OV SSL certificate is the first choice for intranet SSL certificate

Intranet SSL certificate refers to the SSL certificate issued for the intranet IP address and internal domain name. The SSL certificate commonly used by everyone is the Internet SSL certificate. This globally trusted SSL certificate is not allowed to be bound to the intranet IP address and internal domain name, because ownership of the intranet IP address and internal domain name cannot be validated. This article talks about the difference between the intranet SSL certificate and the Internet SSL certificate, and how to choose the appropriate intranet SSL certificate.

1. What is the difference between an intranet SSL certificate and an Internet SSL certificate?

An intranet SSL certificate is an SSL certificate that is bound to an intranet IP address and host name and is only used for intranet web servers to implement HTTPS encryption. An Internet SSL certificate is an SSL certificate that is bound to an Internet domain name and Internet IP address and is used for Internet web servers to implement HTTPS encryption. The SSL certificates that people often talk about generally refer to Internet SSL certificates.

Intranet is generally considered to be a secure network, because it is only accessible to a limited number of internal personnel, so its internal business management system generally does not enable HTTPS encryption. However, now is the era of the Internet of Everything, and all businesses are managed paperless. The original internal network has become an intranet, a network with a wide coverage. Large intranets such as the national government extranet covering all ministries and provinces and cities across the country. Small intranets such as hospital management information systems are internal network systems covering the entire hospital building to each department and each smart terminal device. If the data streams of these intranets are transmitted in HTTP plain text, they are very easy to be illegally stolen and tampered with. They must deploy SSL certificates to implement HTTPS encryption like Internet websites.

However, the current international standards do not allow globally trusted SSL certificates to be bound to intranet IP addresses, because CA cannot validate intranet IP addresses that can be used by anyone, so there is a new product called Intranet SSL Certificate that can be bound to intranet IP addresses. This is the only difference between intranet SSL certificates and Internet SSL certificates.

2. How does the intranet SSL certificate verify the intranet IP address?

The self-signed SSL certificate issued by the intranet administrator is used for intranet HTTPS encryption, this is not a product, but a technical means to ensure the security of intranet traffic. For an intranet SSL certificate to become a product, it must have its value, just as the Internet SSL certificate has its value and everyone is willing to pay for it.

The value of an intranet SSL certificate, like an Internet SSL certificate, lies in browser trust. There is no unsafe warning, and users do not need to manually trust the SSL certificate deployed by the website. The reason why international standards do not allow the issuance of SSL certificates bound to intranet IP addresses is because the bound intranet IP addresses cannot be validated. ZoTrus Technology innovation solves this problem, that is: the common name (CN field) in the SSL certificate must be bound to a verifiable public domain name, while the intranet IP address and host name are bound to the SAN field and do not need to be verified because they cannot be verified. Therefore, when users apply for an intranet SSL certificate, they must complete the domain name control validation just like applying for an Internet SSL certificate. Completing the domain validation of the domain name bound to the certificate means that the user can control the private key of this certificate, and the user can arbitrarily add intranet IP addresses and host names without verification. This perfectly solves the problem of the inability to verify intranet IP addresses. This is a problem that has not been solved in the global industry, and ZoTrus Technology is the first in the world to innovate and solve it.

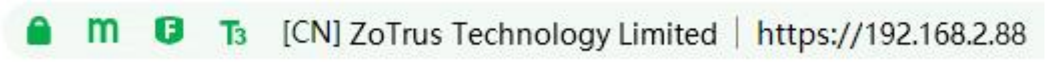
After understanding this key point, users will not repeatedly ask customer service why they must fill in the Internet domain name and complete validation when applying for an intranet SSL certificate. This is because this is the only method that can be used to prove that the user controls the certificate key, and the validation is completed in a validation method that complies with international standards. ZoTrus Technology has grasped that the core of SSL certificate issuance is to validate the control of the SSL certificate key. If the validation of this control is completed for the intranet SSL certificate, the CA can safely and reliably issue the intranet SSL certificates to end users.

3. Why is OV SSL certificate the first choice for intranet SSL certificate?

In order to distinguish between Internet SSL certificates and intranet SSL certificates, and to meet the compliance requirement that Internet root CA certificate cannot issue intranet SSL certificates, ZoTrus Technology has specially established independent intranet-specific RSA algorithm and SM2 algorithm root CA certificates. The dual-algorithm root CA certificates for CerSign Intranet SSL Certificates that users can apply for online are: **CerSign Intranet SM2 Root** and **CerSign Intranet RSA Root**. The dual-algorithm root CA certificates for dual-algorithm SSL certificates automatically configured by ZoTrus Intranet Gateway are: **AAA Intranet SM2 Root** and **AAA Intranet RSA Root**. The reason for taking a neutral root CA certificate name is to design a neutral name for other partners who are interested in customizing intranet SSL issuing CA for selling their own brand of intranet SSL certificates, because browser-trusted intranet SSL certificates are a new SSL certificate market, an emerging market that is broader than Internet SSL certificates, and a golden market that has not yet been cultivated.

Intranet SSL certificates are the same as Internet SSL certificates, and are also divided into Intranet DV SSL certificates, intranet OV SSL certificates, and intranet EV SSL certificates. Since intranet SSL certificates are only used by internal users, there is no longer need EV SSL certificates for enhancing trust, so the EV SSL certificate is not the first choice. As for intranet DV SSL certificate that only validates domain name control, the certificate does not contain organization name information, it is impossible to determine the website identity based on the intranet IP address alone, which is not conducive to intranet users identifying the identity of the intranet system, so the DV SSL certificate is not recommended.

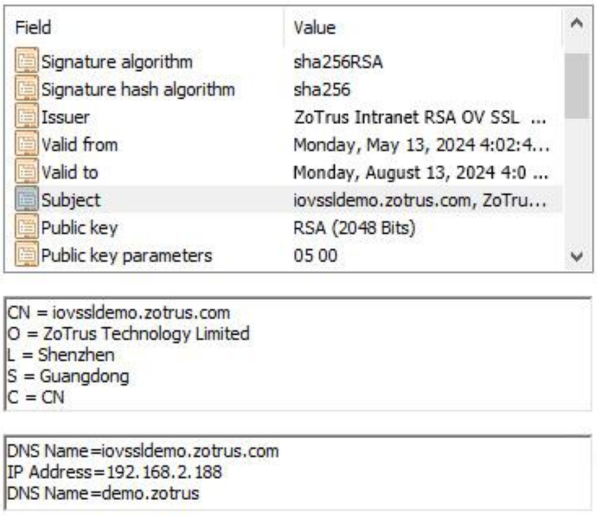
The preferred and recommended choice for intranet HTTPS encryption is an OV SSL certificate containing the organization name, because anyone can use the intranet IP address, and only the organization name is the identity information that can identify this internal website. In this way, when intranet users use ZT Browser to access the intranet system, the organization name will be displayed in the address bar, making it easier for users to identify the real identity information of the intranet system they are accessing. This is the main reason for choosing an intranet OV SSL certificate. In other words, the public domain name of the intranet SSL certificate's common name (CN field) is used to verify the user's control over the intranet SSL certificate private key, while the organization name in the certificate's O field is the unique identifier that proves the identity of this intranet Web system.



[CN] ZoTrus Technology Limited | https://192.168.2.88

4. ZoTrus Intranet Gateway default configuration dual algorithm OV SSL certificate

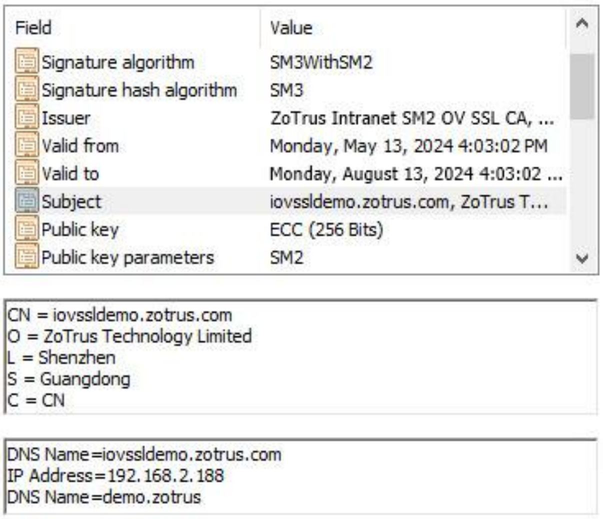
In order to achieve the automatic application and deployment of intranet SSL certificates like Internet SSL certificates, ZoTrus Technology has innovatively launched the Intranet HTTPS Automation Gateway, which is also a global first. It is a hardware gateway device that can automatically apply for and deploy intranet SSL certificates for intranet websites. The automatic configured dual-algorithm SSL certificates are OV SSL certificates, bound to the gateway customer organization name. Intranet users can access the intranet web system using HTTPS with a public domain name (must be resolved to the intranet IP address), directly using the intranet IP address, or using the host name. Not only does the ZT Browser trust and display the organization name in the address bar, but other commonly used browsers also trust it, achieving maximum compatibility with the adaptive cryptographic algorithm.



Field	Value
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	ZoTrus Intranet RSA OV SSL ...
Valid from	Monday, May 13, 2024 4:02:4...
Valid to	Monday, August 13, 2024 4:0 ...
Subject	iovssldemo.zotrus.com, ZoTru...
Public key	RSA (2048 Bits)
Public key parameters	05 00

CN = iovssldemo.zotrus.com
O = ZoTrus Technology Limited
L = Shenzhen
S = Guangdong
C = CN

DNS Name=iovssldemo.zotrus.com
IP Address=192.168.2.188
DNS Name=demo.zotrus



Field	Value
Signature algorithm	SM3WithSM2
Signature hash algorithm	SM3
Issuer	ZoTrus Intranet SM2 OV SSL CA, ...
Valid from	Monday, May 13, 2024 4:03:02 PM
Valid to	Monday, August 13, 2024 4:03:02 ...
Subject	iovssldemo.zotrus.com, ZoTrus T...
Public key	ECC (256 Bits)
Public key parameters	SM2

CN = iovssldemo.zotrus.com
O = ZoTrus Technology Limited
L = Shenzhen
S = Guangdong
C = CN

DNS Name=iovssldemo.zotrus.com
IP Address=192.168.2.188
DNS Name=demo.zotrus

The dual-algorithm OV SSL certificate automatically configured by ZoTrus Intranet Gateway is not a one-year or multi-year SSL certificate, but an OV SSL certificate with a validity period of 90 days. It supports automatic configuration of dual-algorithm Intranet SSL certificates for up to 510 Intranet websites. Each website has an independent key and independent certificate, the key and certificate are updated every 80 days to ensure that the Intranet SSL certificate can meet the upcoming 90-day validity security policy, the same as the Internet SSL certificate, and effectively protect the security of the Intranet HTTPS.

Richard Wang

April 21, 2025
In Shenzhen, China

Follow ZT Browser at X (Twitter) for more info.
The author has published 91 articles in English (more than 121K words) and 210 articles in Chinese (more than 621K characters in total).