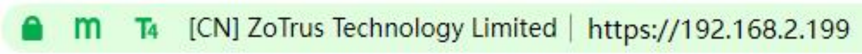
Intranet SSL Certificate is the Must for Intranet Web Security

The intranet is the internal network of the organization, but in fact, many large organizations are already a cross-city WAN, at least a large area network of a park and a building, or an internal LAN of the same building and a floor. These large organizations mostly are the important critical information infrastructure operation organizations, and there are a large number of internal office confidential information on the intranet web server, which is transmitted in HTTP plaintext, and it is very easy to be illegally used in office computers, floor switches or cross-building switches to steal all confidential information. The implementation of HTTPS encryption for intranet traffic must be put on the agenda as soon as possible. The USA Federal Zero Trust Strategy clearly requires that all intranet HTTP traffic must be encrypted with HTTPS, which is very worthy of reference.

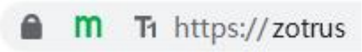
However, an SSL certificate is required to implement HTTPS encryption for intranet traffic, and according to international standards, CAs are strictly required NOT to issue SSL certificates for reserved IP addresses because they can be used by anyone and cannot be validated by CAs. CA is also not allowed to issue SSL certificates to non-FQDN domain names or hostnames, which makes it impossible for the intranet Web system to apply for a globally trusted SSL certificate. So, the common solution is to deploy the self-signed certificate, but the browser will have insecure warning to self-signed certificate, and if the intranet user clicks to trust, it is very easy to encounter malicious attacks of fake website certificates because of the inertia of certificate warnings. So, the solution is to install the root CA certificate of the self-signed certificate to the intranet user's computer. All of these are technical obstacles to the implementation of HTTPS encryption in the intranet, resulting in the use of HTTPS plaintext transmission to use various important internal management information systems, and can only pray in heart that there will be no leakage of confidential data on the intranet.

China "Cryptography Law", "Cybersecurity Law", "Data Security Law" and other laws and regulations require that critical information infrastructure systems must use commercial cryptography to achieve information encryption and ensure the security of important confidential data. These compliance requirements and the technical barriers of intranet HTTPS encryption have formed a contradiction that is difficult to solve, which has made the information directors anxious. How to do? The CerSign Intranet SSL Certificates launched today is jointly created by CerSign Technology and ZoTrus Technology, providing a complete and innovative solution.

Let's take a look at the effect of our innovative solution, as shown in the figure below, 192.168.2.199 is a private IP address, "ZoTrus" is a hostname, CerSign Intranet SSL Certificate supports this intranet IP address and hostname, after deploying this intranet SSL certificate on the web server, access with ZT Browser, it uses SM2 algorithm to achieve HTTPS encryption and display “**m**” icon, ZT Browser trusts this intranet SSL certificate. The figure on the left below shows the display effect of the intranet EV SSL certificate, and the figure on the right below shows the display effect of the intranet DV SSL certificate.

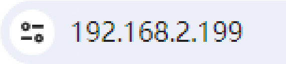


[CN] ZoTrus Technology Limited | https://192.168.2.199

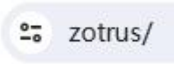


https://zotrus

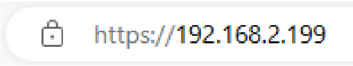
CerSign Intranet SSL Certificates are dual-algorithm certificates same as the Internet SSL certificates. As shown in the figure on the left below, use Google Chrome to visit the same site, HTTPS encryption is trusted and correctly implemented, and it also support intranet IP addresses and internal name. As shown in the figure on the right below, use Microsoft Edge browser to access, trust and display the padlock normally. Google Chrome and Microsoft Edge use the RSA algorithm to implement HTTPS encryption.



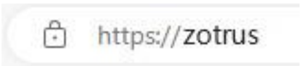
192.168.2.199



zotrus/



https://192.168.2.199

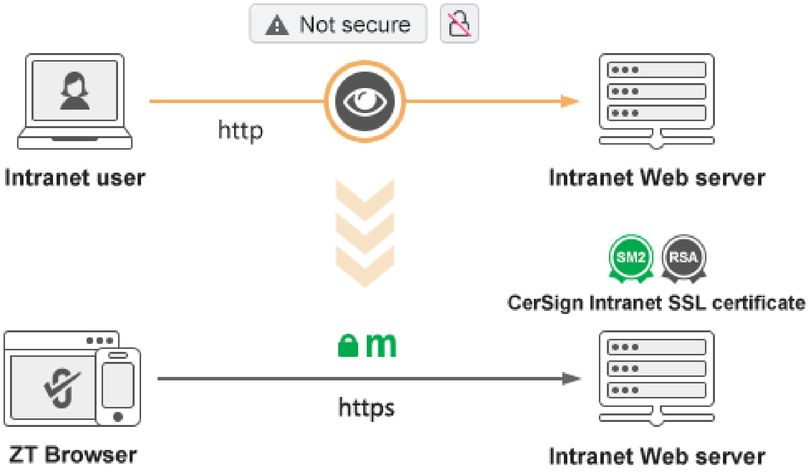


https://zotrus

How does CerSign Technology and ZoTrus Technology do it, and how does it solve this technical problem?

In order to solve the problem of intranet Web traffic encryption, we must first solve the supply problem of intranet SSL certificate, and CerSign Technology has specially created the intranet SM2 algorithm and the RSA algorithm root CA certificates and upgraded the CA system for issuing dual-algorithm intranet SSL certificates, which can issue SM2 and RSA SSL certificates for intranet IP addresses, internal domain names and hostnames, the validity period of the certificate can be 1-5 years, users can purchase an SSL certificate with a validity period of 5 years, to achieve uninterrupted HTTPS encryption without replacing the certificate within 5 years, it can be RSA algorithm HTTPS encryption, if the intranet Web server cannot be modified to support the SM2 algorithm. It is recommended to implement the SM2 HTTPS encryption, if the intranet Web server supports the upgrade to support SM2 algorithm, to meet the requirements of cryptography compliance and cybersecurity protection.

The supply problem of intranet SSL certificate has been solved, but this is only half of the solution, because the SM2 root CA certificate and RSA root CA certificate of this intranet SSL certificate are not trusted by common browsers, and the browser still has insecure warning, so the problem needs to be fully solved by the browser to trust the intranet SSL certificate. ZT Browser can play a big role, ZT Browser has included two intranet root CA certificates of SM2 algorithm and RSA algorithm, which can normally use the intranet SM2/RSA SSL certificate issued by the two intranet root CA certificates, verify and display the padlock normally without security warning, and display the organization name in the address bar for OV SSL certificate and EV SSL certificate, to allows users to easily implement HTTPS encryption on the intranet just like Internet to ensure the security of intranet Web traffic.



ZT Browser not only trusts the CerSign intranet SSL certificate, but also is a completely free SM2 browser that supports the SM2 algorithm, including Windows edition and operating system Kirin and UOS edition (coming soon), so that intranet users can kill two birds with one stone, one is to achieve trusted intranet HTTPS encryption, which effectively guarantees the security of intranet Web traffic, and the other is that users do not need to spend money to buy SM2 browser to achieve intranet cryptography compliance. All you need to do is to apply for and deploy a 5-year SSL certificate and install ZT Browser for free on each intranet computer. Once ZT Browser is installed, other browsers also trust the CerSign RSA intranet SSL certificate, and users can still use these browsers to access the intranet Web system, which is the third thing.

Intranet web security requires an intranet SSL certificate and a browser that trusts the intranet SSL certificate. The CerSign Intranet SSL Certificate plus the completely free ZT Browser perfectly solves the problem of intranet HTTPS encryption, helps intranet users completely solve the security risks of intranet data plaintext transmission, and helps users use HTTPS to ensure the security of intranet confidential data.

Welcome to choose the CerSign Intranet SSL Certificates and download ZT Browser for free use.

Richard Wang

April 22, 2024
In Shenzhen, China