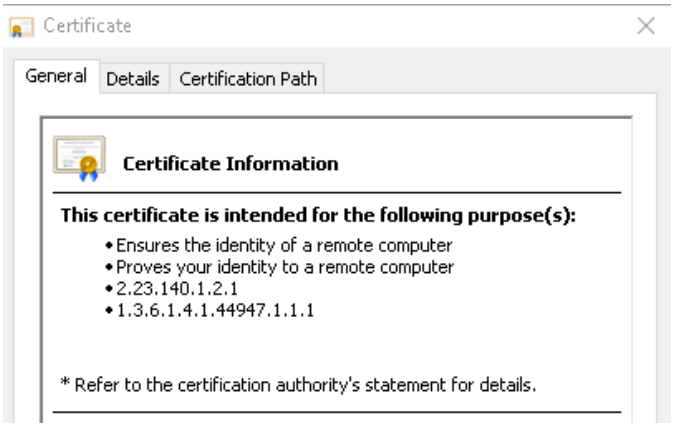
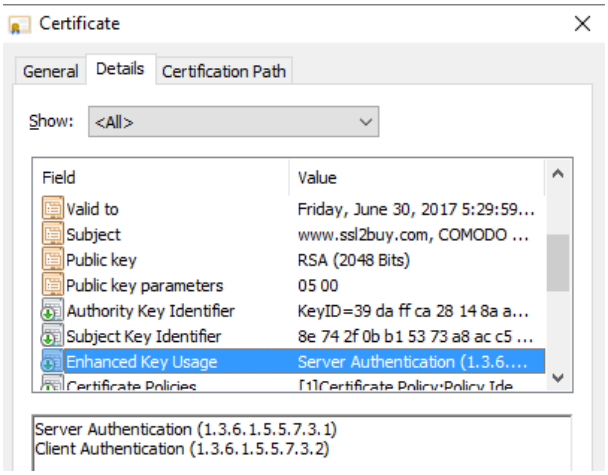
# Re-understanding SSL certificate

According to the latest Certificate Transparency log data, DV SSL certificates that only validate domain name control have accounted for 83.43% of SSL certificate, which means that among the 100 websites visited by netizens that have deployed SSL certificates, 83 websites have deployed an SSL certificate that do not validate the identity of the website owner, DV SSL certificate has become the mainstream SSL certificate. This makes us must re-understand the SSL certificate, what is the SSL certificate? How to face the reality that SSL certificate has become the world of DV SSL certificate.

Click the security padlock of the https website to view the SSL certificate, as shown in the left figure below, the certificate information shows "This certificate is intended for the following purpose(s): Ensure the identity of a remote computer, Proves your identity to a remote computer", the first sentence "remote computer" refers to the web server, meaning that the SSL certificate can prove the identity of the web server; the second sentence "remote computer" refers to the user's computer. When the user uses a browser to access the website, the identity of the website is certified by the SSL certificate to prove the real identity of the website. The core meaning of the two sentences is that the trusted identity of the website is certified by the SSL certificate.




If the reader is still a little confused, you can click the certificate "Details", as shown in the right figure above, the certificate's "Enhanced Key Usage" is "Server Authentication, Client Authentication" and "Key Usage" is " Digital Signature", it can be seen that the main usage of SSL certificate is identity

authentication, and digital signature is used to prove its identity and ensure that the server identity is trusted. HTTPS encryption is only a secondary function. After verifying the identity of the server, the public key of the server is used to encrypt the data exchanged with the web server.

However, the widely used DV SSL certificate does not verify the real identity of the website when it is issued, so the subject of the DV SSL certificate is only the website domain name, and there is no website identity information. The DV SSL certificate is only used for exchanging public keys and for https encryption without verifying the identity of the website. Is the change from "second function" to "first function" far from the original intention of inventing the SSL certificate? The SSL certificate automatically issued after the machine verifies the control of the domain name allows fraudulent and fake websites also can have SSL certificates, so that the fake bank website is the same as the security padlock displayed on the authentic bank website, and the fake government website is displayed the same padlock with the authentic government website. Is this the "Security" we need? This is why the FBI website warns consumers to stop trusting their browser's https padlock. Is the security padlock relied on by netizens around the world no longer secure? What to do?

ZoTrus Technology's solution to this situation is to release ZT Browser, which clearly shows that the website has deployed OV SSL certificate and EV SSL certificate, the address bar is white and green respectively, and display the website owner’s name in the address bar, so that website visitors can easily know the real identity information of this website, instead of making a statement like some government websites, fake websites can also make such a statement. For websites with DV SSL certificates deployed, not only the address bar is grayed out, but also "Identity Not Validated" is displayed directly in the address bar, allowing website visitors to identify the website and make informed security decisions.

In order to solve the identity trust problem of a large number of websites that have deployed DV SSL certificates, ZoTrus Technology has launched a website trusted identity validation service to make up for the lack of website identity in the DV SSL certificates. The website identity validation is completed according to international standards as OV SSL and EV SSL validation, and the identity of the website is displayed in ZT Browser as if the OV SSL certificate and EV SSL certificate are deployed. The DV SSL certificate is only used for https encryption, and its identity authentication function is provided by

ZoTrus Website Trusted Identity Validation Service and ZT Browser, this solution is undertaken to make up for the deficiency that the current DV SSL certificate does not validate the identity of the website, thus effectively guaranteeing the security of the netizens accessing the Internet.

It has been 28 years since the SSL certificate was born in 1994. GeoTrust invented the DV SSL certificate that only validates the domain name in 2002. The DV SSL certificate has made great contributions to the popularization of https encryption. However, this is a "defective" product that "castrated" the identity authentication function of the SSL certificate, but now we can't do without this product, because DV SSL certificates can be obtained for free or at a low price. That is to say, it is time to re-recognize SSL certificate. We must accept the reality that 85% of SSL certificates have no website identity information. We can only treat SSL certificates as an encrypted product, and the work of displaying and verifying website identity can only be done by browser. This work has been provided to global netizens by ZT Browser as a public service product, which will make contributions to ensuring the security and trust of the global Internet.

ZoTrus Website Security Cloud Service is a website security solution that integrates https encryption, WAF protection and website trusted identity validation. It can perfectly make up for the shortage of websites that only deploy DV SSL certificates to implement https encryption only, because customers need a website secure and trusted solution, not just encryption-only, encryption does not equal security.

Richard Wang

**June 6, 2022**
**In Shenzhen, China**