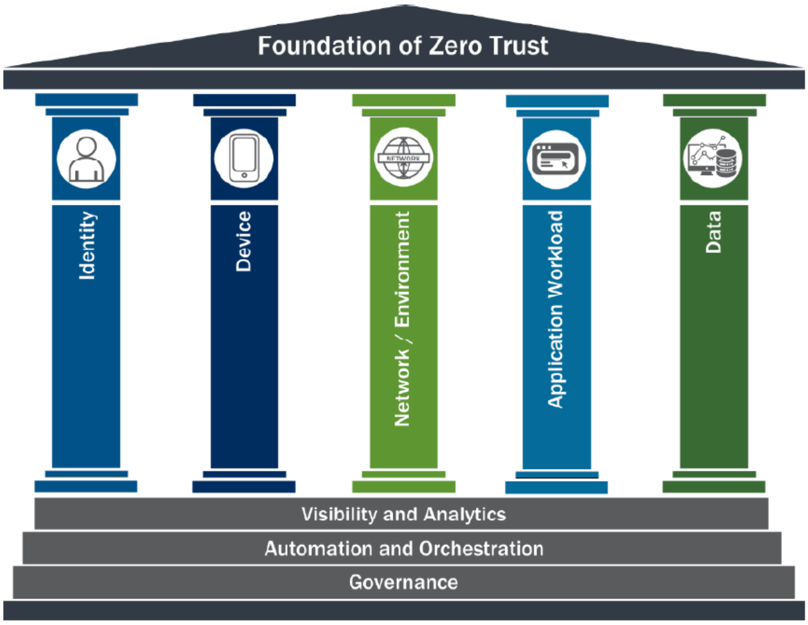
In-depth interpretation of the US Federal Zero Trust Strategy (1)

Since ZoTrus website officially launched ZT Browser and ZoTrus Website Security Cloud Service in June, it has been questioned by some customers and some zero trust security related providers, believing that the services provided by ZoTrus have nothing to do with zero trust security. The author believes that zero trust has been very hot in recent years, but only the traditional security vendors are all promoting it, and they are all "frying leftovers" based on their own traditional security products, which not only has no new ideas, but also misleads the market and customers. The author thinks it is necessary to write more articles to promote what is the true zero trust, although the author has already written some articles, including "Four Misunderstandings of Zero Trust Security", "What kind of Zero Trust do you need?" and "Zero trust implementation, where to start?".

This article will provide an in-depth interpretation of the Federal Zero Trust Strategy released by the U.S. Office of Management and Budget (OMB) on January 26, 2022. The strategy proposes five goals and action plans for zero trust security. Interpreting these goals and actions can help readers understand what zero trust really is. And the author also hopes to use this article to offer suggestions for China e-government system to move towards to zero trust principle and security architecture. Of course, it is not a complete copy, but a combination of China actual situation proposes a zero trust strategy road suitable for China conditions.

The function of the Office of Management and Budget (OMB) is to serve the President of the United States in overseeing the implementation of his or her vision across the Executive Branch. Its mission is to assist the President in meeting policy, budget, management, and regulatory objectives. The Federal Zero Trust Strategy was released to support Executive Order 14028 "Improving the National’s Cybersecurity" signed by the President of the United States to promote and implement the security architecture of U.S. federal agencies to be based on zero trust principles. The word "Zero Trust" is mentioned 11 times in this presidential order, which is rare and only shows that the US government takes zero trust seriously. Therefore, the Office of Management and Budget released this guidance document for the implementation of the federal zero trust strategy.

The goal of the Federal Zero Trust Strategy is to accelerate federal agencies' progress toward a security baseline of zero trust maturity as quickly as possible and requires that these strategic goals be achieved by the end of fiscal year 2024. These goals are organized using the zero trust maturity model developed by CISA (Cybersecurity and Infrastructure Security Agency). CISA's zero trust model describes five complementary areas of effort (pillars) (Identity, Devices, Networks, Applications and Workloads, and Data), with three themes that cut across these areas (Visibility and Analytics, Automation and Orchestration, and Governance).



The Federal Zero Trust Strategy states that a key tenet of zero trust architecture is that no network is implicitly considered trusted—a principle that may be at odds with some agencies' current approach to securing networks and associated systems. All traffic must be encrypted and authenticated as soon as practicable, this includes internal traffic, all data must be encrypted while in transit. This strategy focuses agencies on two critical and widely used protocols, DNS and HTTP traffic. In addition, will evaluate options for encrypting email in transit.

The goals of the Federal Zero Trust Strategy put forward specific action plans and requirements from five aspects: identity, devices, networks, applications and workloads, and data. This article focuses on the interpretation of the requirements for the Networks part, and the requirements for other aspects will continue to be in-depth interpretation in subsequent blog posts.

The Vision for the Networks part is:
Agencies encrypt all DNS requests and HTTP traffic within their environment and begin executing a plan to break down their perimeters into isolated environments.

The Actions for Networks part are:

(1) Agencies must resolve DNS queries using encrypted DNS wherever it is technically supported. CISA's Protective DNS program will support encrypted DNS requests.

(2) Agencies must enforce HTTPS for all web and application program interface (API) traffic in their environment. Agencies must work with CISA to "preload" their .gov domains into web browsers as only accessible over HTTPS.

(3) CISA will work with FedRAMP to evaluate viable Government-wide solutions for encrypted email in transit and to make resulting recommendations to OMB.

(4) Agencies must develop a zero trust architecture plan that describes the agency's approach to environmental isolation in consultation with CISA and submit it to OMB as part of their zero trust implementation plan.

The above content is organized according to the original document. The author believe that this is the most important content that other zero trust security providers will not mention. The author doesn't know if readers have noticed, the summary part of this strategy puts traffic encryption in a very important position. The words used are "key tenet", "focus", "critical". Please note that in the summary part of the Federal Zero Trust Strategy, identity access controls and traffic transmission encryption are at the top of the list, because if the user's identity traffic is not encrypted, it will lose the meaning of "always verify". Never talk about zero trust that only identity authentication is left! For this point, please refer to blog "Four Misunderstandings of Zero Trust Security", the author will not repeat such content in this article.

In the following, the author will focus on the interpretation and summary of the following four points based on his own expertise in cryptography.

First, HTTPS encryption must be enforced on all federal agency's websites, which is the focus and key principle of Zero Trust.

Requires that all federal agency websites must implement https encryption, which is zero trust to http websites with cleartext transmission, this is the first principle of zero trust architecture, and all web traffic must be encrypted. Moreover, it is required that HSTS technology must be used to realize that the browser can only access with https encryption. This is never trusting the http websites will automatically jump to https encryption, and the browser will enforce https connection. This is also a zero trust to agencies whether they can strictly enforce https encryption. These two points are very worthy of China e-government website to learn and learn from.

According to CNNIC statistics, as of December 2021, there are 14,566 government websites in China, and only 4,251 SSL certificates have been applied for the .gov.cn domain names found from the Google Certificate Transparency Log System, and certificates in the case of duplicated application are not excluded. The application rate is only 29%, indicating that most government websites have not yet deployed SSL certificates to implement https encryption. Among the 31 provincial government portal websites, only 19 provinces have implemented https encryption. However, even if some websites have deployed SSL certificates, they are not automatically enforced to https encryption.

Second, China government websites must enforce the SM2 https encryption, which is the focus and key principle of China zero trust strategy, and it is also a compliance requirement of the "Cryptography Law".

For government websites in China, even deploying an SSL certificate to implement https encryption is not enough. The author doesn't know if readers know that after the Russian-Ukrainian conflict, international CA operators have revoked the SSL certificates that have been issued to Russian government websites and bank websites. In just a few days, more than 3,000 certificates have been revoked, causing many government websites and bank websites to fail to function properly. In the current very uncertain international environment, how should China avoid such website security incidents? There is only one answer, that is China government websites and bank websites must all enforce the deployment of SM2 SSL certificates as soon as possible. This is zero trust to RSA algorithm

SSL certificates, and this is also a compliance requirement of the "Cryptography Law", because the "Cryptography Law" explicitly requires that critical information infrastructure must use China Commercial Cryptography to achieve encryption protection.

For better user experience, the website cannot force users to use which browser, the best temporarily solution is the website must deploy dual algorithm (SM2/RSA) dual SSL certificate to achieve adaptive https encryption, to ensure that browsers and mobile Apps that do not support SM2 algorithms can also function normally. Not only that, but also it is necessary to vigorously promote and popularize the use of SM2 browsers that support SM2 algorithms and SM2 SSL certificates, and vigorously promote and enforce the requirement that commonly used mobile Apps must support SM2 HTTPS encryption. Only in this way can we avoid serious security incidents like Russia's website SSL certificate revocation and supply broken. Once users are accustomed to using the SM2 browser to surf the Internet, even someday the RSA algorithm SSL certificate is revoked, it will not affect the user's normal Internet access because the RSA SSL certificate is not really in function.

The author is very happy to see that many government websites have deployed the SM2 SSL certificate to realize the SM2 https encryption, and he personal online banking system of Bank of China has also deployed SM2 SSL certificate to realize SM2 https encrypted online banking transaction data. These websites all deployed dual SSL certificates, which implement https encryption with adaptive encryption algorithm. Once the RSA certificate is revoked, users who do not use the SM2 browser only need to switch to the SM2 browser, which will not affect the normal encryption operation of the website at all. We hope that all China government websites and bank websites can speed up the deployment of the SM2 SSL certificate, which has effectively protected the security of China e-government system and online banking system.

Third, DNS encryption must be taken very seriously, this is zero trust to cleartext DNS.

The Federal Zero Trust Strategy requires that all federal agencies must use encrypted DNS to resolve DNS queries, which is also worth learning. From the relevant search results, DNS encryption has not been taken seriously in China. First, the ISP operators that provide Internet services have not implemented encrypted DNS Internet access by default, and government agencies have no mandatory requirements in this regard. This is worthy of high attention for related departments.

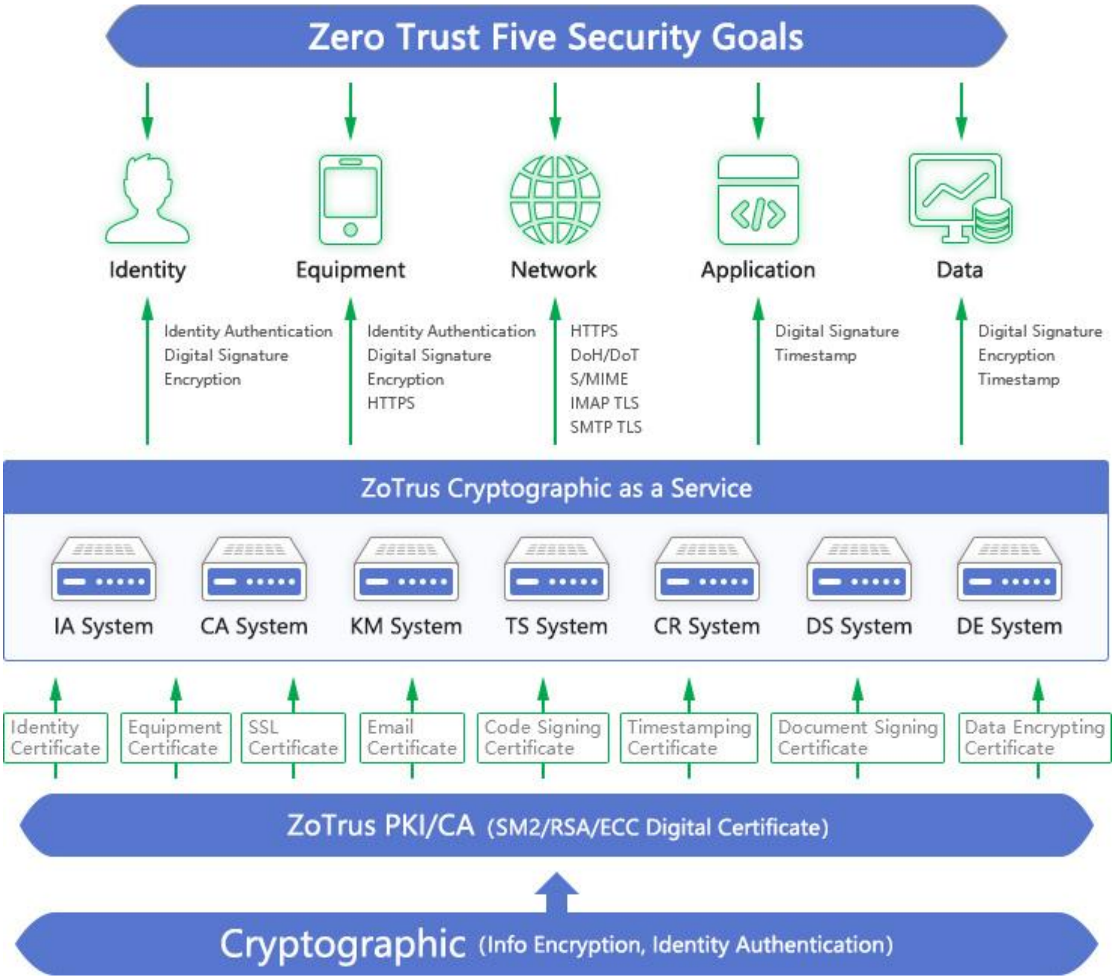
The requirement to use encrypted DNS is zero trust to cleartext DNS, to protect the security of critical data on the Internet and effectively prevent DNS spoofing attacks. The two main technologies for realizing encrypted DNS, DNS over TLS and DNS over HTTPS, are also inseparable from SSL certificate. It is expected that DNS encryption can be implemented and popularized by adopting the SM2 SSL certificate as soon as possible in China.

Fourth, email encryption must be taken seriously, which is zero trust to cleartext emails.

For email encryption, although the Federal Zero Trust Strategy does not provide a solution at present, but email encryption solution is evaluating. Compared with the popularization of email office in west countries, email office is not widely used in China. However, it is worth noting that some province e-government email systems do not deploy SSL certificates, which is also very insecure. It must be deployed as soon as possible to ensure the security of web login accounts and email transmission. Of course, it is recommended to deploy a SM2 SSL certificate. The author will write a separate blog to talk about the topic of email encryption in detail that we are developing an email security cloud service, a cloud service that innovatively solves the problem of email encryption.

The above is the author's in-depth interpretation of the Network part of the five aspects in the US Federal Zero Trust Strategy. Why should the author interpret this part first? Because the content of this part has been seriously ignored in China, Because the "major" zero trust security providers in China don't mention and promote this part since they are not familiar with this field. The author understands why the US Federal Zero Trust Strategy puts the encryption of web traffic in such an important position, the reason is that the web data must be secure, then the user’s identity authentication is meaningful. Otherwise, the web data and user data will be insecure, then lost the meaning of "always verify" user identity. Understanding this is critical to a proper understanding of Zero Trust.

To sum up, the five goals of Zero Trust are identity trust, device trust, traffic encryption, application trust and data encryption. These five goals can be achieved through the digital signature and encryption of digital certificate, its core base technology is cryptography and PKI/CA technology.



The mission of ZoTrus Technology is to "provide innovative cryptographic products and services to protect the security of identities, devices, networks, applications, and data", which is a product line based on zero trust principals that 100% conforms to the Federal Zero Trust Strategy. ZoTrus Technology adopts cryptographic technology and zero trust principles to provide website security cloud service, email security cloud service, application security cloud service, document security cloud service and identity trusted cloud service. ZoTrus Technology is a zero trust security provider based on cryptographic technology.

Richard Wang

Sept. 9, 2022
In Shenzhen, China