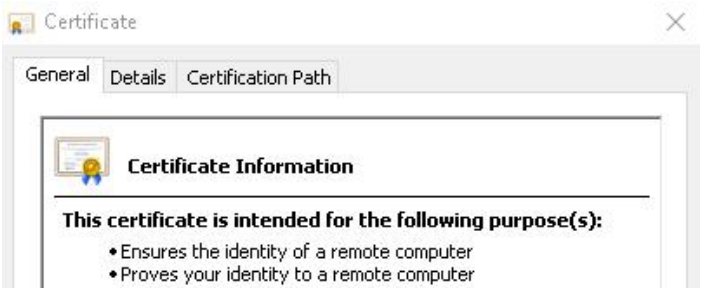
The third of three steps of zero trust security for websites: trusted identity validation

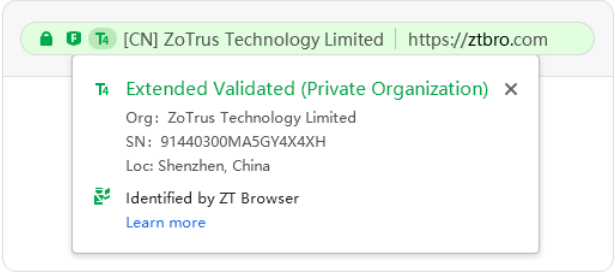
Zero trust is a security principle, it is also very suitable for website security. All browsers display HTTP websites as "Not secure," which is zero trust to websites that don't have a validated trusted identity. Some readers may say that browsers display "Not secure" to HTTP sites because the site does not deploy an SSL certificate for HTTPS encryption, and this is correct. However, let's think about what an SSL certificate is. It is a certificate issued by a CA to prove the trusted identity of a website after completing the identity validation of the website, and this certificate can also be used to transmit encryption and exchange encryption keys. So, that's zero trust for all browsers to website that doesn't pass the identity validation, which will display "Not secure". You can click padlock to view the purpose of the SSL certificate to verify my point of view. As shown in the figure below, the purpose of the SSL certificate is to "Ensure the identity of a remote computer and prove your identity to a remote computer", which is used to prove the trusted identity of the websites, encryption is only a secondary function, its main function is server authentication.

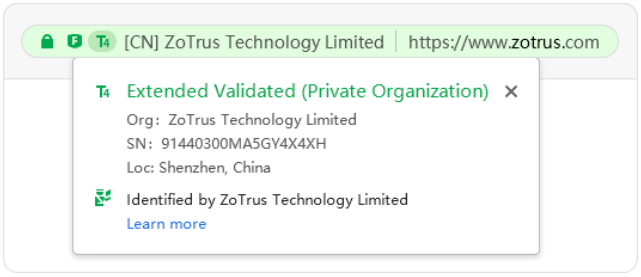


The author explained in detail in the blog post "The first of three steps of zero trust security for websites: HTTPS encryption", which is the basis of website security. However, HTTPS encryption alone is not enough for a website, and cloud WAF protection is also required. This is what the second blog post "The second of three steps of zero trust security for websites: cloud WAF protection" talks about. The website has HTTPS encryption and cloud WAF protection, but it is still not enough, and the trusted identity validation of the website is also required. If the SSL certificate that implements HTTPS encryption is the OV SSL certificate or EV SSL certificate that has validated the identity of the website, it perfectly fulfills the three protection requirements of website security: HTTPS encryption, cloud WAF protection and trusted identity validation.

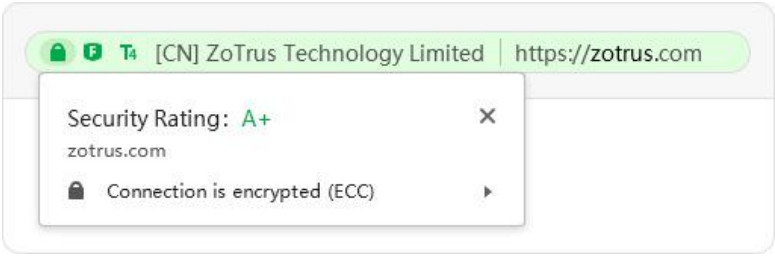
It is a pity that 83% of the websites that have deployed SSL certificates in the world are deploying DV SSL certificates that do not validate the trusted identity of the website, which enables fake and fraudulent websites to have HTTPS and cloud WAF protection. I believe that no one will think that this fake and fraudulent website is secure. The FBI's Internet Crime Complaint Center warns consumers - don't trust a website just because it has a lock icon or “https” in the browser address bar, as shown in the figure below. This is zero trust to website identity and zero trust tor https encryption.

Therefore, website zero trust security also needs an independent website identity validation service to make up for the lack of website trusted identity validation of DV SSL certificate. Website trusted identity validation is the third important element of website security, it is as important as HTTPS encryption and cloud WAF protection! The solution of ZoTrus Technology is ZoTrus Website Trusted Identity Validation Service. Websites owners deploying DV SSL certificate can apply for website trusted identity validation service. ZT Browser will automatically retrieve the website trusted identity data and display it directly in the address bar. As shown on the left below. For websites that have deployed IV SSL, OV SSL, and EV SSL with validated identities, ZT Browser directly reads the O field information in the subject of SSL certificate to display the trusted identity of the website, as shown in the right figure below. Clicking the trusted validation icon will not only display the detailed website identity information, but also show who validated the identity of this website.





The address bar of the ZT Browser displays the trusted identity of the website, so that website visitors can check the real and trusted identity of the website immediately, which can effectively enhance the online trust of website visitors. Whether a website has passed the trusted identity validation accounts for 20% of the website security rating integrated in ZT Browser. With trusted identity validation, the security rating level of the website can be effectively improved.



In summary, for website security, it is necessary to have zero trust to the identity of websites that are not validated, so all browsers will display "Not secure". ZT Browser always verifies the trusted identity of the website, and it is the first in the world to restore the green bar with organization name for EV SSL certificate deployed websites and EV certified websites that it is the most stringent website identity validation, and takes the lead in innovatively to display light green bar and organization name for OV SSL certificate deployed websites and OV certified websites, and takes the lead in innovatively to display light green bar and personal name for IV SSL certificate deployed websites and IV certified websites, which perfectly realizes the third step of zero trust security for websites. Customers can use ZT Browser to understand the actual situation of this step in real time, compare and understand the improvement of website security status before and after using ZoTrus Website Security Cloud Service and applied the Website Trusted Identity Validation Service in a simple and clear way (the website security rating will rise), so that customers can be assured of their website security status, and they can focus on doing their own business well.

Richard Wang

June 24, 2022
In Shenzhen, China