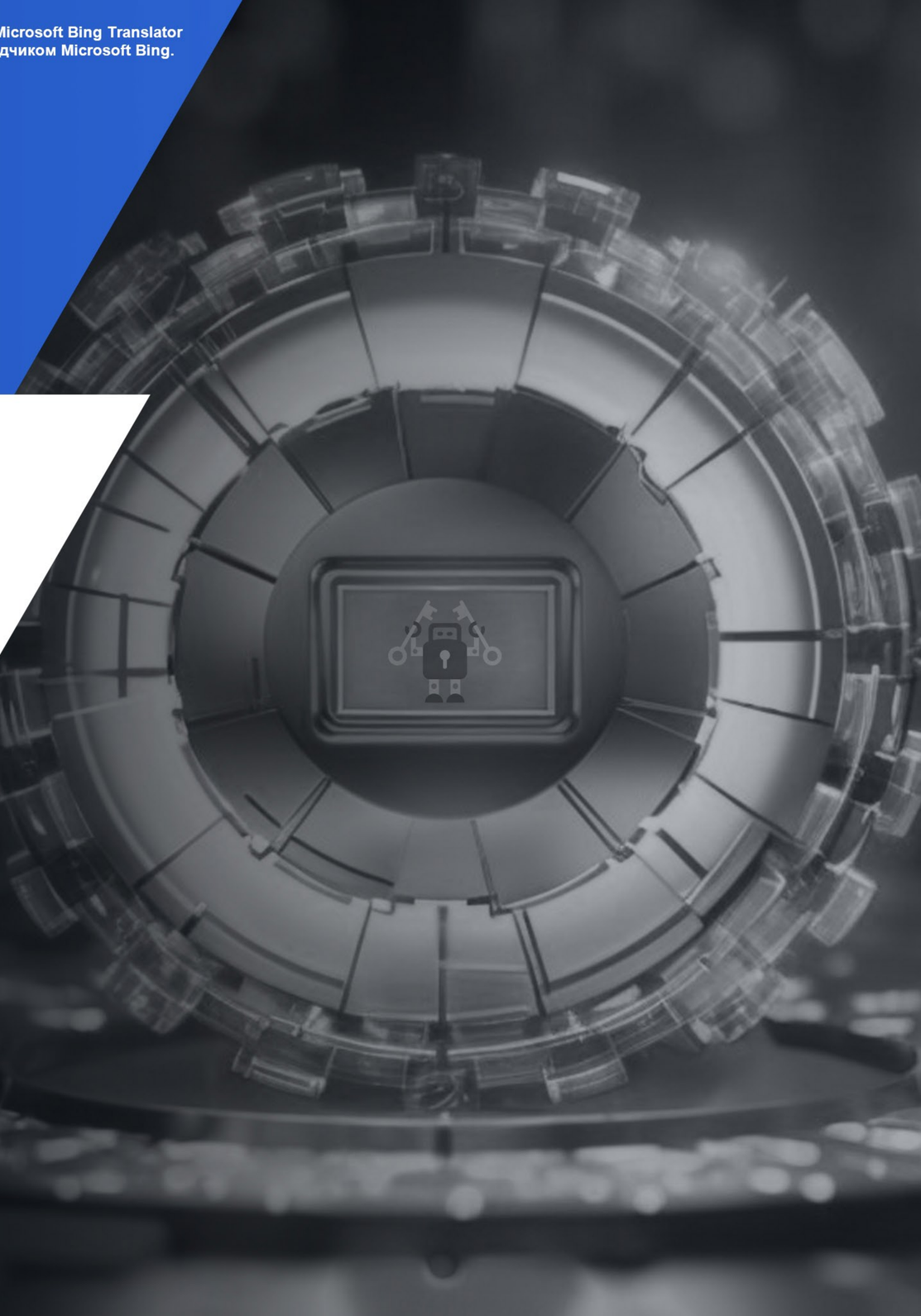
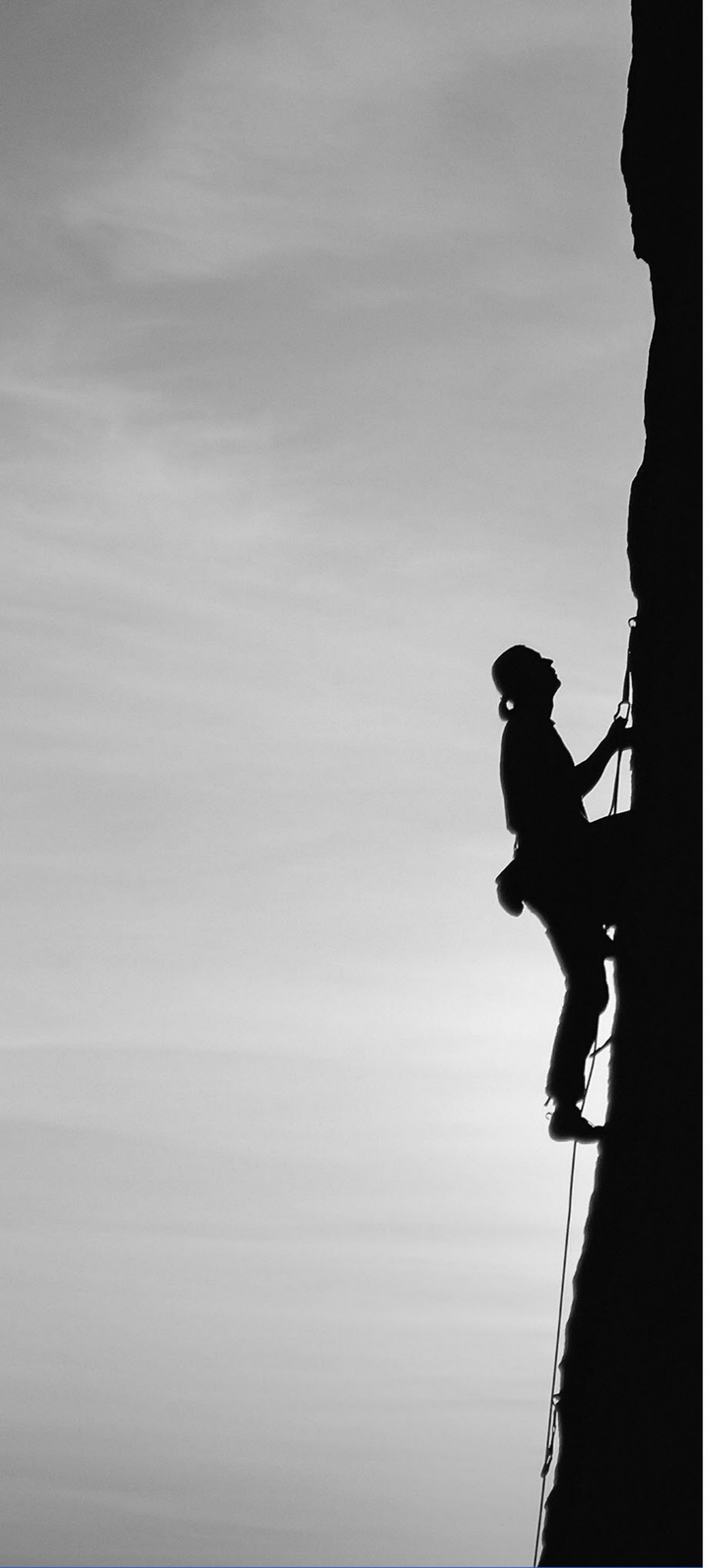
* This Russian version is translated from the English version by Microsoft Bing Translator
* Эта русская версия переведена с английской версии переводчиком Microsoft Bing.

ZoTrus®

Решение ZoTrus для управления автоматизацией HTTPS



ZoTrus Technology Limited
ЗоТрус Технолоджи Лимитед
2024.01

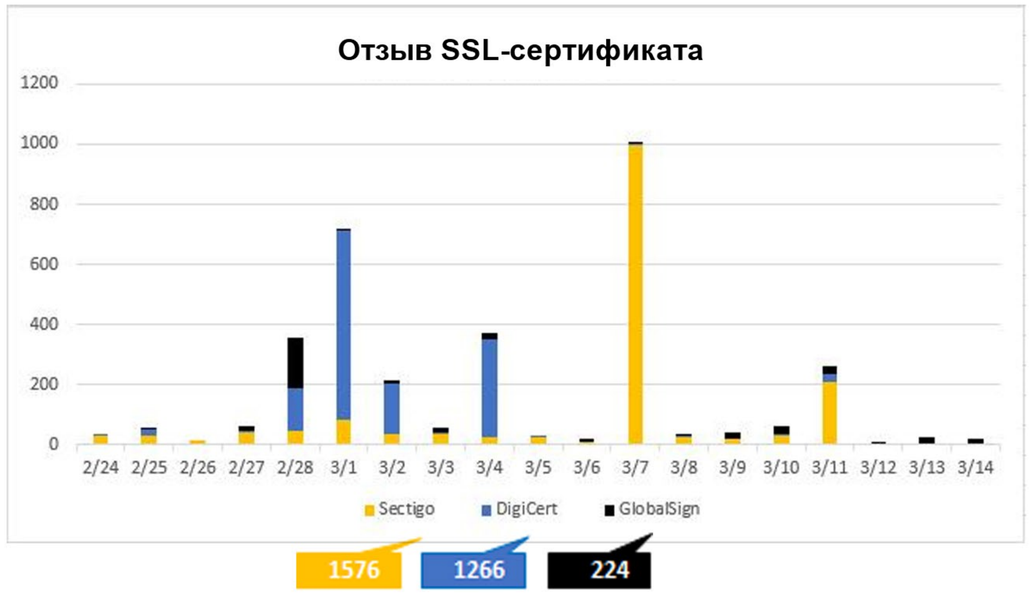


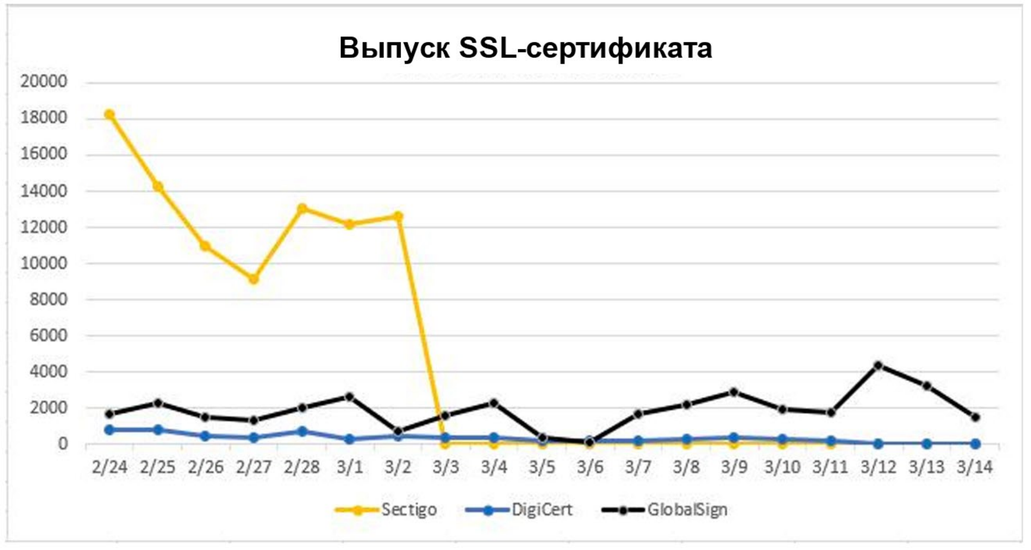
СОДЕРЖАНИЕ

ZOTRUS

1 Проблемы при внедрении шифрования HTTPS

Отзыв и прекращение предоставления SSL-сертификатов для домена .ru/.by/.su после российско-украинского конфликта (правительственные и банковские сайты)





Что это значит?

Глобальному Интернету нужна система, отличная от криптографической системы RSA для шифрования HTTPS, система SM2 - еще один выбор!

Еще 3 проблемы при внедрении шифрования HTTPS

Проблема первая:

Ручное развертывание SSL-сертификатов — невыполнимая задача.

Чтобы реализовать шифрование https, пользователь должен подать заявку на получение SSL-сертификата в ЦС, получить сертификат после завершения проверки удостоверения, а затем установить SSL-сертификат на веб-сервере, чтобы включить шифрование https. Этот процесс очень громоздкий, трудоемкий и трудоемкий. Для управления десятками тысяч веб-сайтов это большая рабочая нагрузка для ИТ-администраторов, они должны инвестировать больше персонала по эксплуатации и обслуживанию, чтобы реализовать шифрование https для нескольких веб-сайтов. В противном случае, как только срок действия SSL-сертификата системы истечет, и вы забудете продлить и повторно развернуть SSL-сертификат, это серьезно повлияет на нормальную работу бизнес-системы и приведет к неизмеримым убыткам.

Проблема вторая:

Реализовать шифрование SM2 https сложно.

Одним из требований соответствия Cyber Security Protection and Cryptography Security Protection является «безопасность сети и передачи данных», то есть шифрование веб-сервера по протоколу HTTPS, которое должно быть реализовано с помощью алгоритма SM2. Для этого необходимо, чтобы веб-сервер развернул SSL-сертификат SM2, пользователю необходимо подать заявку на получение SSL-сертификата SM2 в ЦС и развернуть его на веб-сервере по протоколу https.

Однако, чтобы включить SSL-сертификат SM2, необходимо не только установить SSL-сертификат, но и модифицировать веб-сервер для поддержки алгоритма SM2, а пользователи обязаны использовать браузер, поддерживающий алгоритм SM2 для реализации шифрования SM2 https. Но некоторые критически важные веб-серверы, используемые в настоящее время, не могут быть изменены, не могут повлиять на работающую бизнес-систему, а некоторые программы веб-серверов вообще не могут быть изменены.

Проблема третья:

Срок действия SSL-сертификата будет сокращен до 90 дней.

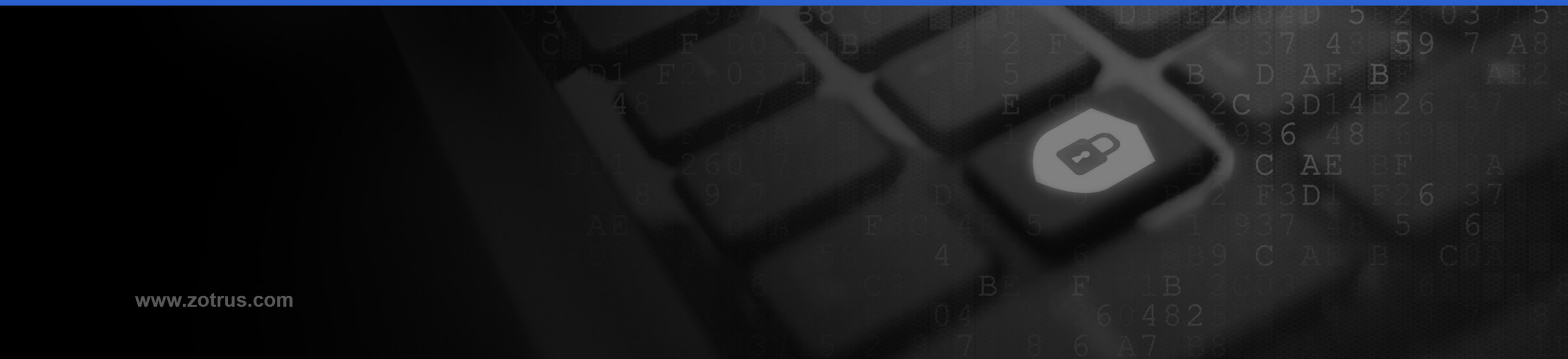
Это предстоящая проблема. Чтобы обеспечить безопасность шифрования https, Google продвигает сокращение срока действия SSL-сертификатов с текущего 1 года до 90 дней, с намерением сделать экосистему PKI гибкой, чтобы противостоять квантовым алгоритмам. Это значит, что первоначальная необходимость раз в год подавать заявку и разворачивать SSL-сертификат для сайта стала 5 раз в год, а огромная нагрузка на Problem One увеличилась в 5 раз! Это делает невозможным ручное применение и развертывание SSL-сертификатов!

Ожидается, что это революционное технологическое изменение произойдет в 2024 году, и все администраторы веб-сайтов должны заранее подготовиться к реализации автоматического управления SSL-сертификатами.

Решение: Автоматическая настройка SSL-сертификата с двойным алгоритмом для шифрования https

- Три вышеупомянутые проблемы - это три большие горы, которые тяготят администратора веб-сервера, и должны быть решения для решения этих проблем.

- ZoTrus Technology инновационно разработала три решения и сопутствующие продукты для реализации автоматического применения, развертывания и продления сертификатов SSL с двойным алгоритмом, полностью автоматических, с нулевой реконструкцией и без необходимости беспокоиться о сроке действия SSL-сертификатов, полностью и идеально решая вышеуказанные три проблемы и одну большую задачу.

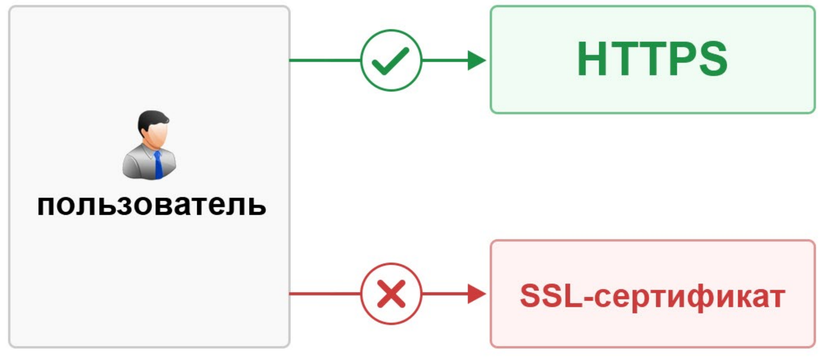


2 Ручная установка SSL-сертификата для реализации шифрования HTTPS — это не то, что вам нужно

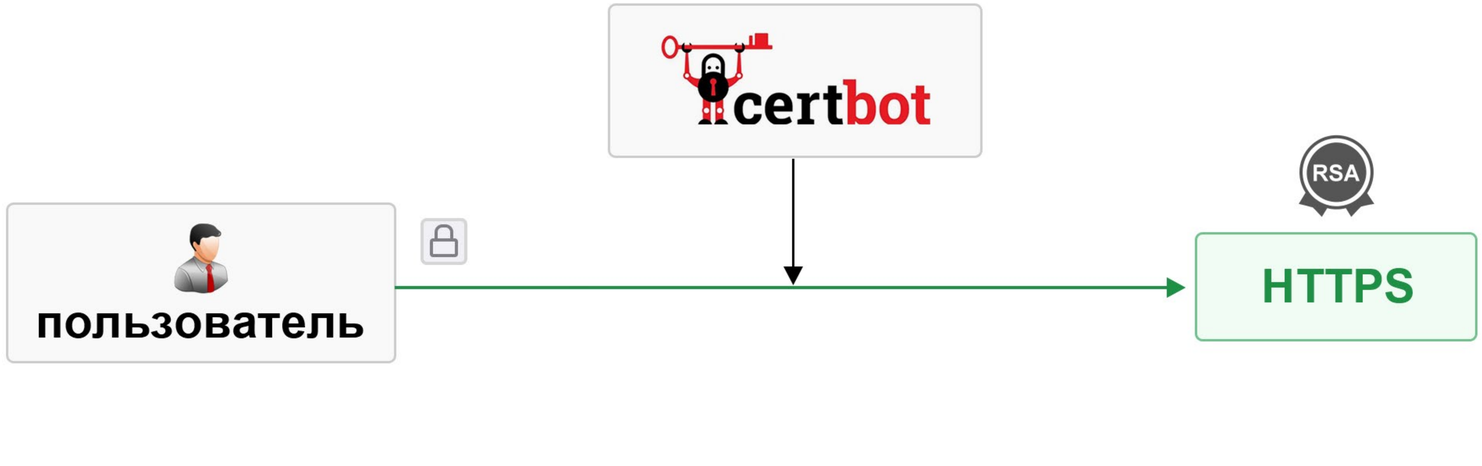
ZOTRUS

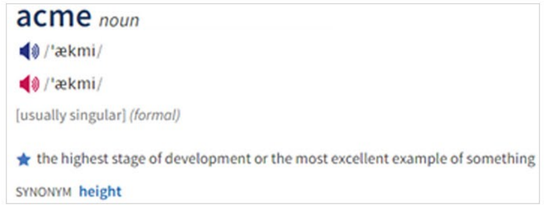
- Что вам нужно, так это шифрование https, что им нужно, так это устранить предупреждение «небезопасно» браузера, и что им нужно, так это соответствие Закону о криптографии Китая. Не SSL-сертификат!

- Мы должны предоставлять решения для шифрования https, а не SSL-сертификаты, которые на самом деле не нужны пользователям!



3 ACME, Решение acme для шифрования HTTPS





Международное решение

ACME: Automatic Certificate Management Environment, RFC8555, предоставить пользователям продукт, который им нужен - шифрование https вместо SSL-сертификата! Let's Encrypt пользуется большим успехом!

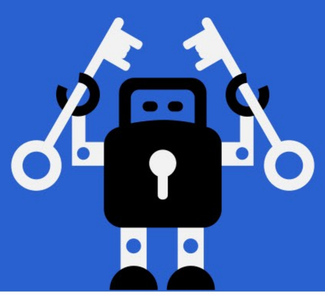
Китайское решение

SM2 ACME,
идеальное решение для шифрования SM2 HTTPS

Если мы хотим популяризировать применение SM2 SSL сертификата,
то также есть только один путь - автоматизировать управление сертификатами!

Тем не менее, ACME, возможно, не является универсальным способом,
он может быть не всегда доступен. И он не поддерживает SSL-сертификаты SM2.

Программное обеспечение веб-сервера также не поддерживает алгоритм SM2!



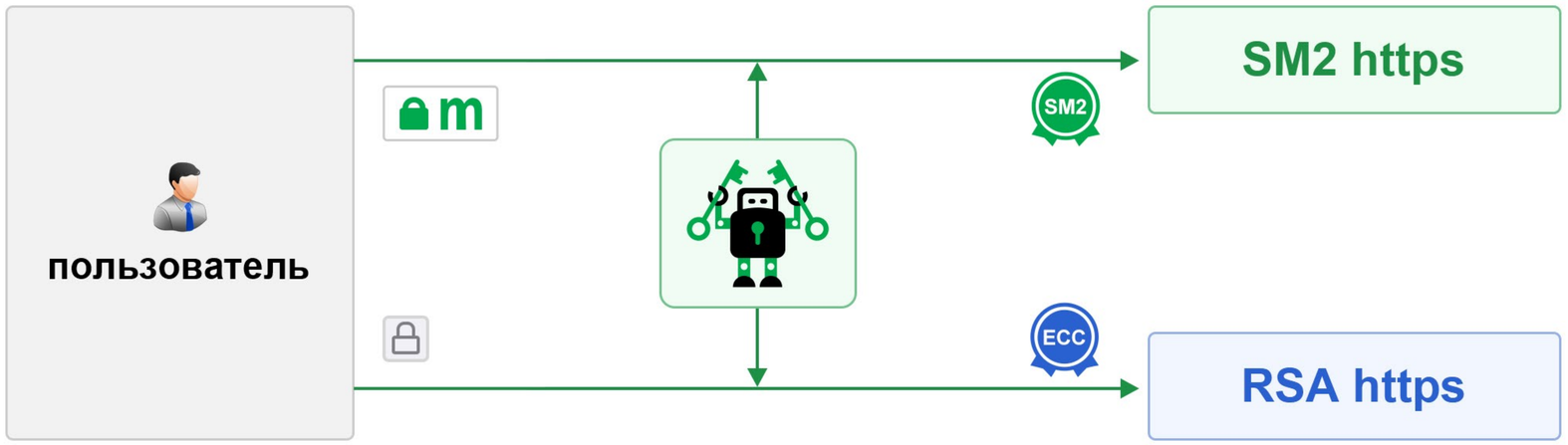
Китайское решение:

SM2 ACME = ACME + SSL-сертификат SM2 + модуль алгоритма SM2

ZoTrus Technology стремится создать идеальное решение для шифрования SM2 https!

Китайское решение

SM2 ACME,
идеальное решение для шифрования SM2 HTTPS



SSL-сертификат RSA

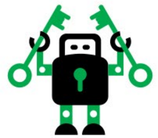
SM2 ACME = ACME + SSL-сертификат SM2 + модуль алгоритма SM2

Компания ZoTrus Technology построила экосистему автоматического управления сертификатами SM2 (SM2 ACME)

4 ZoTrus HTTPS автоматизация три решения, полностью и идеально решают проблемы HTTPS

Решение первое:

Однократная установка, включение клиента ZoTrus SM2 ACME - SM2cerBot



Это решение аналогично клиентскому программному обеспечению ACME: CertBot. Разница заключается в том, что SM2cerBot автоматически запрашивает, развертывает и обновляет SSL-сертификаты с двойным алгоритмом, один 90-дневный действительный сертификат ECC SSL и одну 90-дневную пару SSL-сертификатов SM2. И он поставляется с модулем поддержки алгоритма SM2, который автоматически заменяет Nginx, не поддерживающий SSL-сертификат SM2, на новый Nginx, который поддерживает алгоритм SM2 и SSL-сертификат SM2, автоматически реализует шифрование https.

Недостатком этого решения является то, что оригинальное серверное программное обеспечение Nginx необходимо удалить, что может повлиять на бизнес-систему, и подходит для развертывания нового веб-сайта для реализации автоматизации шифрования https.

Решение второе:

Одноразовое развертывание, включающее шлюз автоматизации ZoTrus SM2 HTTPS

Это решение подходит для сценария, когда на исходном веб-сервере работает критически важная бизнес-система, и сервер не может быть изменен. Исходный веб-сервер не требует реконструкции для реализации шифрования SM2 https, что не требует применения и установки SSL-сертификата. Ему нужно только развернуть шлюз автоматизации HTTPS и установить исходный IP-адрес веб-сайта на шлюз, шлюз реализует шифрование https, выгрузку и переадресацию на исходный веб-сайт.

ZoTrus SM2 HTTPS Automation Gateway может автоматически настраивать двухалгоритмические SSL-сертификаты для 255 веб-сайтов в течение 5 лет. Стоимость одних только SSL-сертификатов достигает 1,25 миллиона юаней, а стоимость экономии затрат на персонал инженеров достигает 1,5 миллиона юаней, это действительно очень ценное решение для автоматизации шифрования https.

Решение третье:

Одноразовая настройка, включающая облачный сервис SM2 HTTPS Облачный сервис автоматизации

Это решение подходит для сценариев, когда клиентское программное обеспечение ACME не может быть установлено на веб-сервере, а аппаратный шлюз не хочет приобретаться или не может быть развернут. Это облачная служба, которая может автоматически запрашивать, развертывать и продлевать двойные SSL-сертификаты, выполнив всего 3 разрешения доменных имен. Исходный веб-сервер является нулевой реконструкцией для реализации шифрования SM2 https.

ZoTrus SM2 HTTPS Automation Cloud Service - это комплексное решение для защиты безопасности веб-сайтов, основанное на ведущем в отрасли сервисе Alibaba Cloud CDN/WAF, которое объединяет автоматизацию шифрования HTTPS, высокоскоростную распределительную сеть CDN, защиту на границе WAF, подходит для защиты безопасности одного веб-сайта и автоматической реализации шифрования https.

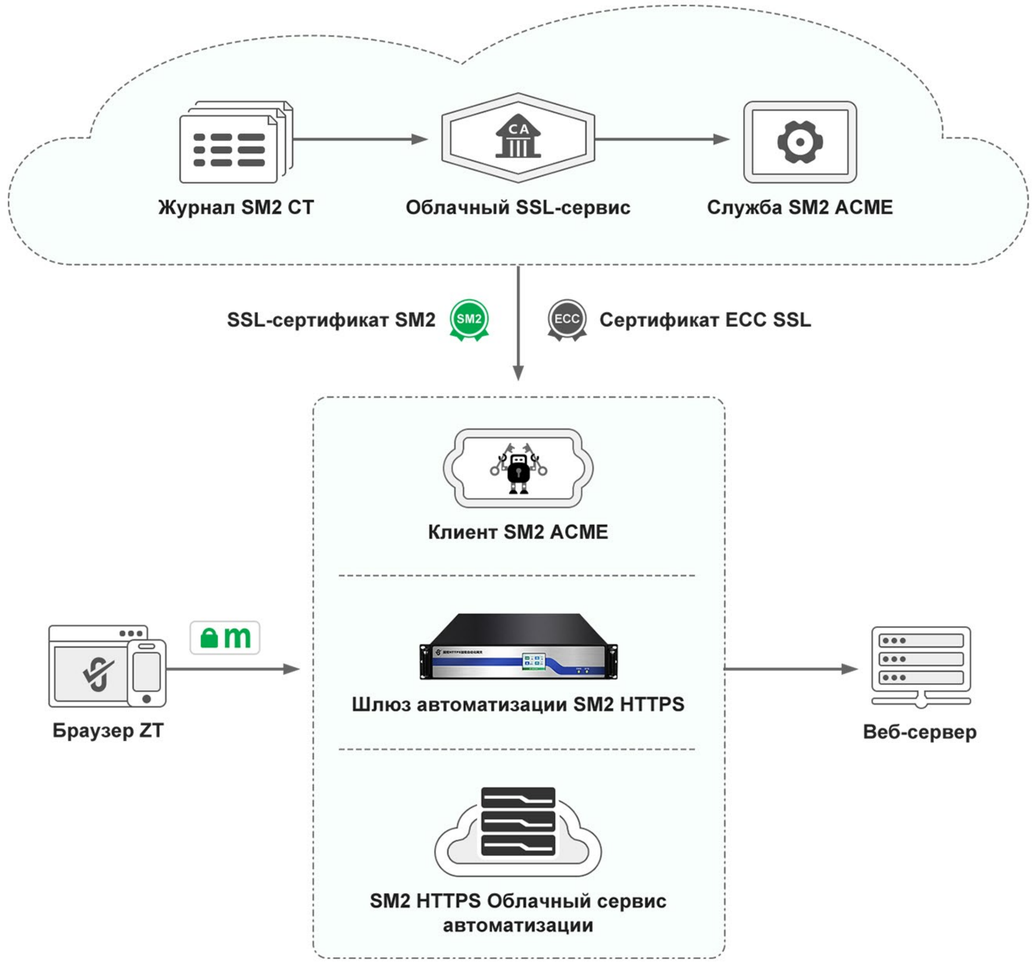
Сравнительная таблица трех решений ZoTrus по управлению автоматизацией HTTPS

	Решение первое Клиент ZoTrus SM2 ACME	**Решение второе** Шлюз автоматизации HTTPS ZoTrus SM2	**Решение третье** Облачный сервис автоматизации ZoTrus SM2 HTTPS
Разовая операция	Установка клиентского программного обеспечения	Развертывание аппаратного устройства	Разрешение домена
Автоматическая подача заявок и развертывание двойных SSL-сертификатов	Сертификат ECC DV SSL сроком на 90 дней	Сертификат ECC DV SSL сроком на 1 год	Сертификат ECC DV SSL сроком на 1 год
	SSL-сертификат SM2 DV сроком на 90 дней	SSL-сертификат SM2 OV сроком на 1 год	SSL-сертификат SM2 OV сроком на 1 год
Автоматическое продление двойных SSL-сертификатов	Да, каждые 90 дней	Да, каждые 365 дней	Да, каждые 365 дней
Количество поддерживаемых сайтов	Без ограничений	50/100/150/255 сайтов	1 сайт, опционально несколько сайтов
Период обслуживания	Без ограничений	5 лет	1 год, опционально несколько лет
Стоимость (юани)	свободный	198K – 998K	4,888 – 98,888
Типы сертификатов необязательны	Дополнительный сертификат DV/OV/EV SSL сроком на 1 год	Опционально ECC OV/EV и SM2 EV	Дополнительный сертификат ECC OV/EV SSL
Нулевая трансформация исходного веб-сервера	Нет	Да	Да
Включить защиту WAF	Нет	Да	Да
Подключить услугу CDN	Нет	Нет	Да
Включить услугу WTIV	Нет	Да	Да
Поддержка браузеров	SSL-сертификат ECC: все браузеры	SSL-сертификат ECC: все браузеры	SSL-сертификат ECC: все браузеры
	SSL-сертификат SM2: Браузер ZT	SSL-сертификат SM2: все браузеры SM2	SSL-сертификат SM2: все браузеры SM2
Прикладная сцена	Новый сайт	Существует несколько систем веб-сайтов, которым необходимо автоматически развертывать SSL-сертификаты для независимого управления	Система одного или нескольких веб-сайтов должна автоматически развертывать SSL-сертификаты без покупки оборудования
Недостатки	Нужно переустановить Nginx и установить клиентское программное обеспечение	Никакой	Положитесь на облачные сервисы

Компания ZoTrus создала восемь основных продуктов решения для автоматического управления SM2 HTTPS

Компания ZoTrus Technology успешно создала восемь основных продуктов, в том числе журнал прозрачности сертификатов ZoTrus SM2, облачную систему обслуживания SSL ZoTrus, сервисную систему ZoTrus SM2 ACME, сертификат SSL ZoTrus SM2 и сертификат RSA / ECC SSL, Браузер ZT, клиент ZoTrus SM2 ACME, шлюз автоматизации ZoTrus SM2 HTTPS и облачный сервис автоматизации ZoTrus HTTPS, предоставляющие сопутствующие продукты и услуги, чтобы система веб-сайта пользователя и устройства Интернета вещей могли полностью автоматически реализовывать HTTPS алгоритм шифрования и адаптивной криптографии (RSA/ECC/SM2), чтобы удовлетворить требования различных пользователей к приложениям HTTPS для соответствия криптографии и глобального доверия.

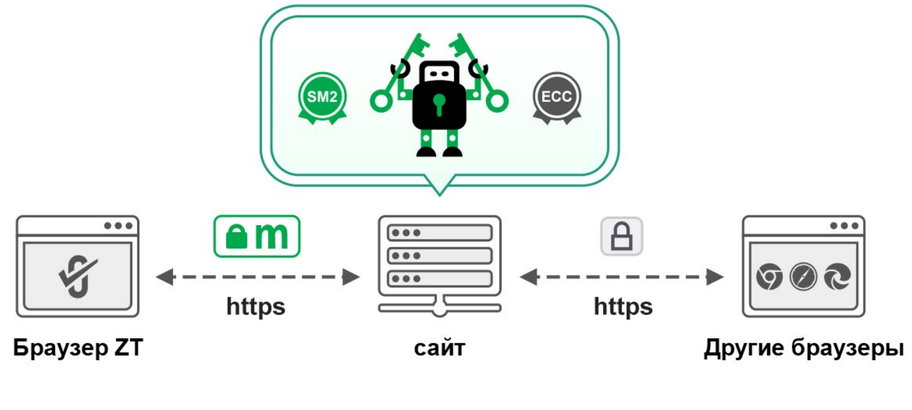
www.zotrus.com



Решение 1

Одноразовая установка, постоянное и автоматическое внедрение шифрования SM2 HTTPS

- Просто установите SM2cerBot на сервер в один клик
- Автоматическая подача заявки и развертывание 90-дневного SSL-сертификата SM2 DV
- Автоматическая подача заявки и развертывание 90-дневного сертификата ECC DV SSL
- Двойной сертификат автоматически продлевается по истечении срока действия
- Развертывание с двойным сертификатом, адаптивный алгоритм HTTPS
- Браузер ZT использует алгоритм SM2 для HTTPS, другие браузеры используют алгоритм ECC, чтобы обеспечить соответствие Закону о криптографии Китая и глобальное доверие



Эффект после внедрения

https://sm2test.cersign.cn

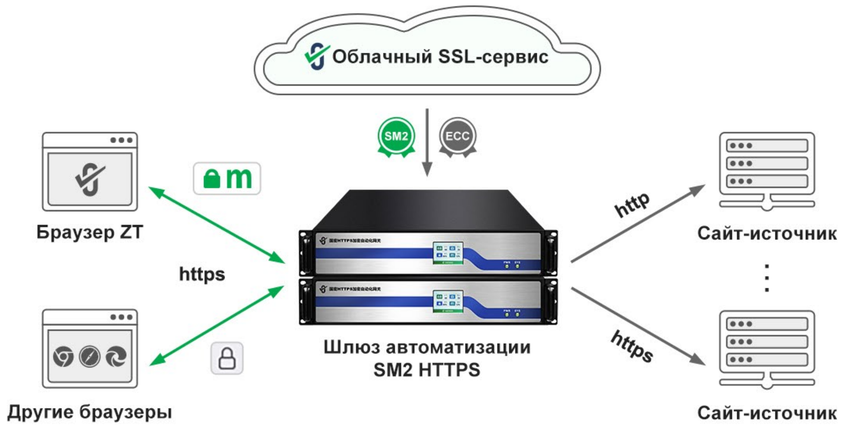
sm2test.cersign.cn

Он не может удовлетворить потребности критически важных системных серверов, которые не могут быть изменены, и применим только к новым веб-сайтам!

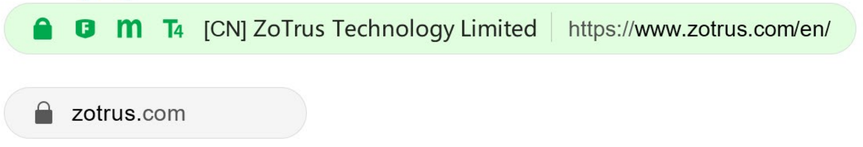
Решение 2

Одноразовая установка, постоянное и автоматическое внедрение шифрования SM2 HTTPS

- Нужно только развернуть шлюз HTTPS для высокоскоростного ответа шифрования https и быстрой разгрузки https
- Нулевая модификация оригинального сервера
- Автоматическая подача заявок и развертывание SSL-сертификатов SM2
- Автоматическая подача заявок и развертывание сертификатов ECC SSL
- Двойной сертификат автоматически продлевается по истечении срока действия
- Развертывание с двумя сертификатами, адаптивный алгоритм HTTPS, защита WAF и проверка доверенной идентификации веб-сайта
- Браузер ZT использует алгоритм SM2 для HTTPS, другие браузеры используют алгоритм ECC, чтобы обеспечить соответствие Закону о криптографии Китая и глобальное доверие



Эффект после внедрения



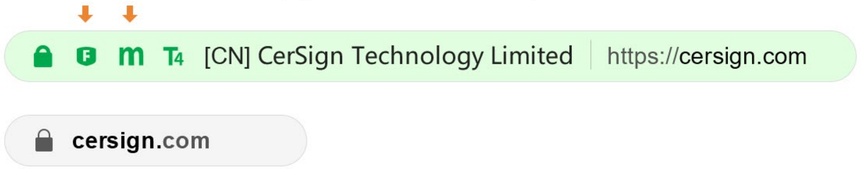
Он может удовлетворить потребности критически важного системного сервера, который не может быть изменен, поддерживать до 255 веб-сайтов

Решение 3

Одноразовая настройка, автоматическая реализация шифрования SM2 HTTPS и CND с защитой WAF

- Разрешение доменных имен нужно настроить только один раз
- Нулевая модификация оригинального сервера
- Автоматическая подача заявок и развертывание SSL-сертификатов SM2
- Автоматическая подача заявок и развертывание сертификатов ECC SSL
- Двойной сертификат автоматически продлевается по истечении срока действия
- Развертывание с двумя сертификатами, адаптивный алгоритм HTTPS, CDN с защитой WAF и проверка доверенной идентификации веб-сайта
- ZT Browser использует алгоритм SM2 для HTTPS, другие браузеры используют алгоритм ECC, чтобы обеспечить соответствие Закону о криптографии Китая и глобальное доверие

Эффект после внедрения



Он может удовлетворить потребности критически важных системных серверов, которые не могут быть изменены, но он полагается на сторонний облачный сервис

5 Решение для автоматизации ZoTrus SM2 HTTPS три вспомогательных сервиса

Первая вспомогательная служба:

Бесплатное предоставление браузера SM2 - Браузер ZT

Браузер ZT - это полностью бесплатный браузер SM2, который поддерживает алгоритмы SM2 и SSL-сертификаты SM2, а также поддерживает прозрачность сертификатов SM2. Конечно, это также стандартный общий браузер на основе Google Chromium, он поддерживает алгоритм SM2 в шифрах, который реализует автоматическое согласование алгоритма шифрования, когда браузер пожимает руку веб-серверу, а также он поддерживает три набора алгоритмов шифрования RSA/ECC/SM2 и реализует адаптивный алгоритм шифрования https.

Браузер ZT является первым в мире приложением, в которое интегрирована полнофункциональная программа для чтения PDF-файлов, которая не только беспрепятственно читает PDF-документы, но и проверяет цифровую подпись документа в режиме реального времени и отображает доверенную личность подписывающей стороны.

Вторая вспомогательная служба:

Бесплатная выдача SSL-сертификатов с двойным алгоритмом

Облачная система SSL-сервиса ZoTrus обеспечивает бесплатную поддержку решений по автоматизации ZoTrus HTTPS для обеспечения автоматического применения и выдачи услуг SSL-сертификатов с двойным алгоритмом. Клиентам не нужно отдельно подавать заявку на получение SSL-сертификатов в ЦС, и не нужно тратить дополнительные деньги на покупку SSL-сертификатов. Все три решения уже включают в себя SSL-сертификаты с двойным алгоритмом, необходимые для службы, SSL-сертификат ECC/RSA ЯВЛЯЕТСЯ глобально доверенным и поддерживает все браузеры, сертификат SM2 SSL совместим с криптографией и поддерживает все браузеры SM2.

Что особенно ценно, так это то, что Шлюз автоматизации HTTPS предоставляет один сертификат ECC SSL и два SSL-сертификата SM2 для 255 доменных имен веб-сайтов в течение 5 лет, что совершенно бесплатно и абсолютно выгодно.

Третья вспомогательная служба:

Бесплатное предоставление сервиса журнала прозрачности сертификата SM2

В целях обеспечения безопасности SSL-сертификатов SM2, выпущенных для решений по автоматизации ZoTrus HTTPS, ZoTrus предоставляет сервис журнала прозрачности сертификатов SM2 для всех SSL-сертификатов SM2. Каждый предоставленный SSL-сертификат SM2, как и SSL-сертификаты ECC/RSA, также имеют защиту прозрачности сертификатов, которая эффективно защищает законные права и интересы клиентов и безопасность веб-сайта.

6 Авторитетные сертификаты и кейсы клиентов

Сертификат сертификации коммерческой криптографической продукции

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 ZoTrus Technology Limited
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 Шлюз автоматизации HTTPS ZoTrus SM2
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

Шлюз автоматизации ZoTrus SM2 HTTPS прошел сертификацию SSL VPN Product / Security Gateway Class Security Level 2 Commercial Cryptography Product. Это первый шлюз Шлюз автоматизации SM2 HTTPS в Китае, прошедший сертификацию, дата вступления в силу - 27 сентября 2023 года.

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

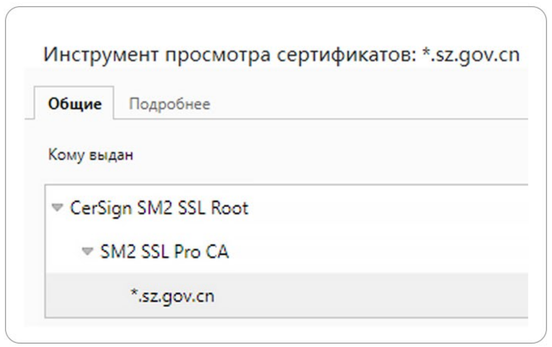
中国国际高新技术成果交易会组委会

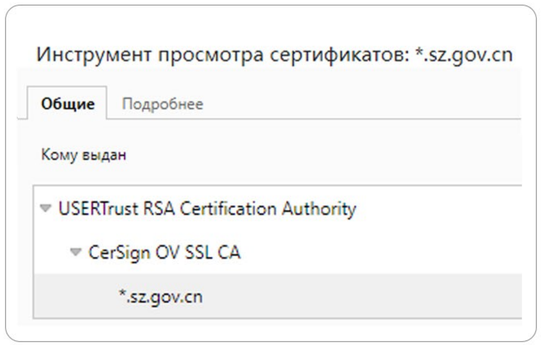
二〇二三年十一月

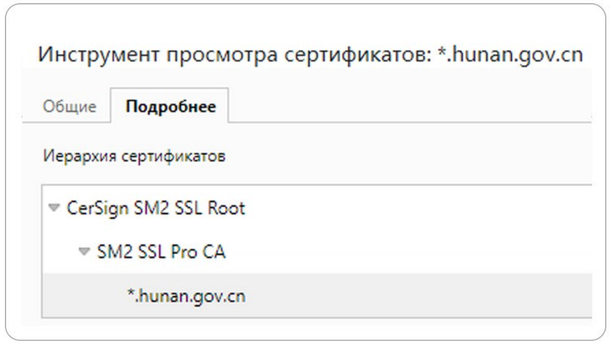
Шлюз автоматизации ZoTrus SM2 HTTPS получил награду «Отличный продукт», выданную Организационным комитетом 25-й (2023) Китайской международной выставки высоких технологий

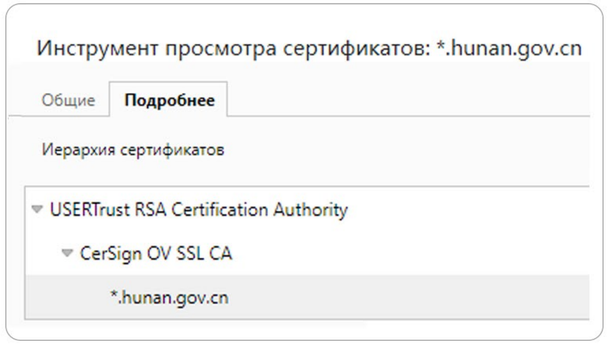
Кейсы клиентов

ZOTRUS









Следуйте проекту китайских стандартов коммерческой криптографии «Спецификация автоматического управления сертификатами» и «Спецификация прозрачности сертификатов»

Технический комитет по стандартизации криптографии Китая

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 Технолоджи Лимитед

序号	项目名称	类型	时间安排	工作组
1	证书透明规范 Спецификация прозрачности сертификатов	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 Спецификация автоматического управления сертификатами	制定	2025.12 完成 标准报批稿	基础 工作组

- Компания ZoTrus Technology взяла на себя ведущую роль в разработке двух коммерческих стандартов криптографии: «Спецификация прозрачности сертификатов» и «Спецификация автоматического управления сертификатами»
- Браузер ZT и Шлюз автоматизации HTTPS ZoTrus SM2 являются первыми, кто следует двум проектам стандартов

Обратиться к чтению

Что такое SM2 ACME? SM2 HTTPS идеальное решение!

ACME реализует автоматическое применение и развертывание международных SSL-сертификатов, а SM2 ACME реализует автоматическое применение и развертывание двойных SSL-сертификатов SM2 SSL-сертификата и ECC SSL-сертификата, а также реализует поддержку алгоритма SM2 веб-серверов. Это идеальное решение для шифрования HTTPS!

Нулевая реконструкция для шифрования SM2 https (II)

«Коммерческая криптографическая реконструкция» требует времени и сил, но это нужно сделать! Что делать? ZoTrus инновационно запустил SM2 HTTPS Gateway, встроил клиент SM2 ACME, реализовал шифрование SM2 https без какой-либо реконструкции! Решение acme, лучший выбор для восстановления шифрования https веб-сайта электронного правительства Sm2!

Автоматическое развертывание SSL-сертификата, обеспечивающее непрерывное шифрование https бизнес-системы

Сервис SM2 ACME в настоящее время является единственным инновационным облачным сервисом, который может автоматически запрашивать и настраивать SSL-сертификаты SM2 и ECC SSL-сертификаты без перебоев. Это обязательный выбор для обеспечения бесперебойного шифрования https.

ZoTrus®

Добро пожаловать в решение для управления автоматизацией ZoTrus HTTPS,

Наслаждайтесь беспроблемным шифрованием HTTPS для автоматического и непрерывного обеспечения безопасности вашей бизнес-системы!

customer service

Public Info

Свяжитесь с нами : +86755-26604080, WeChat: CerSignZoTrus, Email: help@zotrus.com