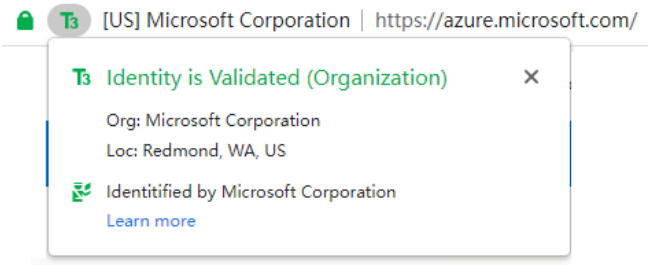
Displaying website identity is the browser's obligation

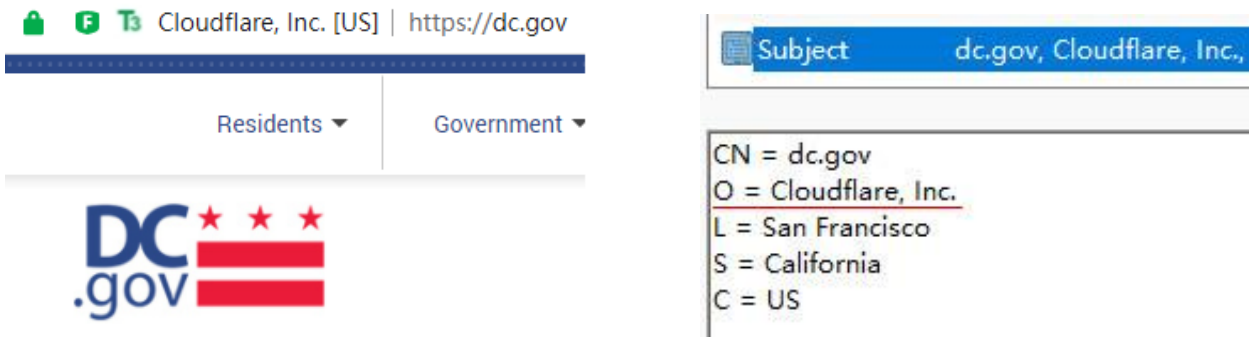
The author said in the blog post "The green address bar is back" that Google Chrome and Firefox browsers no longer display the green address bar of EV SSL certificate, this has encountered opposition from many CAs and many well-known CA experts. As a CA specialist who has been in the CA business for 18 years, the author is also opposed to this change. Today, the release of ZT Browser not only shows my opposition attitude, but also a real action, which not only brings back the green address bar of EV SSL certificate, but also innovatively demonstrates the deployment of OV SSL and IV SSL certificate website's identity information. I think that it is the responsibility and obligation of the browser to display the identity of the website since browser is the tool for user access to the Internet, so the identity information of the website must be provided very intuitively for users to make correct security decisions, it should not be made inappropriate changes without listening to the opinions of the industry. After all, the browser is not an ordinary product, but a must-have public product for public welfare.



From how ZT Browser shows the EV SSL certificate and the OV SSL certificate above screenshot, you can be seen that ZT Browser reads the O field information in the SSL certificate and display it on the address bar. Please look at the ZT Browser official website: www.ztbrowser.com using Cloudflare service, if we don't use the policy of ZoTrus validated identity priority, ZT Browser will display this website as shown in the left picture below since the certificate subject O field name is Cloudflare, Inc. and C field is US, as shown in the right picture below.

But ZT Browser used the ZoTrus validated identity database to correct this mistake that display this website green address bar and company name correctly, see below picture. Please note that this is effect of ZoTrus Website Trusted Identity EV Certification service whether this website deployed a DV SSL or OV SSL certificate.

Let's check another website: **dc.gov**, if the browser displays the certificate O field in the address bar, then it will be displayed as shown in the left picture below. Please don't think this display is wrong, the wrong is the certificate, see below left picture for the subject O filed of this certificate.



To solve this mismatch identity problem for all Cloudflare WAF protected website, ZT Browser setup a special processing rule that these websites will not display the certificate O field info and treat all certificate as DV SSL certificate. And these websites that have passed the ZoTrus Trusted Identity Validation, ZT Browser display its validated identity preferentially, so the identity of the government website of District of Columbia is displayed correctly, see below picture.

These website identity mistakes are caused by the fact that current browsers no longer display the identity information in the SSL certificate. It can be said that this is a technology backward. This is also the inevitable result of everyone deploying only cheap DV SSL certificate since the browser displays the SSL certificates of different validation levels are the same, only the security padlock is displayed in the address bar. And this is why ZoTrus launched Website Trusted Identity Validation service and why ZT Browser adopts preferentially displaying the ZoTrus validated organization name.

Readers should be able to appreciate the uniqueness of ZT Browser in displaying website identity from the above demonstration cases, and innovatively and accurately display the identity of the website, which is convenient for website visitors to correctly identify the identity of the website, to make correct security decisions. To facilitate your understanding of our innovative solutions, the author recommend a blog post "Why Are You Removing Website Identity, Google and Mozilla? ", that it against Google Chrome and Firefox browsers no longer displaying EV SSL certificate green bar. The author is Tim Callan, Chief Compliance Officer of Sectigo, published on the official website of the PKI Consortium on August 27, 2019. I copied the last section "Recommendations" of Tim's blog post for the reference because these words are also what I want to say.

"We were among the group who put together the original EV specification. At that time, we envisioned EV would be an ongoing, evolving standard that the community continued to make better. Hearing objections about EV being less than perfect, one cannot help but think of the adage about perfect being the enemy of good. EV is good. It's really good, and the statistics indicate that it is helping make the web a better place. Let's focus our energy on making it even better.

The CA Security Council believes that the industry should evolve the EV certificate indicators, rather than remove them. To combat phishing and raise identity standards for websites, we believe the

browser companies should work together to develop common security indicators for laptops and mobile devices, and to engage with CAs on user training to help users make good security decisions based on available identity information. There's a great opportunity for innovation and collaboration here, that will benefit web users and the whole industry."

Richard Wang

June 1, 2022
In Shenzhen, China