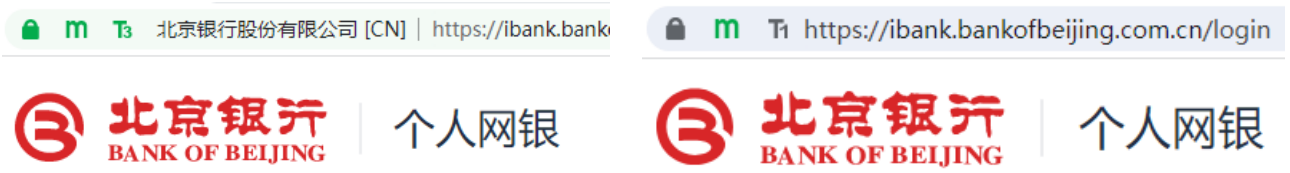
How does the browser identify the type of SSL certificate?

Some users reported that after ZT Browser was upgraded to version 114, the version 97 displayed that the website with a website identity validation icon T3 was displayed as T1, and the company name displayed in the light green address bar also disappeared. What's going on? This article will talk about this issue. This issue has nothing to do with version 114. It is an issue about how to define the type of SM2 SSL certificate and how to identify it by browser. It is also a pending issue in the relevant SM2 standards, the author believes that it is necessary to talk about this issue, in order not only to answer users' questions, but also to inspire discussions on the types of certificates in the formulation of the SM2 SSL Certificate standards, which will help the industry to reach a consensus.

As shown in the left picture below, this is ZT Browser displaying the Bank of Beijing personal online banking page before the upgrade, displaying the green padlock, green SM2 encryption icon and the green T3 trust level icon on the light green address bar. The picture on the right is the new UI after the upgrade, this is nothing to do with the version 114 upgrade, but it has to do with the change of the UI display rules in this upgrade. This website that normally displays the website identity validation level as "T3" has changed to display as "T1". This is not because the ZT Browser made a mistake, but because the SSL certificate deployed by this website does not have the correct certificate type OID. This article will talk about the certificate type OID in detail.



There are 4 types of SSL certificates: DV SSL, IV SSL, OV SSL, and EV SSL, which are defined according to the identity validation level. The DV SSL certificate only needs to validate the domain control, the IV SSL certificate not only needs to validate the domain control, but also needs to verify the personal identity of the website owner; the OV SSL certificate not only needs to validate the domain control, but also needs to verify the identity of the website owner; EV SSL certificates not only need

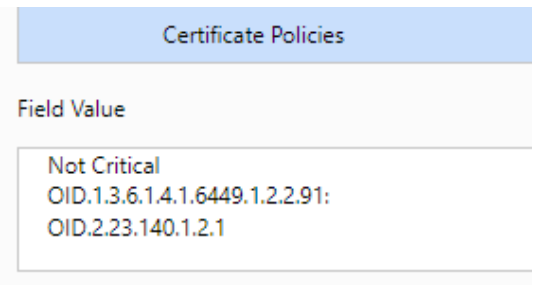
to validate the domain control, but also need to extend to verify the identity of the website owner in accordance with stricter validation standards.

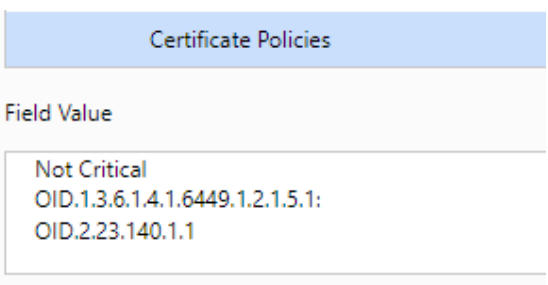
Based on this classification, ZoTrus Technology also defines 4 levels for website trusted identities: T1, T2, T3 and T4. T is the first letter of the English "Trust", and T1, T2, T3 and T4 correspond to DV SSL, IV SSL, OV SSL, and EV SSL respectively. That is to say, for any website deployed with DV SSL certificate, the address bar of ZT Browser will display the T1 icon, and so on, the website deployed with IV/OV/EV SSL certificate will display the T2/T3/T4 icon respectively. Why does the T3 icon on the Bank of Beijing website you see in the left picture above changed to T1 icon in the right picture after upgrading to version 114? This is the focus of this article.

In order for the browser to recognize the certificate type and identity validation level of the SSL certificate deployed on the website, the CA/Browser Forum defines 4 OIDs for the 4 types of SSL certificates, which are:

- DV SSL Certificate: CA/B Forum OID: 2.23.140.1.2.1
- IV SSL certificate: CA/B Forum OID: 2.23.140.1.2.3
- OV SSL Certificate: CA/B Forum OID: 2.23.140.1.2.2
- EV SSL Certificate: CA/B Forum OID: 2.23.140.1.1

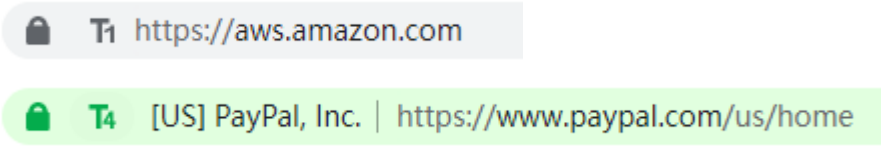
All publicly trusted RSA/ECC SSL certificates will contain one of these 4 OIDs in the "Certificate Policy" field of the SSL certificate to prove what type of SSL certificate this SSL certificate is. The left picture below shows the certificate policy "Policy Identifier=2.23.140.1.2.1" of the SSL certificate deployed on the ZoTrus official website, which indicates that this SSL certificate is a DV SSL certificate, and the right picture shows the SSL certificate deployed on the CerSign official website, the certificate policy is "Policy Identifier=2.23.140.1.1", which indicates that this SSL certificate is an EV SSL certificate.



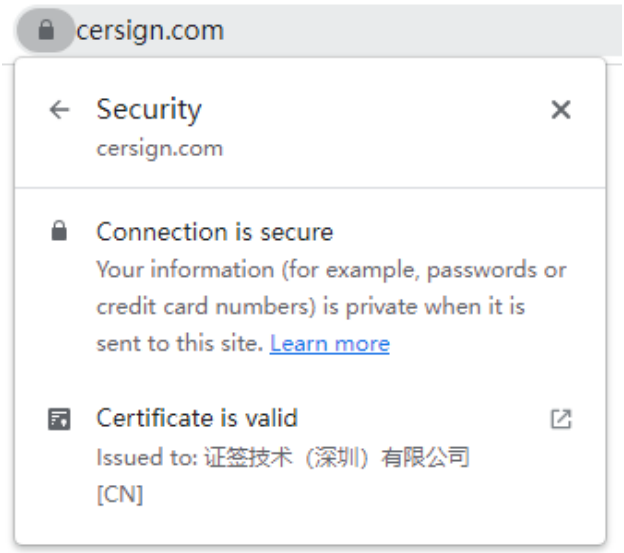


In the early years, all browsers displayed a green address bar for websites deployed with EV SSL certificates based on the EV SSL OID. In order to prevent the CA from using the EV SSL type OID by mistake, browsers generally require the CA to provide another EV SSL certificate OID assigned from each CA's own OID system. The first OID in the above right figure is Sectigo dedicated EV SSL OID. The browser will also manage a list of root CA certificates that can issue EV SSL certificate. The figure below shows the effect of the EV SSL certificate displayed by the IE browser.

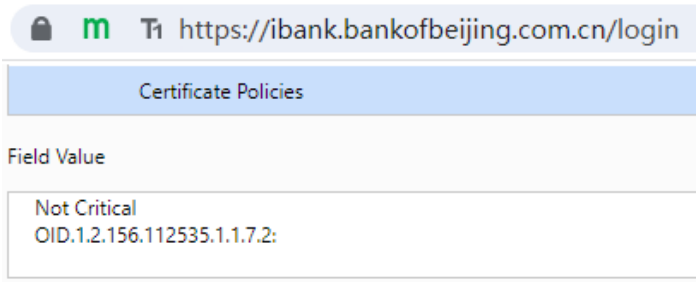
Although other browsers have now abandoned the green address bar of the EV SSL certificate, Z Browser believes that the EV green address bar is still very valuable, allowing users to recognize at a glance that this website is a highly trusted website, because its real identity has been strictly validated by a trusted third-party. Therefore, ZT Browser continues to maintain the green address bar of the EV SSL certificate, and continues to display the green address bar for websites that deployed EV SSL certificate. Other types of SSL certificates also identify the type of SSL certificate deployed by the website according to the international standard certificate type OID, thus displaying different UIs. For websites deployed with DV SSL certificates, the address bar displays the T1 icon, while for websites deployed with EV SSL certificate, the address bar displays the T4 icon.



Although Google Chrome has given up the EV green address bar, it still retains the organiztion name in the certificate subject O field displayed under the "Certificate Valid" logo for websites that have deployed EV SSL certificates.



Back to the user's question, the "Certificate Policies" of the SM2 SSL certificate deployed by the Bank of Beijing does not contain one of the four OIDs shown above, as shown in the left figure below. Therefore, ZT Browser can only display the "T1" icon, because the reason why this SSL certificate can be issued must have completed the domain control validation and must meet the requirements for displaying the T1 icon. Users will definitely ask: Since there is no required OID, why can the 97 version can display the "T3" icon? Please see the picture on the right, there is an O field in the subject of this SSL certificate. The 97 version is based on the fact that this SSL certificate has an O field, so the Browser displayed the T3 icon and the name of the organization in the certificate O field. This is a compromise plan after finding that almost all SM2 SSL certificates do not have a certificate type OID at the release of ZT Browser. After upgrading to version 114 now, ZTBrowser adjusted the UI policy to display the SSL certificate type deployed on the website in strict accordance with international standards. Therefore, the new version browser displays the "T1" icon because it cannot find the required certificate type OID.

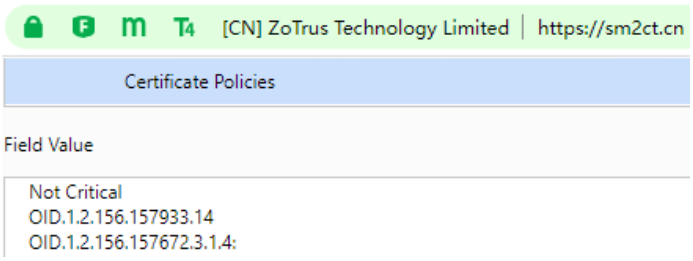


Maybe professional users or the issuing CA will ask: Why do the SM2 SSL certificate types must have

the international SSL certificate type OID? We like to use our own OID. Can the Browser identify the correct certificate type based on our own OID? These are good questions. ZT Browser has clearly informed all CAs when releasing the ZoTrus Trusted Program that ZT Browser has defined 4 OIDs for the SM2 SSL certificate type for free, and all CA can use these 4 OIDs for free for its issued SM2 SSL certificates.

- DV SSL certificate: 1.2.156.157933.11, corresponding to CA/B Forum OID: 2.23.140.1.2.1
- IV SSL certificate: 1.2.156.157933.12, corresponding to CA/B Forum OID: 2.23.140.1.2.3
- OV SSL certificate: 1.2.156.157933.13, corresponding to CA/B Forum OID: 2.23.140.1.2.2
- EV SSL certificate: 1.2.156.157933.14, corresponding to CA/B Forum OID: 2.23.140.1.1

That is to say, ZT Browser will idetify the type of SM2 SSL certificate based on the 4 international standard certificate type OIDs and 4 ZT Browser defined certificate type OIDs. If the certificate policy of the SSL certificate contains OID: 1.2.156.157933.14 or 2.23 .140.1.1, ZT Browser will know that this SSL certificate is an EV SSL certificate, and will display the T4 icon, as shown in the left figure below, the "Certificate Policies" in this SM2 SSL certificate has "Policy ID: 2.23.140.1 .1", ZT Browser displays the T4 icon. As shown in the figure on the right below, the "Certificate Policies" in this SM2 SSL certificate has "Policy ID: 1.2.156.157933.14", ZT Browser also displays the T4 icon.

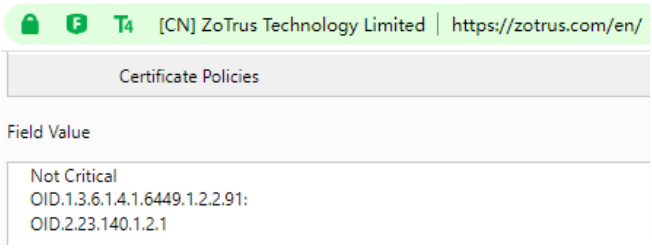


All SM2 SSL certificates issued by ZoTrus Cloud SSL Service System only contain the four SM2 SSL certificate type OIDs defined by ZT Browser, and will not contain the international SSL certificate type OID. This is because the official website of the CA/Browser Forum publishes international OID page clearly indicates the scope of application of these international OIDs, such as the definition of EV SSL certificate OID: extended-validation(1) - 2.23.140.1.1 (Certificate issued in compliance with the Extended Validation Guidelines). All SM2 SSL certificates only refer to international standards, and do not fully follow EV Guideline standards. Therefore, according to the above definition, these

international OIDs cannot be used to define SM2 EV SSL certificates. This is the basis for ZoTrus Technology's proposal that "the SM2 SSL certificate type OID must be defined under the SM2 algrithm OID arc" when discussing the establishment of the SM2 SSL certificate standard. Before the SM2 SSL certificate type OID is defined in GM/T standard, ZoTrus Technology provided 4 SM2 SSL certificate type OIDs for free use.

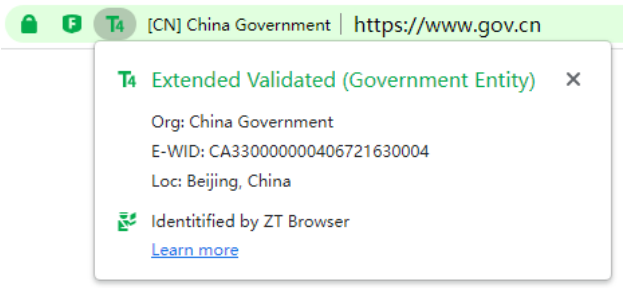
The current policy adopted by ZT Browser is to be compatible with the international certificate type OID. No matter whether the SM2 SSL certificate contains the international SSL certificate type OID or the SM2 SSL certificate type OID defined by ZT Browser, ZT Browser can correctly display the SM2 SSL certificate type, and other OIDs other than these two types can not correctly identify, resulting in the certificate type being displayed as T1. ZT Browser cannot recognize the certificate type OID customized by each CA.

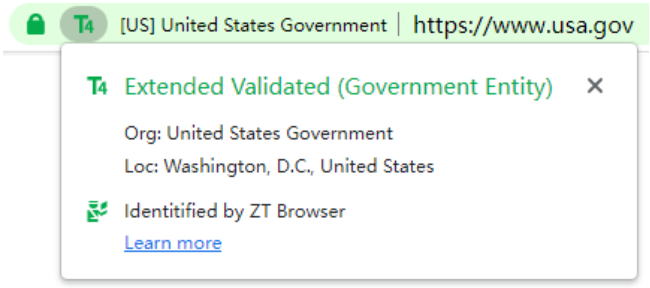
Careful readers may also ask: The certificate policy in the SSL certificate deployed in ZoTrus website is "OID.2.23.140.1.2.1" that it is a DV SSL certificate, why does the ZT Browser display the T4 icon? Similarly, why does the official website of the USA government deploy the DV SSL certificate (OID.2.23.140.1.2.1), but why does ZT Browser display the T4 icon?



This is also one of the innovations of ZT Browser - Website Trusted Identity Validation Service. In view of the fact that 83% of the world's websites deploy DV SSL certificates that have not verified the identity of the website, in order to solve the problem of the lack of trusted identity of these websites, ZoTrus Technology has launched a website trusted identity validation service, and ZoTrus Technology will complete the website's trusted identity validation, no matter whether the SSL certificate deployed on the website is a DV SSL certificate without identity information or an OV SSL certificate, ZT Browser will display the "T4" icon and the green address bar, and the display effect is equivalent to the website deployed an EV SSL certificate. The above figure shows that the website with the "T4"

icon has passed the EV Certification, so the "T4" icon is displayed.





The author believes that through the above explanation, you should be able to understand why the upgraded ZT browser will display the website that displaying “T3” in the old version as "T3". The author hereby reminds all the SM2 CAs trusted by ZT Browser to upgrade the CA system as soon as possible and add the 4 SSL certificate type OIDs defined by ZT Browser or the international SSL certificate type OID to the issued SM2 SSL certificates, so that ZT Browser can correctly identify the types of SM2 SSL certificates issued by CAs, and correctly display the trusted level icon of the website.

Welcome to apply for ZoTrus Website Trusted Identity Validation Service. The website can still deploy free or cheap DV SSL certificates, after passing the EV Certification, ZT Browser will display the "T4" icon, organization name in the green address bar. Website security requires https encryption and trusted identity at the same time, which can effectively enhance the confidence of website visitors, thereby facilitating more online transactions.

Richard Wang

August 8, 2023
In Shenzhen, China