

### Why ZT Browser Launch Trusted Root Program for Intranet SSL Certificate?

The intranet is the inter network of the enterprise that cannot be accessed through the public Internet, and there are many web systems on the intranet that are limited to the access of intranet users, and people often think that access in the intranet is secure and does not need HTTPS encryption. However, IT managers of government agency and large enterprises with higher requirements for data security have realized that intranet web systems also need HTTPS encryption, that is, they need to apply for an SSL certificate and deploy an SSL certificate to achieve HTTPS encryption.

However, international standards do not allow CAs to issue SSL certificates that contain a reserved IP address or called private IP address and an internal name, as such names and IP addresses cannot be validated according to the relevant standards. In other words, if the SSL certificate is bound to a reserved IP address, the CA cannot verify the user's control of the internal IP address, then cannot issue the SSL certificate containing this IP address, which is the basic requirement of an SSL certificate issuance. How to do? People has no choice but to use self-signed certificates, but self-signed certificates are not trusted by all browsers and there will be security warnings. Users have to ignore the security warnings and trust self-signed certificates. However, once this habit is developed, self-signed certificates will be used for fake websites, this also creates security risks, which is not a good idea either. What to do?

ZoTrus Technology has released an innovative solution, not only has it started to issue the CerSign brand intranet SSL certificate, but also include and trust the RSA root CA certificate and SM2 root CA certificate that issue the intranet SSL certificates, so that users can seamlessly use the intranet SSL certificate to achieve HTTPS encryption for intranet traffic. And we share this solution with worldwide CAs, so that CAs can issue intranet SSL certificates trusted by ZT Browser for their customers, which completely helps customers get rid of the dilemma of self-signed SSL certificate that all browsers have security warning, which not only solves the problem of customers, but also brings new profit growth points to CAs.

## 1. What is an Intranet SSL Certificate?

An Intranet SSL Certificate is an SSL certificate whose Subject Alternative Name field contains an internal name and/or reserved IP address, which follows the definition in the CA/B Forum TLS BR 1.6.1.

- (1) **Reserved IP Address:** An [IP v4](#) or [IP v6](#) address that is contained in the address block of any entry in either of the IANA registries.
- (2) **Internal Name:** A string of characters (not an IP address) in a Common Name or Subject Alternative Name field of a Certificate that cannot be verified as globally unique within the public DNS at the time of certificate issuance because it does not end with a Top-Level Domain registered in IANA's Root Zone Database. Simply, it refers to a non-public domain name.

## 2. The baseline requirements for the ZT Browser trusted Intranet SSL Certificates

The reason why international standards do not allow CAs to issue intranet SSL certificates is because they cannot be validated. How does ZT Browser solve this problem? After in-depth research and actual certificate issuance experiments, ZoTrus Technology has formulated the following baseline requirements for intranet SSL certificates.

- (1) The "Subject" field or "Common Name" of the Intranet SSL Certificate must be a public domain name (FQDN), and shall not contain an internal name or reserved IP address, which is used by the CA to validate the ownership of the intranet SSL certificate, and the CA must complete the domain name or IP address validation in accordance with Section 3.2.2.4 or Section 3.2.2.5 of the CA/B Forum TLS BR. This requirement solves the problem of verifiable the intranet SSL certificate.
- (2) Internal names or reserved IP addresses can only be included in the "Subject Alternative Name" field of the SSL certificate, and the CA does not need to validate these internal names and reserved IP addresses. However, the CA must validate all public domain names and IP addresses contained in the Subject Alternative Name field according to the TLS BR. This requirement solves the problem of how an intranet SSL certificate contains the internal name and reserved IP address.
- (3) The validity period of an intranet SSL certificate can be 1-5 years. This is due to the fact that the intranet is a relatively secure system that is only accessible to internal personnel, and the intranet security protection system can ensure that the private key of the certificate is secure to use within

5 years. This greatly facilitates customers to install SSL certificates once and no longer have to apply for certificate and installation certificate within 5 years.

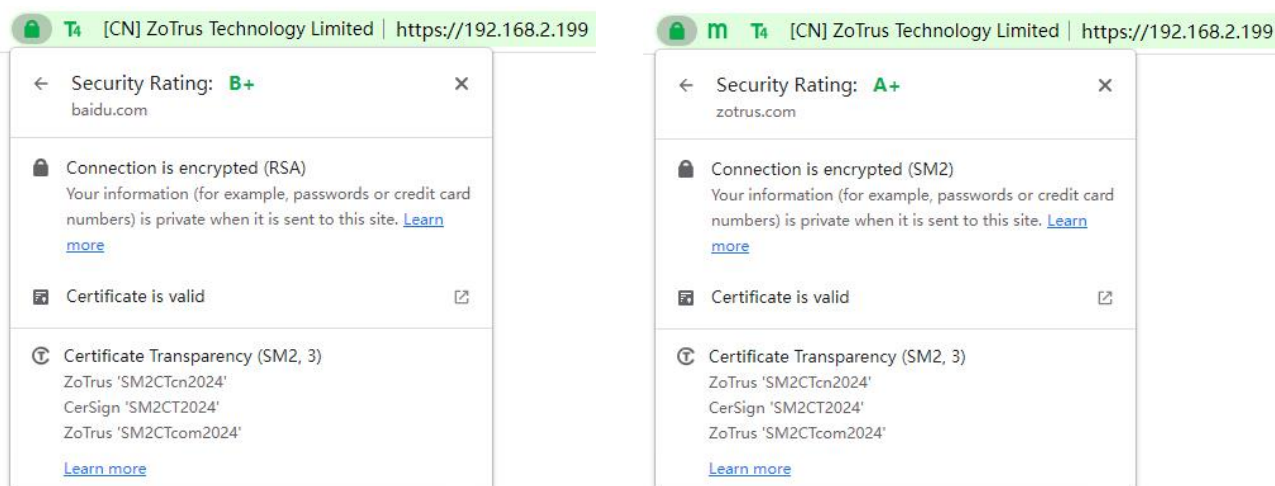
- (4) In view of the fact that only the 3 certificate transparency log systems trusted by ZT Browser currently support intranet SSL certificates, the intranet SSL certificate with a certificate validity period of less than or equal to 180 days must contain 1 certificate transparency SCT data trusted by ZT Browser, and the intranet SSL certificate more than 180 days must contain 2 SCT data. If there are more certificate transparency log systems in the market that support intranet SSL certificates, and it passes ZT browser certification and included, the certificate transparency policy of the intranet SSL certificate will be updated and implemented to the same as the Internet SSL certificates policy.
- (5) Other technical requirements for intranet SSL certificates comply with international SSL certificate standards and SM2 SSL certificate standards.

### **3. How does ZT Browser verify the intranet SSL certificate?**

If only the CA can issue an intranet SSL certificate without browser trust, it is not feasible, and it is also necessary to have a browser to strictly verify the intranet SSL certificate as it handles the internet SSL certificate, not only having the intranet SSL certificate trust CA program, but also the most important thing is that it must support certificate transparency like the internet SSL certificate, only in this way can the security and trust of the intranet SSL certificate itself be guaranteed.

Therefore, ZT Browser not only has the intranet SSL certificate trust program and formulates strict technical requirements for intranet SSL certificates, but also opens ZoTrus SM2 Certificate Transparency Log System to all certified CAs for free, so that they can submit the precertificate to the certificate transparency log system to obtain the certificate transparency log signature data (SCT) and write the SCT data into the intranet SSL certificate just like issuing an internet SSL certificate, so that global users can supervise the issuance of intranet SSL certificates in the same way as supervising the issuance of internet SSL certificates. ZT Browser only trusts the intranet SSL certificate that embedded the SCT data signed by the certificate transparency log system trusted by ZT Browser, to protect the legitimate rights and interests of all intranet SSL certificate users.





Since the certificate transparency log system trusted by Google Chrome does not support intranet SSL certificates, so, CAs can only use ZoTrus SM2 Certificate Transparency Log, and the log signature algorithm adopts the SM2 algorithm, and the CA submits to the certificate transparency log using the SM2 algorithm to obtain log signature data, whether it issues an RSA/ECC SSL certificate or an SM2 SSL certificate. If the CA does not know how to parse the returned SCT data signed by SM2 algorithm, it can also ignore it and simply write the SCT data into the SSL certificate. Of course, before the official issuance of the intranet SSL certificate, the intranet SSL certificate must be deployed, and check if ZT Browser can parse and display the SCT data. As shown in the figure on the left below, ZT Browser displays that the RSA algorithm SSL certificate, but the SCT data is signed by SM2 algorithm, which indicates that the RSA intranet SSL certificate has correctly embedded the SM2 signature SCT data. As shown in the figure on the right below, ZT Browser displays that the SM2 algorithm SSL certificate and SCT data is signed by SM2 algorithm, which indicates that the SM2 intranet SSL certificate has correctly embedded SM2 signature SCT data.



ZoTrus SM2 Certificate Transparency Log supports SSL certificates with RSA, ECC and SM2 algorithms, and ZoTrus does not plan to set up a certificate transparency log server using ECC algorithm for RSA/ECC intranet SSL certificates and uses the ZoTrus SM2 Certificate Transparency Log in a unified manner for all algorithm certificates. CAs are welcome to operate an ECC algorithm certificate transparency log dedicated to intranet SSL certificates, and ZT Browser will quickly include and trust after passing the test, so that the RSA/ECC algorithm intranet SSL certificates issued by global CAs can use the ECC algorithm certificate transparency log service.

In addition to verifying whether the intranet SSL certificate is trusted and whether it supports certificate

transparency, ZT Browser will also display different address bars UI according to different certificate types, but the certificate type international OID used for Internet SSL certificates cannot be used for intranet SSL certificates, so ZT Browser specifies 4 OIDs to identify the intranet SSL certificate types, the details are shown in the following table. If these OIDs are not included in the intranet SSL certificate, the default UI is the intranet DV SSL certificate, displays T1 trust level icon.

SSL Type	Certificate OID	ZT Browser Address Bar UI Display
DV SSL	1.3.6.1.4.1.57933.81	 T1 https://192.168.2.199
IV SSL	1.3.6.1.4.1.57933.82	 T2 [CN] Richard Wang   https://192.168.2.199
OV SSL	1.3.6.1.4.1.57933.83	 T3 [CN] ZoTrus Technology Limited   https://192.168.2.199
EV SSL	1.3.6.1.4.1.57933.84	 T4 [CN] ZoTrus Technology Limited   https://192.168.2.199

**4. Global CAs are welcome to apply for the ZoTrus Trusted Root Program for Intranet SSL Certificates to jointly ensure the security of global intranet Web traffic.**

The security of intranet Web traffic requires the intranet SSL certificate. It also requires a browser to trust the intranet SSL certificate issued by the CA. And it requires a browser to take the lead in formulating the baseline requirements for the intranet SSL certificate, which is the reason why ZT Browser launched the intranet SSL certificate trusted root program.

All CAs are welcome to [apply](#) for ZoTrus Trusted Root Program for Intranet SSL Certificate, includes a dedicated root CA certificate for intranet SSL certificate in ZT Browser, and issue intranet SSL certificates for customers to jointly ensure the security of intranet Web traffic.

*Richard Wang*

April 24, 2024  
In Shenzhen, China