Create an Intranet SSL Certificate Application Ecosystem

The CerSign intranet SSL certificate was officially launched today. It took nearly a year from the planned development of the intranet SSL certificate in May last year to the launch of the intranet SSL certificate today. Everyone will be curious, why does it take so long? Because this is creating an intranet SSL certificate ecosystem that is unprecedented in the world, and it is not just about simply issuing an SSL certificate. This article explains in detail how ZoTrus Technology builds this ecosystem.

1. The security problem of intranet HTTP traffic is very serious.

The status of intranet HTTP traffic is that either clear text HTTP streaking or deploying a self-signed certificate that all browsers do not trust. In both cases, all browsers will prompt "Not secure". One ZT Browser user has deployed an SSL certificate that the browser does not trust on the intranet and asked us how to eliminate this Not-secure warning. We told the user to manually install and trust the root CA certificate that issued the intranet SSL certificate. The result is that it still doesn’t work, we told the user to send us the SSL certificate deployed on their system. Only after looking, we can understand why there is still a security warning even if the root CA certificate is manually trusted. Because this SSL certificate has the following security problems:

(1) The public key of the certificate is RSA 1024 bits, which is very insecure! International standards require that the issuance of 1024-bit SSL certificates be stopped on December 31, 2010, and 1024-bit certificates be disabled on December 31, 2013. But such an important intranet system is still using 1024-bit RSA algorithm SSL certificates thirteen years later!

(2) The certificate signature algorithm is SHA-1, which is very insecure! International standards require that the issuance of SHA-1 certificates be stopped on December 31, 2015. But such an important intranet system is stilling using SHA-1 certificate seven years later!

(3) The certificate does not have a Subject Alternative Name (SAN) field, only the CN field = IP address of 10.142.xx.xx. This is a big problem because the browser verifies that the domain name or IP address bound to the SSL certificate in SAN field. Without this field, it is impossible to determine whether the IP address bound to the certificate is consistent with the IP address of the

website the user is visiting. Of course, there will be a "Not secure" warning.

(4) The SSL certificate does not have the enhanced key usage (EKU) of "server authentication and client authentication", so it must not be able to achieve two-way authentication.

(5) The certificate does not have a required key usage (Critical), which is also a very serious problem.

(6) The certificate has no certificate policy field and no certificate transparency SCT list.

(7) The certificate does not have an accessible revocation list URL and Authorization Information Access (AIA) URL. Anyway, the internal network cannot access the external network, which is acceptable.

(8) This SSL certificate is used on the intranet and is bound to the intranet IP address 10.142.xx.xx. This is not a problem. However, this SSL certificate has expired for more than a year and is still in use. This is a big problem.

This SSL certificate has so many serious security problems, but it is still in use in a very important intranet management system, the user asked: some browser can be used normally, why can ZT Browser not be used normally? Our customer service team was asked, I had to ask how I should answer the user's question, I was also speechless for a while, thinking that this some browser that can be used "normally" can still be called a "browser"? The SSL certificate deployed by the website has so many insecure problems, this browser can still be accessed normally? It can be seen that this some browser is also trying to adapt to the user's application environment, and there is no security bottom line at all, which is actually harming users!

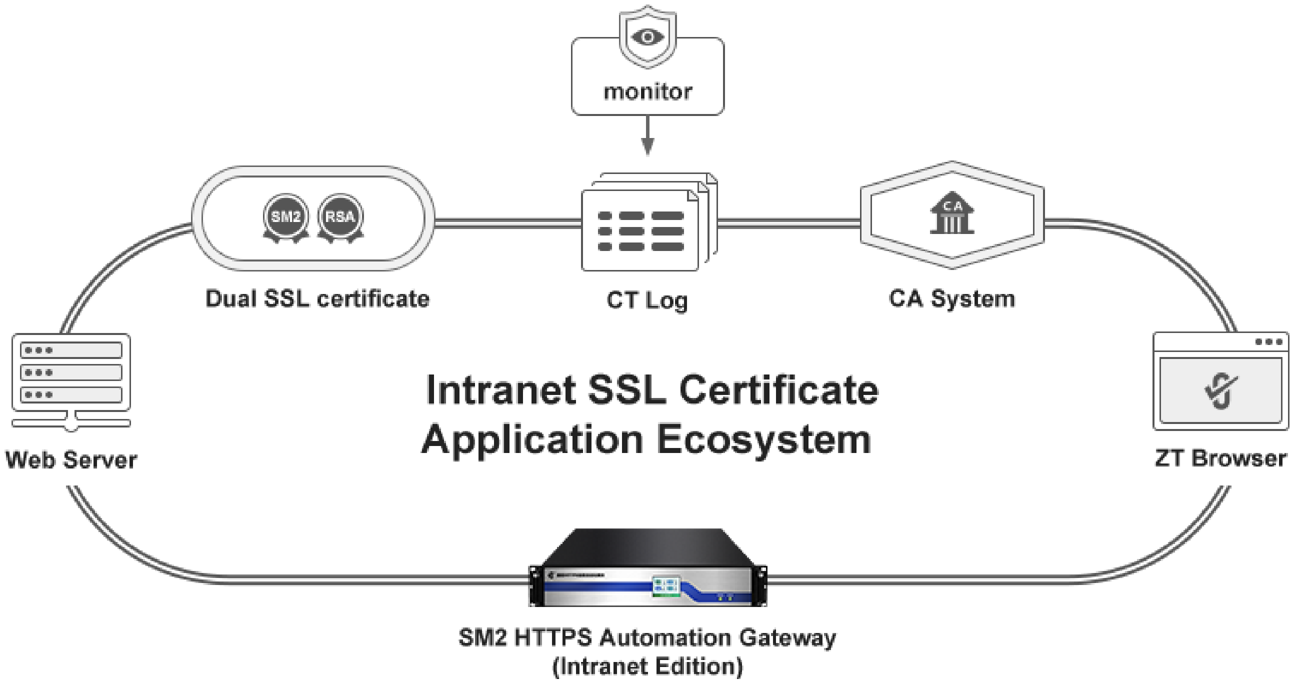
Maybe the user is also helpless, because the SSL certificate with so many serious security problems is issued by a CA, and some users may have more security problems with the SSL certificate signed by themselves, that even use the RSA 512-bit key and MD5 signed certificate. This touched the author's decision to provide intranet SSL certificate for users, we must be anxious for the users, we must solve the users' problem, to provide intranet SSL certificate for users with reference to the international standard for RSA algorithm intranet SSL certificate and national standard for SM2 algorithm intranet SSL certificate, the only difference can only be to support the private IP address and internal name, other technical parameters must follow the relevant international standards and national cryptography standards.

2. ZoTrus create an application ecosystem for intranet SSL certificates.

As you can see, the generation date of the root CA certificate of the internal SSL certificate is June 6, 2023, that is, it has been decided to issue an intranet SSL certificate for users since May last year. Not only does the CA system need to be able to issue an intranet SSL certificate, but it also needs to be trusted by the browser and be able to verify the intranet SSL certificate, and the intranet SSL certificate also needs to support certificate transparency. This only solves the problem of the supply of intranet SSL certificates, and intranet SSL certificates also need to be deployed automatically, because some intranet web servers that have been used for many years may not support or are inconvenient to install SSL certificates, but the intranet cannot be connected to the Internet, and the same client-cloud integrated solution as public SSL certificate automation cannot be used.

When you see these works, you should be able to understand why it took us almost a year to launch an intranet SSL certificate. Not only have we successfully built all the products required for the application ecology of intranet SSL certificates, but we have also opened this ecosystem to global CAs and launched the ZT Browser Intranet SSL Certificate Trusted Root Program, so that global CAs can issue intranet SSL certificates for global users according to the intranet SSL certificate baseline requirements we have formulated, and jointly solve the security problems of intranet web traffic for global users.

The application ecosystem of intranet SSL certificate created by ZoTrus Technology involves CA system, dual SSL certificates (SM2 algorithm SSL certificate and RSA algorithm SSL certificate), certificate transparency log system, ZT Browser, and ZoTrus SM2 HTTPS Automation Gateway (Intranet Edition), the international standards do not allow CAs to issue SSL certificates bound to private IP addresses, because these private IP addresses can be used by anyone, it is impossible to verify that they have legal control, which is the problem of the entire intranet SSL certificate application ecosystem.


monitor
Dual SSL certificate
SM2
RSA
CT Log
CA System
CA
Web Server
Intranet SSL Certificate Application Ecosystem
ZT Browser
SM2 HTTPS Automation Gateway (Intranet Edition)

Since the international standard does not allow the issuance of intranet SSL certificates by public trusted root CA certificates, we must have a root CA certificate dedicated to issuing intranet SSL certificates, and we have generated the intranet RSA CA root certificate and SM2 root CA certificate key (Root Key Ceremony) with reference to international standards and national cryptography standards, and issued intranet DV/OV/EV SSL sub-CA certificate from these root CA certificates, RSA root certificate uses 2048-bit public key instead of 4096-bit, mainly considering that some intranet server system may be very old and does not support 4096-bit, 2048-bit can already ensure the security of the key. The user certificate adopts the 2048-bit public key and SHA-256 signature that conform to international standards, and the other certificate fields are of course in line with international standards. Both SM2 root CA certificate and user certificate adopt SM2 algorithm, and each certificate field refers to international standards.

The first challenge is how to verify the private IP address and internal name, which has no precedent in the world. We must study and explore a viable solution. After repeated research and testing, we have come up with a feasible solution: the SSL certificate CN field must be bound to a public domain name, and this domain name must complete domain name control verification in accordance with international standards, including designated administrator email validation, CNAME domain name validation and web file validation, and complete the validation of the common name domain, so that users can add the private IP address and internal name in the SAN field that do not need to be validated, but as long as there are public domain names and public IP addresses in the SAN field, they need to be validated in accordance with international standards. The purpose of the CN field requirement to bind a public domain name is to confirm who the intranet SSL certificate belongs to and who has the right to own this intranet SSL certificate. Of course, it is recommended that users apply for an OV/EV intranet SSL certificate and lock the organization name in the O field of the certificate subject, which can better prove that the binding of an unverifiable private IP address or intranet hostname is used by a certain organization to ensure the security and trust of the private SSL certificate.

The validation of the intranet SSL certificate has been solved, and second issue is the certificate transparency support. Since 2013, every globally trusted RSA/ECC algorithm SSL certificate has supported certificate transparency, should intranet SSL certificates also support it? The answer is of course it should be. However, how to support certificate transparency is another difficult problem in front of us, because we only have the SM2 algorithm certificate transparency log system, and it only supports SM2 algorithm SSL certificates, and the intranet SSL certificate is also a dual algorithm SSL certificates, an RSA algorithm SSL certificate and an SM2 algorithm SSL certificate. After research and experiments, we finally chose to continue to use the ZoTrus SM2 Certificate Transparency Log System to provide certificate transparency services for both the intranet SM2 algorithm SSL certificate and the intranet RSA algorithm SSL certificate, so that each intranet SSL certificate is submitted to the ZoTrus SM2 Certificate Transparency Log System to achieve certificate transparency, which is the world's first to realize the RSA algorithm SSL certificate submitted to the SM2 certificate transparency log system to obtain the SM2 algorithm SCT data, and embedded it in the intranet SSL certificate, realizing the full transparency of the issuance of dual SSL certificates.

This leads to the third problem that needs to be solved, there must be one browser that trust intranet SSL certificates, including RSA algorithm SSL certificates and SM2 algorithm SSL certificates, and there must be one browser that can verify the SM2 transparency log data embedded in the intranet SSL certificate. ZT Browser undertakes this task, not only included and trust the intranet SSL root certificate, but also takes the lead in the world to realize the SM2 SCT data validation for the RSA algorithm SSL certificate, which is another technological innovation.

In other words, ZoTrus Technology is the first in the world to realize the SM2 certificate transparency log system supporting SM2 algorithm, RSA algorithm and ECC algorithm SSL certificate, and the current signature key of the international certificate transparency log system is to use the ECC algorithm to sign SCT data, and only supports the SSL certificate issued by the RSA algorithm and the ECC algorithm. ZoTrus Technology makes each intranet SSL certificate as transparency as the public SSL certificate, effectively ensuring the security and trustworthiness of the intranet SSL certificate.

The fourth problem is the automation of intranet SSL certificates, because the intranet cannot be connected to the Internet, it is impossible to use the ACME technology solution for publicly trusted SSL certificates, and the only feasible solution is to deploy a gateway on the intranet, and the gateway can realize the self-sufficiency of the intranet SSL certificate, automatic deployment and automatic implementation of HTTPS encryption, and it is also adaptive encryption algorithm, ZT Browser that supports the SM2 algorithm uses the SM2 algorithm to achieve HTTPS encryption, and other browsers that do not support the SM2 algorithm use RSA algorithm to achieve HTTPS encryption. The intranet edition of ZoTrus SM2 HTTPS Automation Gateway is still under development and internal testing, which is the only product in the intranet SSL certificate application ecosystem that is still under development.

3. Intranet SSL certificate application ecosystem, ensure the security of intranet Web traffic.

Intranet SSL certificates are required for the security of intranet web traffic, but this is not a simple matter of issuing an SSL certificate, but to create an ecosystem. On the basis of the successful creation of the SM2 certificate transparency ecosystem and the SM2 certificate automation management ecosystem, ZoTrus Technology has successfully created the third ecosystem - the Intranet SSL Certificate Application Ecosystem, where users can purchase the intranet SSL certificate with a validity period of 1-5 years on the CerSign official website and buy the SSL certificate within the 5-year period, and the user will get a dual algorithm SSL certificate with a validity period of 5 years, so as to achieve one installation and HTTPS encryption security for intranet web traffic within 5 years. Intranet SSL certificates support up to 1000 intranet IPs, intranet hostnames, internal names, public IPs and public domain names, all of which are dual-algorithm (RSA/SM2) SSL certificates, and both algorithm SSL certificates support SM2 certificate transparency.

Another important product of the intranet SSL certificate application ecosystem is ZT Browser, which trusts the CerSign intranet SSL certificates, and preferentially uses the SM2 algorithm to achieve HTTPS encryption. Once ZT Browser is installed, other browsers also trust the CerSign RSA algorithm intranet SSL certificate, and users can still use these browsers to implement the RSA algorithm HTTPS encryption to access the intranet Web system.

Welcome to apply the CerSign intranet SSL certificates, there are completely free 90-day dual SSL certificates and paid 1-5 years SSL certificate validity period SSL certificates. Welcome to use the completely free SM2 browser - ZT Browser, to effectively ensure the security of intranet web traffic and the security of confidential information of important information systems in the intranet.

Richard Wang

April 22, 2024
In Shenzhen, China