# OV SSL/EV SSL Certificate O Field Mistakes Found and Solution

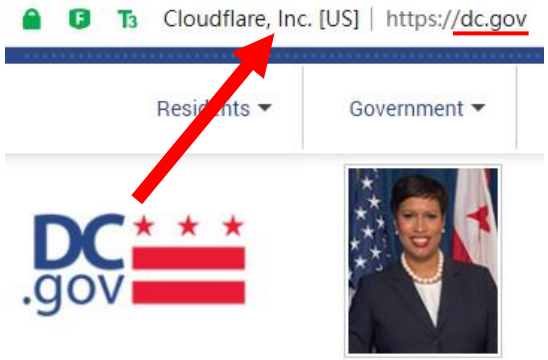
**ZoTrus Technology Limited**

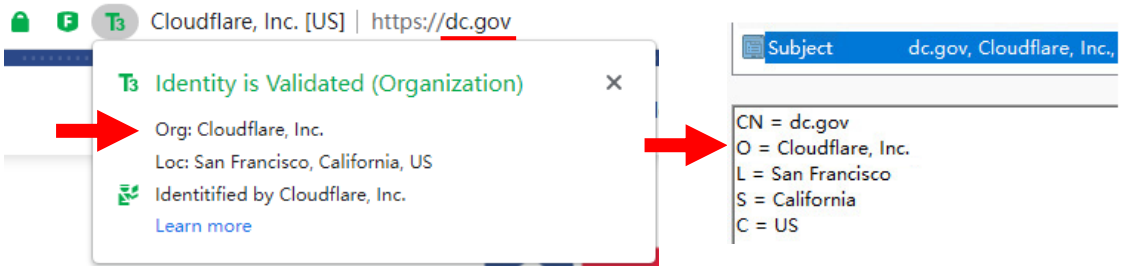
Richard Wang (richard@zotrus.com)

2022.06.03

CONTENTS

# Website identity mismatch case study

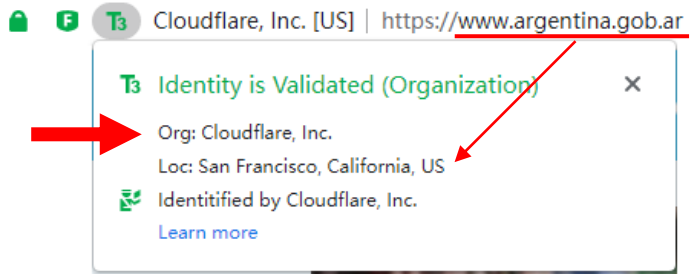


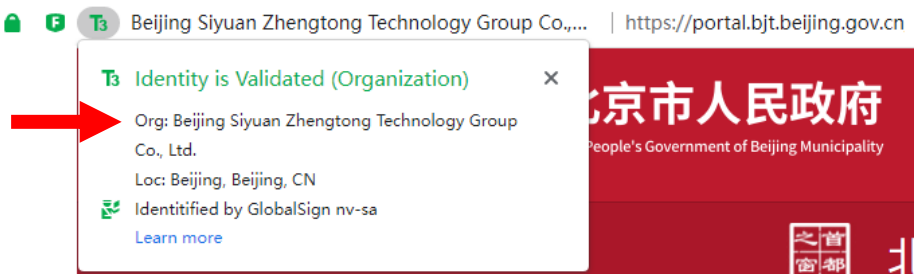




ZT Browser display the O field info in the address bar


# Website identity mismatch case study



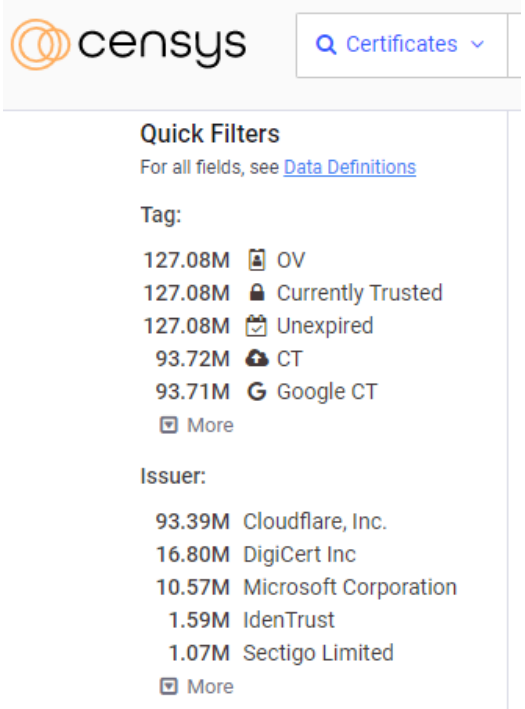


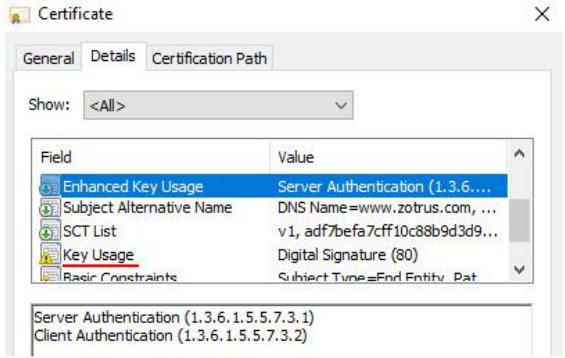


# Why so many website identity mismatched?

- There are many websites identity that are not matched with its real identity, not just government website. all certificates issued by Cloudflare (**93.39M**) O field name is Cloudflare, Inc.
- Are these identity mismatched certificates violate BR?
- Maybe NOT, the company provided the proof documents and validated the .gov domain control, then CA issued the certificate.
- So, **how we can improve it and solve this problem?**



# Re-think the SSL certificate function – Prove identity

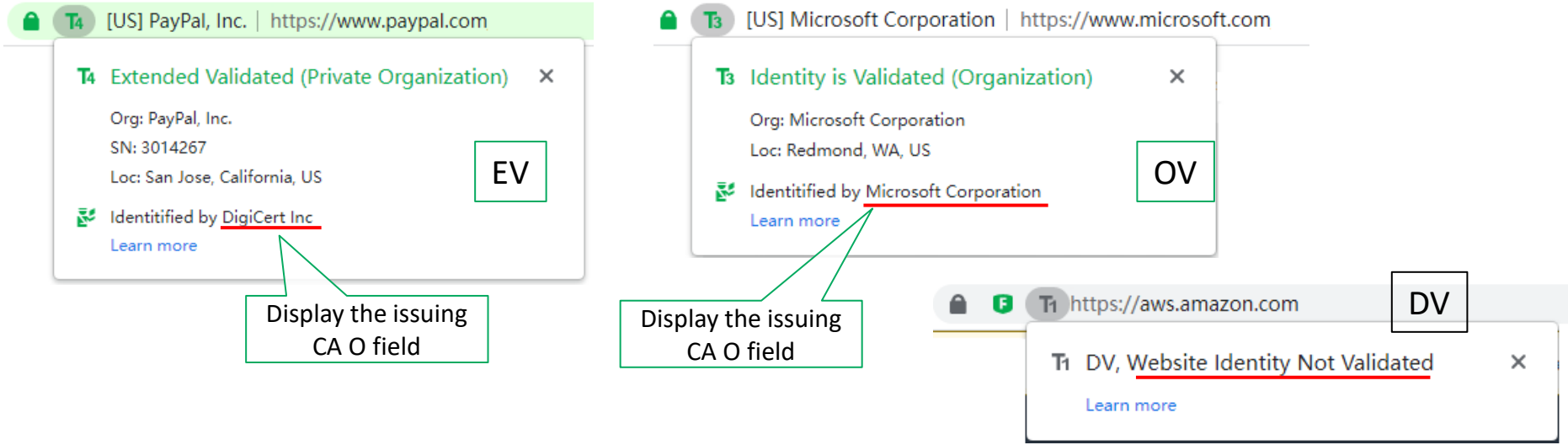

- According to the latest CT log data, DV SSL certificates have accounted for 85% of all SSL certificate, this means SSL certificate is no longer a certification of website identity!
- Why so many website installed a mismatched identity certificate is because no one care about the SSL certificate identity function.
- More mismatch certificate issued, more customer don't like to buy OV SSL and EV SSL certificate. Is it good for CA industry? Is it good for global Internet security?
- **NO! We must do something to make change!**

# Possible solutions for CA/B Forum discussing

- Double check the *.gov.** domain applicant identity if it is a government agency, if it is a company, CA operator must reject and ask for providing government entity proof document.
- ……

# ZoTrus solution – ZT Browser

Display the OV SSL and EV SSL certificate identity info in the address bar. For EV SSL, green address bar and T4 trust icon. For OV SSL, white address bar and T3 trust icon. For DV SSL, gray address bar and T1 icon.



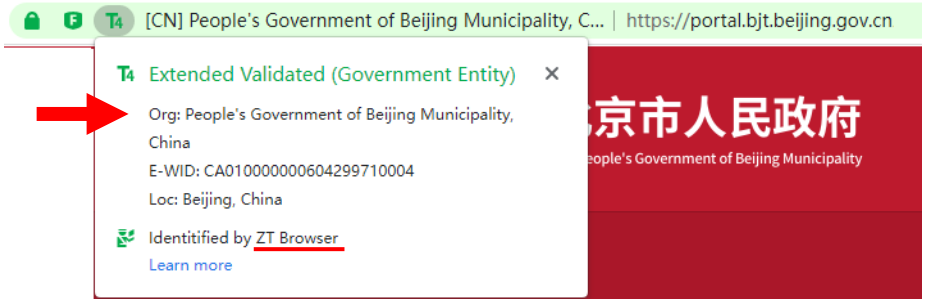
# ZoTrus solution – ZT Browser

To solve the mismatched websites, ZT Browser display its identity info preferentially based on ZoTrus Website Trusted Identity Database, not based on the certificate O field, so the identity of the government website is displayed correctly.


# ZoTrus solution – ZT Browser

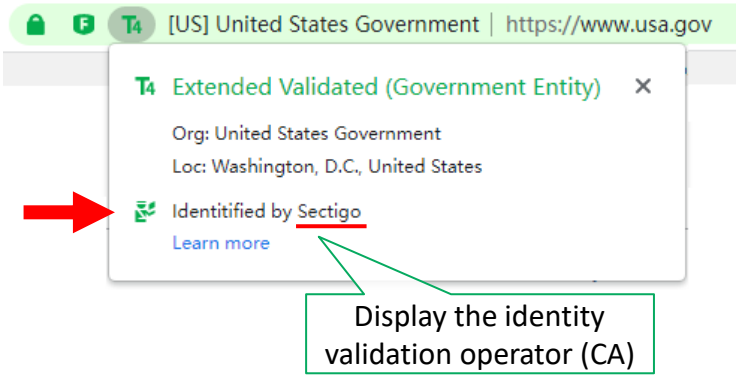
To solve the mismatched websites, ZT Browser display its identity info preferentially based on ZoTrus Website Trusted Identity Database, not based on the certificate O field, so the identity of the government website is displayed correctly.



# ZoTrus solution – ZT Browser

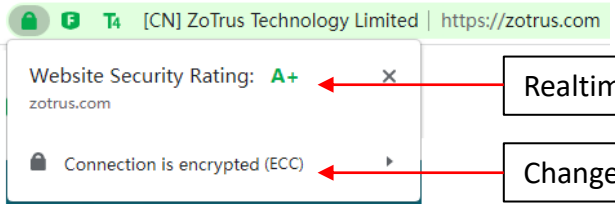
For DV SSL certificate without identity, ZoTrus Website Trusted Identity Validation Service provide validation service that the OV Certified and EV Certified website identity will display like OV SSL and EV SSL deployed, no matter the website deployed a DV SSL. The website identity can be done by CA or by ZT Browser. All ZT Browser trusted CA can post the validated website identity info to ZoTrus Website Trusted Identity Database for green bar displaying.




# ZT Browser other features

Website Security
100%

- https encryption
  60%
- WAF protection
  20%
- Trusted Identity
  20%




Realtime security test rating

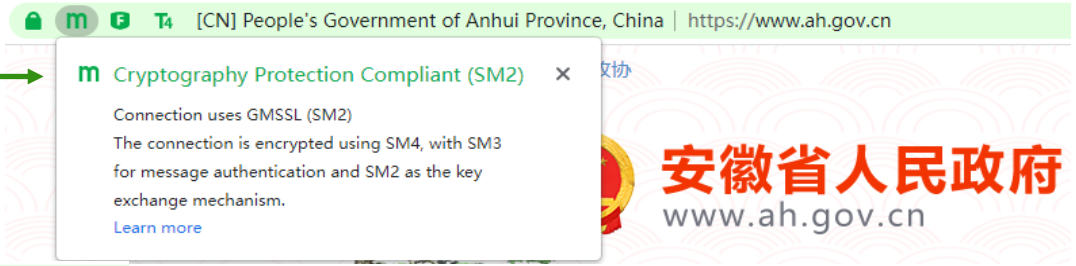
Change displaying “secure” to “encrypted”

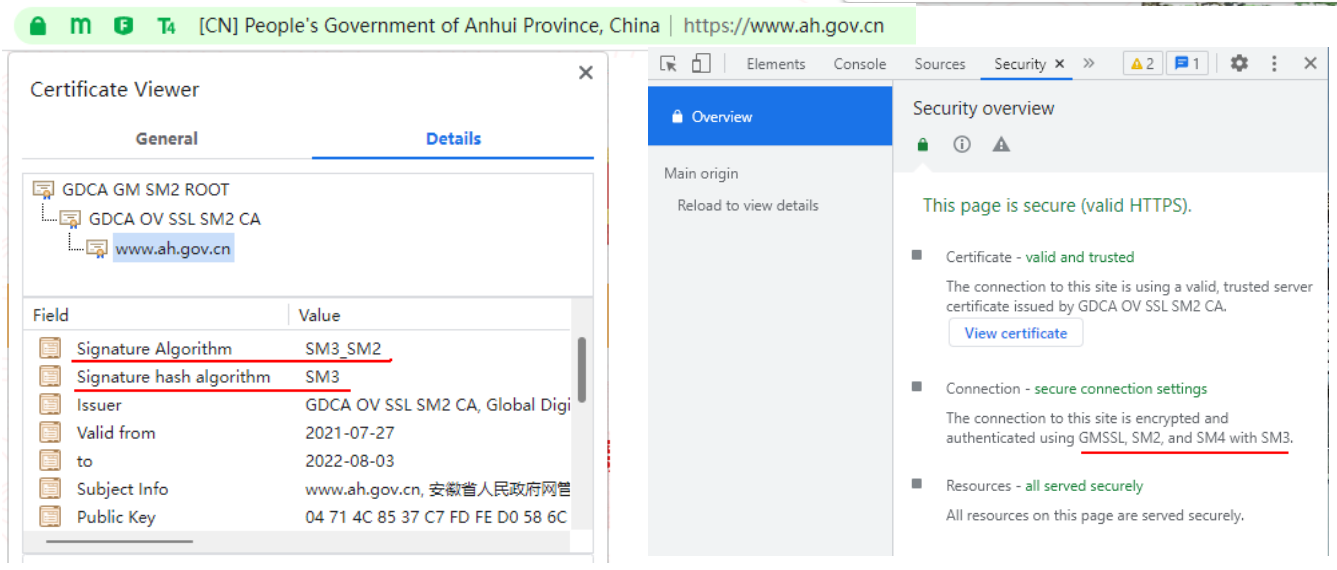

No WAF protection, no security


No validated identity, no security

# ZT Browser other features

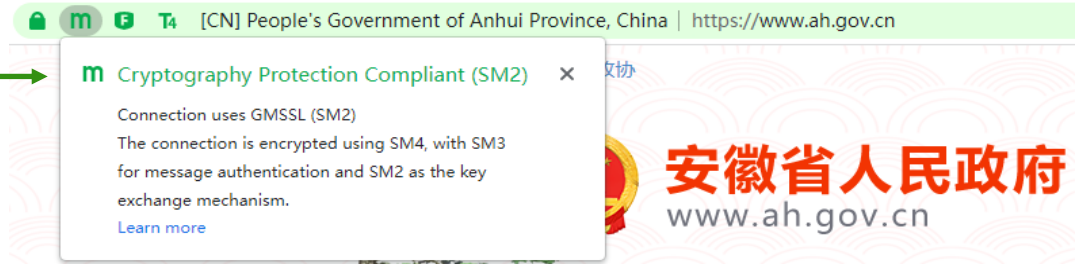
Special for China market
- SM2 algorithm support

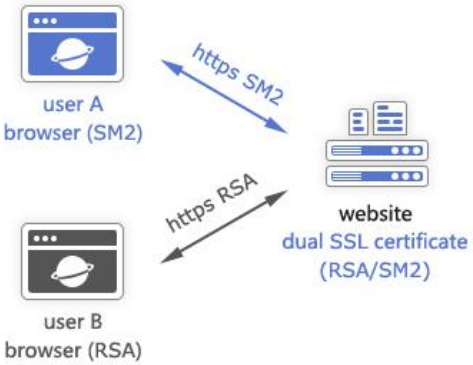


# ZT Browser other features

Special for China market
- SM2 algorithm support




Currently, in order to support all browsers, the website installed dual SSL certificate for RSA/SM2 algorithm auto-adaption.

**Question for CA/B Forum:**
When SM2 SSL certificate can be included in the BR?
SM2/SM3/SM4 is included in ISO/IEC14888-3/AMD1.

# ZoTrus Trusted Root Program

https://ztbrowser.com/trust-root-program.html

- All RSA/ECC algorithm root certificates included in Chromium 97 is trusted as default, but we will change our policy at any time without notice that we may des-include some default roots.
- SM2 algorithm root certificate inclusion applicant must have a valid China CA license issued by MIIT and SCA, must have its own SM2 Root certificate or sub-CA issued by the Chinese SM2 Root CA for issuing SM2 SSL/TLS certificates.
- ZoTrus accepts and removes root certificates as it deems appropriate at its sole discretion. ZoTrus prioritizes root inclusion requests as it deems appropriate at its sole discretion.
- All ZT Browser trusted root CA operators are qualified to provide ZT Browser trusted Website Trusted Identity Validation service. ZT Browser not only display the validation level of the SSL certificate issued by trusted CA for free, but also trust its website validation data that the CA operators are qualified to synchronize to the trusted website data to ZoTrus Trusted Website Database, and ZT Browser will also display its validation level in the address bar for free.