

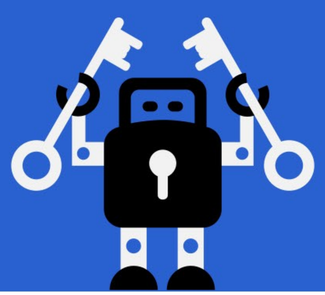
China Solution

SM2 ACME, the ultimate solution for SM2 HTTPS encryption

To popularize the application of SM2 SSL certificate,
there is also only one way - automate certificate management!

However, the ACME maybe is not a universal way,
it may not always available. And it does not support SM2 SSL certificates.

The web server software also does not support the SM2 algorithm!



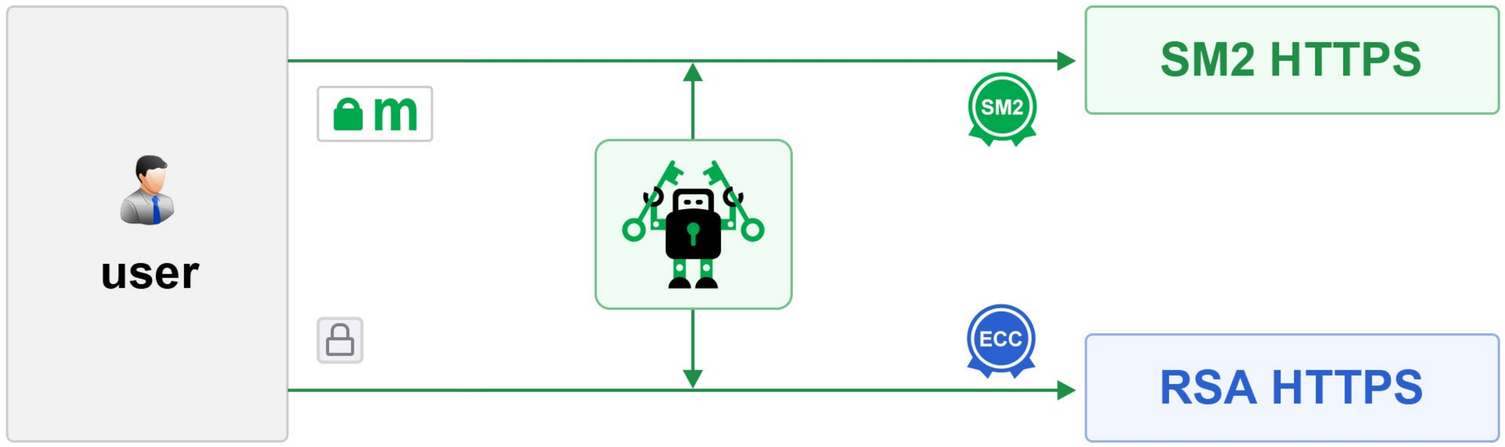
China solution is:

SM2 ACME = ACME + SM2 SSL Certificate + SM2 Algorithm Module

ZoTrus Technology strives to create the ultimate solution for SM2 https encryption!

China Solution

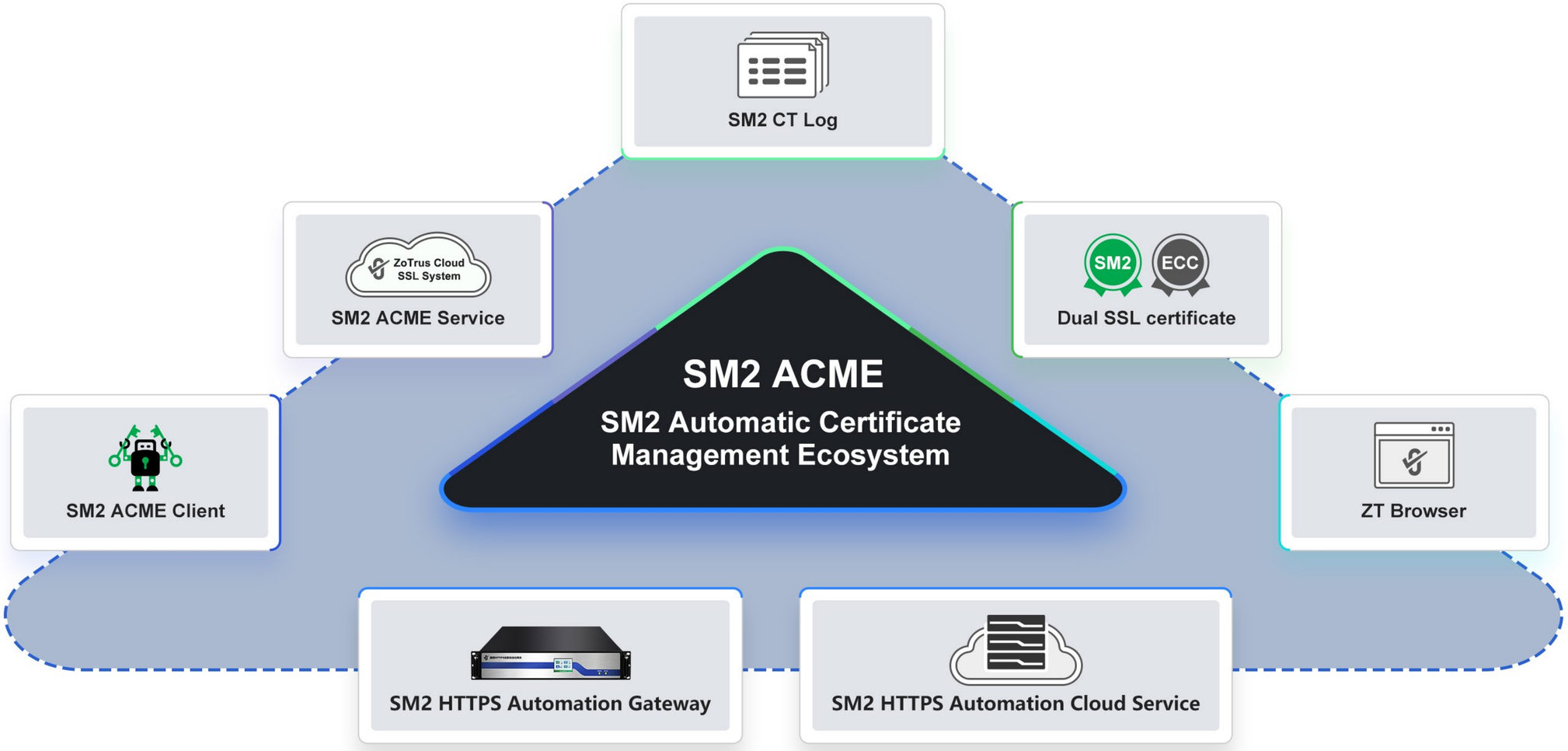
SM2 ACME, the ultimate solution for SM2 HTTPS encryption



RSA SSL Certificate

SM2 ACME = ACME + SM2 SSL Certificate + SM2 Algorithm Module

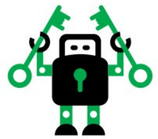
ZoTrus Technology has built an SM2 Automatic Certificate Management Ecosystem (SM2 ACME)



4 ZoTrus HTTPS automation three solutions, completely and perfectly solve the HTTPS challenges

Solution One:

Onetime installed, enabling ZoTrus SM2 ACME client - SM2cerBot



This solution is similar to the ACME client software: CertBot. The difference is that SM2cerBot automatically applies for, deploys and renews dual-algorithm SSL certificates, one 90-day valid ECC SSL certificate and one 90-day SM2 SSL certificate pair. And it comes with a SM2 algorithm support module, which automatically replaces the Nginx that does not support the SM2 SSL certificate with the new Nginx that supports the SM2 algorithm and SM2 SSL certificate, automatically implements https encryption, adaptive encryption algorithm.

The disadvantage of this solution is that the original Nginx server software needs to be uninstalled, which may have an impact on the business system, and is suitable for new website deployment to realize https encryption automation.

Solution Two:

Onetime deployment, enabling ZoTrus SM2 HTTPS Automation Gateway

This solution is suitable for the scenario where the original web server is running critical business system, and the server cannot be changed. The original web server is zero-reconstruction to realize SM2 https encryption that no need to apply and install SSL certificate. It only needs to deploy the HTTPS Automation Gateway and set the original website IP address to the gateway, the gateway implements https encryption, offloading and forwarding to the original website.

ZoTrus SM2 HTTPS Automation Gateway can automatically configure dual-algorithm SSL certificates for up to 255 websites for 5 years. The value of the SSL certificates alone is as high as 1.25 million RMB Yuan, and the value of the saving HR cost of engineers is as high as 1.5 million RMB Yuan, this is a really very valuable https encryption automation solution.

Solution Three:

Onetime setup, enabling ZoTrus SM2 HTTPS Automation Cloud Service

This solution is suitable for scenarios where ACME client software cannot be installed on the web server, and hardware gateway do not want to be purchased or cannot be deployed. This is a cloud service that can automatically apply for, deploy, and renew dual SSL certificates by doing only 3 domain name resolutions. The original web server is zero- reconstruction to realize SM2 https encryption.

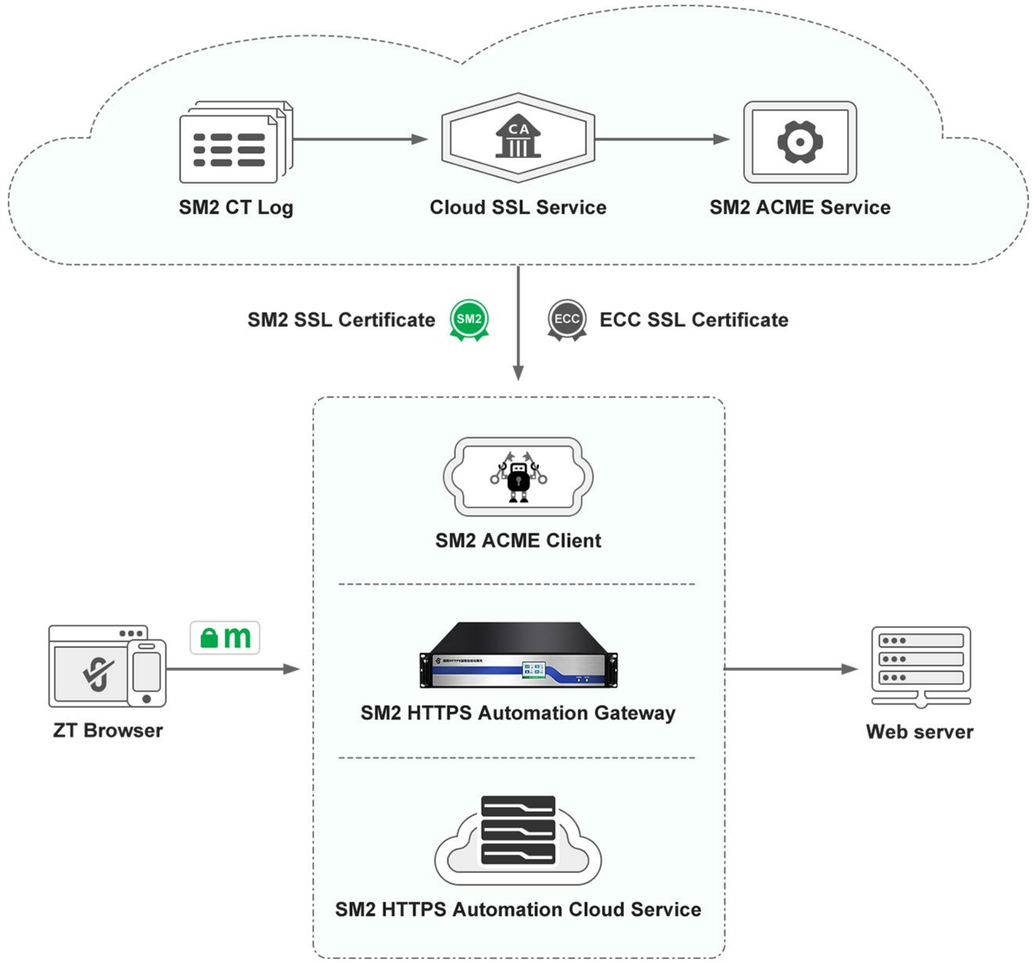
ZoTrus SM2 HTTPS Automation Cloud Service is a comprehensive website security protection solution based on the industry-leading Alibaba Cloud CDN/WAF service, which integrates HTTPS encryption automation, CDN high-speed distribution network, edge WAF protection, suitable for the security protection of a single website and the automatic implementation of https encryption.

Comparison table of the three solutions of ZoTrus HTTPS automation management

	Solution One ZoTrus SM2 ACME client	Solution Two ZoTrus SM2 HTTPS Automation Gateway	Solution Three ZoTrus SM2 HTTPS Automation Cloud Service
Onetime Operation	Install client software	Deploy hardware device	Do the domain resolution
Auto-apply for and deploy dual SSL certificates	90-day ECC DV SSL certificate 90-day SM2 DV SSL certificate	1-year ECC DV SSL certificate 1-year SM2 OV SSL certificate	1-year ECC DV SSL certificate 1-year SM2 OV/EV SSL certificate
Auto-renewal the dual SSL certificates	Yes, every 90 days	Yes, every 365 days	Yes, every 365 days
Number of supported sites	No limit	50/100/150/255 sites	1 site, optional multi-sites
Service Period	No limit	5 Years	1 Year, optional multi-year
Cost (RMB Yuan)	free	198K – 998K	4,888 – 98,888
Certificate types optional	Optional 1-year DV/OV/EV SSL certificate	Optional ECC OV/EV and SM2 EV	Optional ECC OV/EV SSL certificate
Zero-transformation of the original web server	No	Yes	Yes
Include WAF Protection	No	Yes	Yes
Include CDN service	No	No	Yes
Include WTIV service	No	Yes	Yes
Browsers Support	ECC SSL certificate: all browsers SM2 SSL certificate: ZT Browser	ECC SSL certificate: all browsers SM2 SSL certificate: all SM2 browsers	ECC SSL certificate: all browsers SM2 SSL certificate: all SM2 browsers
Application Scene	New website	There are multiple website systems that need to automatically deploy SSL certificates for independent management	One or few websites system need to automatically deploy SSL certificates without purchasing hardware
Disadvantages	Need to reinstall Nginx and install client software	None	Rely on cloud services

ZoTrus has built eight core products of SM2 HTTPS automatic management solution

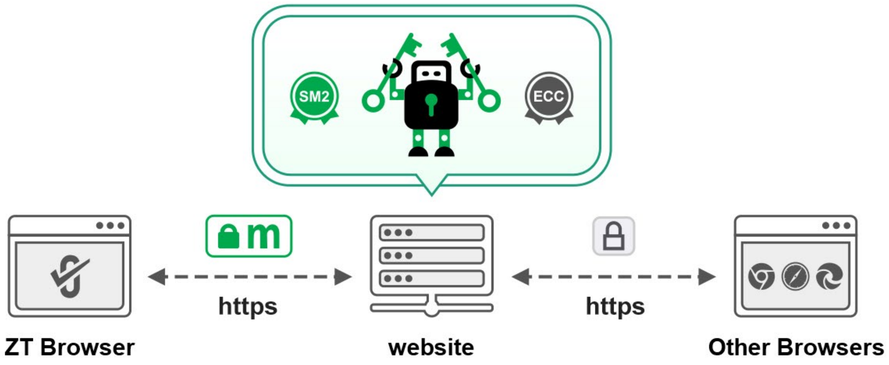
ZoTrus Technology has successfully built eight core products, including ZoTrus SM2 Certificate Transparency Log, ZoTrus Cloud SSL Service System, ZoTrus SM2 ACME Service System, ZoTrus SM2 SSL Certificate and RSA/ECC SSL Certificate, ZT Browser, ZoTrus SM2 ACME Client, ZoTrus SM2 HTTPS Automation Gateway and ZoTrus HTTPS Automation Cloud Service, providing related products and services, so that the user's website system and Internet of Things devices can fully automatically realize HTTPS encryption and adaptive cryptography algorithm(RSA/ECC/SM2), to meet the different users HTTPS application requirement for cryptography compliance and globally trusted.



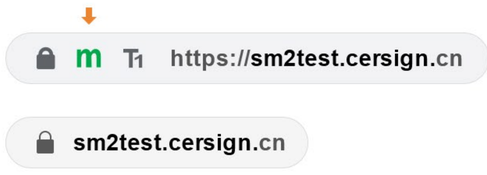
Solution 1

One-time installation, permanent and automatic implementation of SM2 HTTPS encryption

- Just install SM2cerBot on the server with one click
- Automatically apply for and deploy a 90-day SM2 DV SSL certificate
- Automatically apply for and deploy a 90-day ECC DV SSL certificate
- The dual certificate is automatically renewed upon expiration
- Dual-certificate deployment, adaptive HTTPS algorithm
- ZT Browser use SM2 algorithm for HTTPS, other browsers use ECC algorithm, to achieve China Cryptography Law compliance and global trust



Effect after implementation

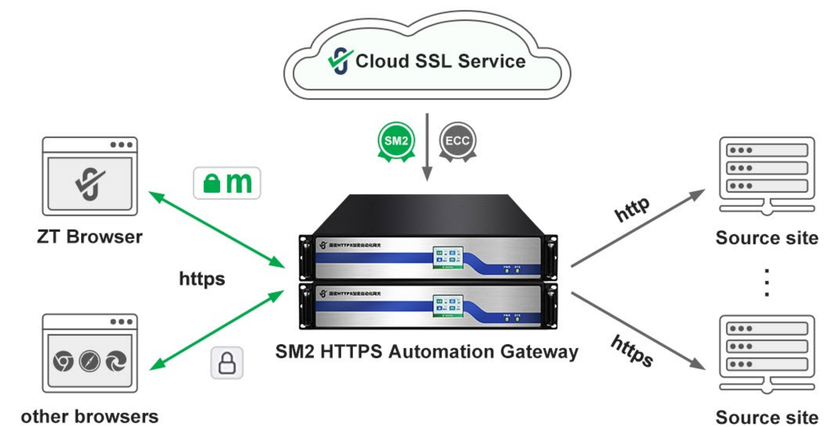


It can't meet the needs of the critical system servers that can't be changed, and it is only applicable to new websites!

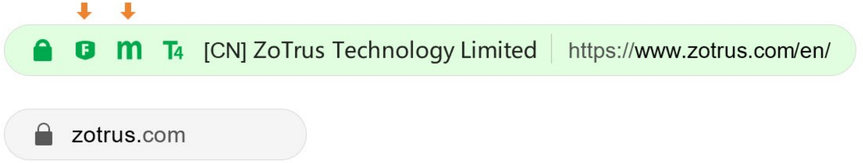
Solution 2

One-time deployment, automatic implementation of SM2 https encryption and WAF protection

- Only need to deploy a HTTPS Gateway for high-speed https
- encryption response and fast https offloading
- Zero modification of the original server
- Automatically apply for and deploy SM2 SSL certificates
- Automatically apply for and deploy ECC SSL certificates
- The dual certificate is automatically renewed upon expiration
- Dual-certificate deployment, adaptive HTTPS algorithm, WAF protection, and Website Trusted Identity Validation
- ZT Browser use SM2 algorithm for HTTPS, other browsers use ECC algorithm, to achieve China Cryptography Law compliance and global trust



Effect after implementation

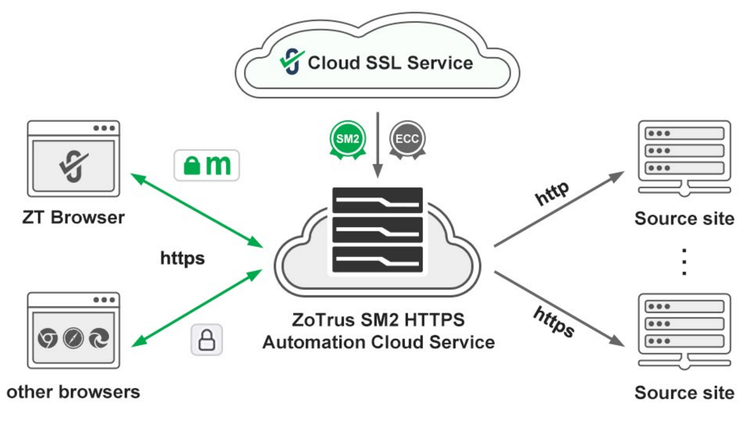


It can meet the needs of the critical system server that can't be changed, support up to 255 websites

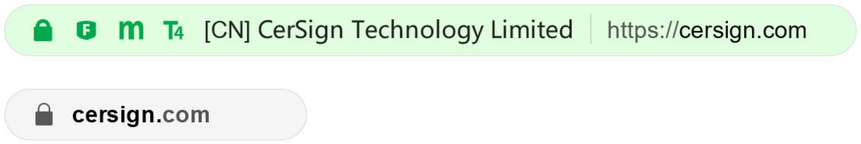
Solution 3

One-time set up, automatic implementation of SM2 https encryption and CND with WAF protection

- Only need to set up the domain name resolution once
- Zero modification of the original server
- Automatically apply for and deploy SM2 SSL certificates
- Automatically apply for and deploy ECC SSL certificates
- The dual certificate is automatically renewed upon expiration
- Dual-certificate deployment, adaptive HTTPS algorithm, CDN with WAF protection, and Website Trusted Identity Validation
- ZT Browser use SM2 algorithm for HTTPS, other browsers use ECC algorithm, to achieve China Cryptography Law compliance and global trust



Effect after implementation



It can meet the needs of the critical system servers that can't be changed, but it relies on third-party cloud service

5 ZoTrus SM2 HTTPS automation solution three supporting services

Supporting Service One:

Providing SM2 browser for free - ZT Browser

ZT Browser is a completely free SM2 browser that supports SM2 algorithms and SM2 SSL certificates and supports SM2 certificate transparency. Of course, it is also a standard general browser based on Google Chromium, it supports SM2 algorithm in the cipher suits, which realizes the automatic negotiation of cipher algorithm when the browser shakes hands with the Web server, and it supports RSA/ECC/SM2 three cipher algorithm suites and realizes the adaptive algorithm https encryption.

ZT Browser is the world's first to integrate a full-featured PDF reader, which not only seamlessly reads PDF documents, but also verifies the digital signature of the document in real time and displays the signer's trusted identity.

Supporting Service Two:

Issuing the dual-algorithm SSL certificates for free

ZoTrus Cloud SSL Service System provides free support for ZoTrus HTTPS automation solutions to provide automatic application and issuance of dual-algorithm SSL certificate services. Customers do not need to apply for SSL certificates from CA separately, and do not need to spend additional money to purchase SSL certificates. The three solutions all already include the dual-algorithm SSL certificates required for the service, the ECC/RSA SSL certificate is globally trusted and supports all browsers, the SM2 SSL certificate is cryptography compliant and supports all SM2 browsers.

What's particularly valuable is that the HTTPS Automation Gateway provides one ECC SSL certificate and two SM2 SSL certificate for up to 255 website domain names for 5 years, which is completely free and absolutely value-for-money.

Supporting Service Three:

Providing SM2 certificate transparency log service for free

In order to ensure the security of the SM2 SSL certificates issued for ZoTrus HTTPS automation solutions, ZoTrus provides SM2 certificate transparency log service for all SM2 SSL certificates. Every SM2 SSL certificate provided is like the ECC/RSA SSL certificates also have certificate transparency security protection, which effectively protect the legitimate rights and interests of customers and website security.

6 Authoritative Certifications and Customer Cases

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

Commercial Cryptography Product Certification Certificate

ZoTrus SM2 HTTPS Automation Gateway has passed the SSL VPN Product / Security Gateway class Security Level 2 Commercial Cryptography Product Certification. This is the first SM2 HTTPS Automation Gateway in China that has passed the certification, the effective date is Sept. 27, 2023.

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

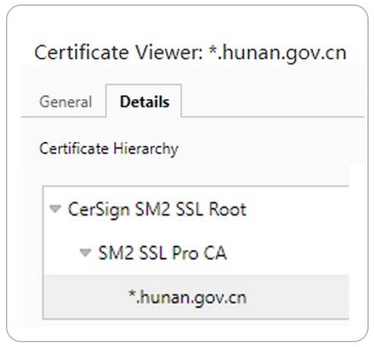
获奖项目：零信国密HTTPS加密自动化网关

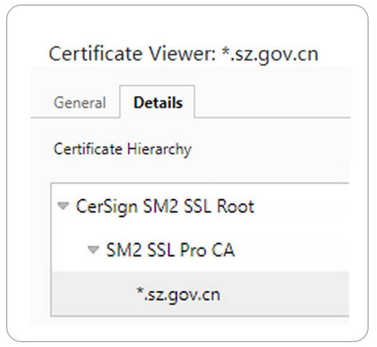
中国国际高新技术成果交易会组委会
二〇二三年十一月

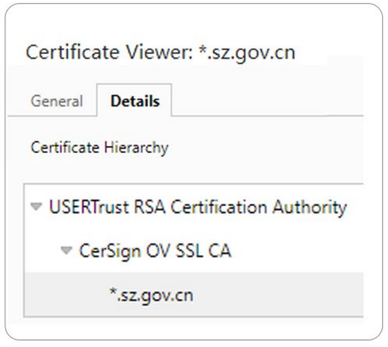
Excellent Product Award

ZoTrus SM2 HTTPS Automation Gateway won the "Excellent Product Award" issued by the Organizing Committee of the 25th (2023) China International Hi-Tech Fair

Customer Cases







Follow the draft China commercial cryptography standards of the “Automatic Certificate Management Specification” and the “Certificate Transparency Specification”

China Cryptography Standardization Technical Committee

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 ZoTrus Technology Limited

序号	项目名称	类型	时间安排	工作组
1	证书透明规范 Certificate Transparency Specification	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 Automatic Certificate Management Specification	制定	2025.12 完成 标准报批稿	基础 工作组

- ZoTrus Technology took the lead in formulating two commercial cryptography standards "Certificate Transparency Specification" and "Automatic Certificate Management Specification"
- ZT Browser and ZoTrus SM2 HTTPS Automation Gateway are the first to follow the two draft standards

Refer to reading

What is SM2 ACME? SM2 HTTPS ultimate Solution!

ACME realizes the automatic application and deployment of international SSL certificates, and SM2 ACME realizes the automatic application and deployment of dual SSL certificates of SM2 SSL certificate and ECC SSL certificate, and it also realizes the support of SM2 algorithm of web servers. It is the ultimate solution for HTTPS encryption!

Zero reconstruction for SM2 https encryption (II)

"Commercial Cryptography Reconstruction" takes time and effort, but it must be done! what to do? ZoTrus launched the SM2 HTTPS Gateway innovatively, built-in SM2 ACME client, realized the SM2 https encryption without any reconstruction! The acme solution, the first choice for e-government website Sm2 https encryption reconstruction!

SSL certificate automatic deployment, ensure uninterrupted https encryption of business system

The SM2 ACME Service is currently the only innovative cloud service that can automatically apply for and configure SM2 SSL certificate and ECC SSL certificate without interruption. This is the must choice for ensuring uninterrupted https encryption.

ZoTrus®

Welcome to ZoTrus HTTPS automation management solution,

Enjoy worry-free HTTPS encryption to automatically and continuously ensure the security of your business system!

customer service

Public Info

Contact us: +86755-26604080, WeChat: CerSignZoTrus, Email: help@zotrus.com