



OV SSL/EV SSL Certificate 0 Field Mistakes Found and Solution

ZoTrus Technology Limited

Richard Wang (richard@zotrus.com)

2022.06.03

A vertical image on the left side of the slide shows a desk setup. At the top left is a small potted succulent in a white hexagonal pot. Below it is a white folder. In the center is a laptop with a keyboard visible. To the right of the laptop are several papers pinned to a light blue wall. One paper features a line graph, a pie chart, and a mail icon. Another paper shows gears and a dollar sign. A third paper has a bar chart. The word 'CONTENTS' is overlaid in white capital letters on a grey rectangular background across the middle of the image.

CONTENTS

01 Website Identity Mismatch Case Study

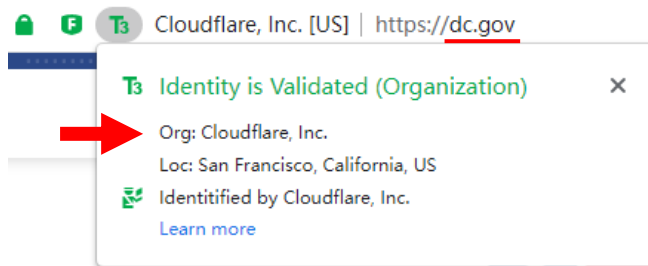
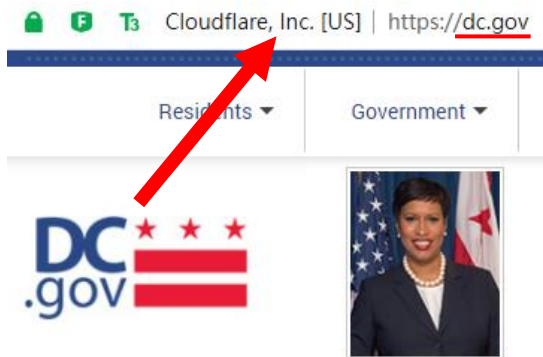
02 Find the Reason

03 Give Solution

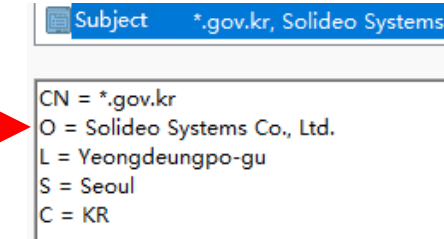
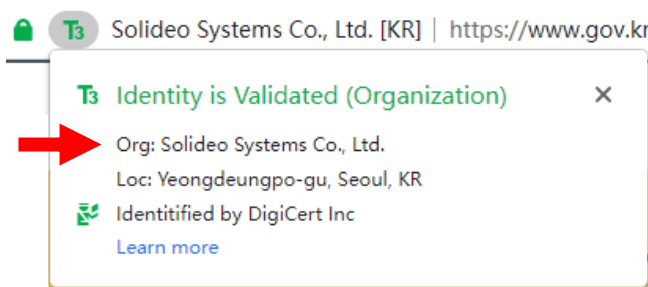
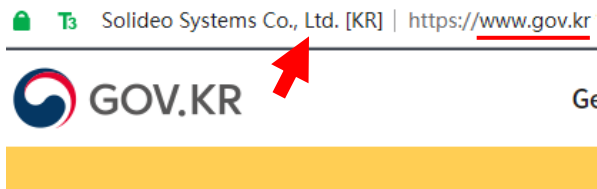
04 ZT Browser Introduction



Website identity mismatch case study



ZT Browser display the O field info in the address bar





Website identity mismatch case study

Cloudflare, Inc. [US] | <https://www.argentina.gob.ar>

Argentina.gov.ar

Beijing Siyuan Zhengtong Technology Group Co.,... | <https://portal.bjt.beijing.gov.cn>

北京市人民政府
The People's Government of Beijing Municipality

Cloudflare, Inc. [US] | <https://www.argentina.gob.ar>

Identity is Validated (Organization)

Org: Cloudflare, Inc.
Loc: San Francisco, California, US
Identified by Cloudflare, Inc.
[Learn more](#)

Beijing Siyuan Zhengtong Technology Group Co.,... | <https://portal.bjt.beijing.gov.cn>

Identity is Validated (Organization)

Org: Beijing Siyuan Zhengtong Technology Group Co., Ltd.
Loc: Beijing, Beijing, CN
Identified by GlobalSign nv-sa
[Learn more](#)

Subject: argentina.gob.ar, Cloudflare,

CN = argentina.gob.ar
O = Cloudflare, Inc.
L = San Francisco
S = California
C = US

Subject: portal.bjt.beijing.gov.cn, Beijing Siyuan Zhe

CN = portal.bjt.beijing.gov.cn
O = Beijing Siyuan Zhengtong Technology Group Co., Ltd.
L = Beijing
S = Beijing
C = CN



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?**

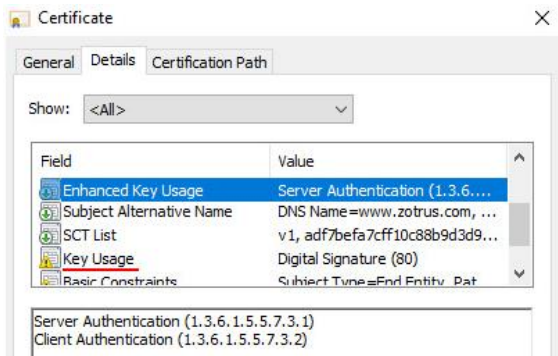
A screenshot of the Censys Certificates search interface. The header shows the Censys logo and a search bar with the text 'Certificates'. Below the header, there are 'Quick Filters' for various certificate attributes. The 'Tag' section lists: 127.08M OV, 127.08M Currently Trusted, 127.08M Unexpired, 93.72M CT, 93.71M Google CT, and a 'More' link. The 'Issuer' section lists: 93.39M Cloudflare, Inc., 16.80M DigiCert Inc, 10.57M Microsoft Corporation, 1.59M IdenTrust, 1.07M Sectigo Limited, and a 'More' link.

Tag	Count
OV	127.08M
Currently Trusted	127.08M
Unexpired	127.08M
CT	93.72M
Google CT	93.71M
More	

Issuer	Count
Cloudflare, Inc.	93.39M
DigiCert Inc	16.80M
Microsoft Corporation	10.57M
IdenTrust	1.59M
Sectigo Limited	1.07M
More	



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.

T4 [US] PayPal, Inc. | https://www.paypal.com

T4 Extended Validated (Private Organization) x

Org: PayPal, Inc.
SN: 3014267
Loc: San Jose, California, US

Identified by DigiCert Inc
[Learn more](#)

EV

Display the issuing
CA O field

T3 [US] Microsoft Corporation | https://www.microsoft.com

T3 Identity is Validated (Organization) x

Org: Microsoft Corporation
Loc: Redmond, WA, US

Identified by Microsoft Corporation
[Learn more](#)

OV

Display the issuing
CA O field

T1 https://aws.amazon.com

T1 DV, Website Identity Not Validated x

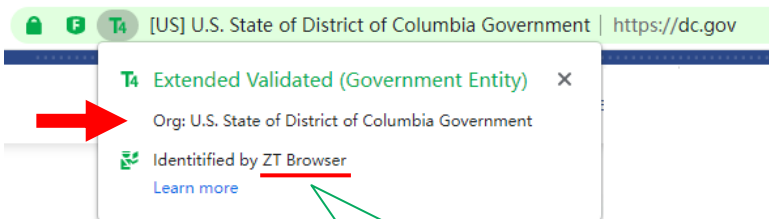
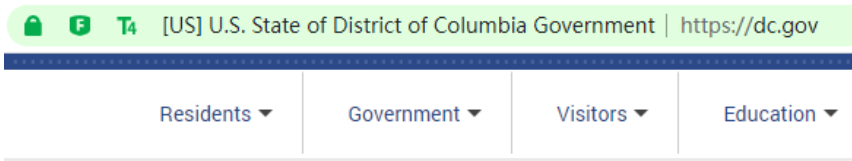
[Learn more](#)

DV

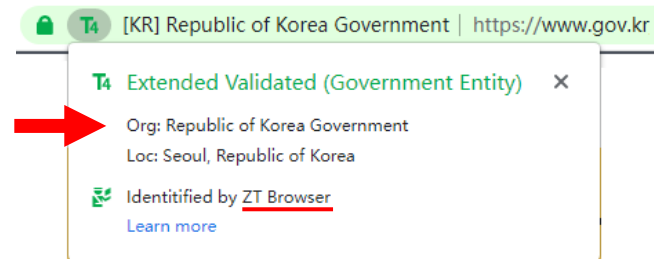


ZoTrus solution – ZT Browser

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.



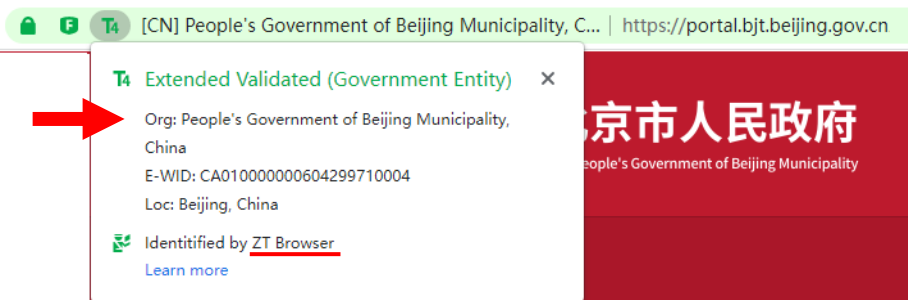
Display the identity validation operator





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.

[US] United States Government | https://www.usa.gov

Extended Validated (Government Entity) x

Org: United States Government
Loc: Washington, D.C., United States

Identified by Sectigo
[Learn more](#)

Display the identity validation operator (CA)

[CN] China Government | https://www.gov.cn

Extended Validated (Government Entity) x

Org: China Government
Loc: Beijing, China

Identified by ZT Browser
[Learn more](#)

Display the identity validation operator (ZoTrus)



ZT Browser other features

Website Security

100%

https encryption

60%

WAF protection

20%

Trusted Identity

20%

[CN] ZoTrus Technology Limited | https://zotrus.com

Website Security Rating: **A+**

zotrus.com

Connection is encrypted (ECC)

Realtime security test rating

Change displaying "secure" to "encrypted"

[CN] ZoTrus Technology Limited | https://ztbrowser.com

Cloud WAF Security Protection

Provided by Cloudflare Cloud WAF

Learn more

No WAF protection, no security

[CN] ZoTrus Technology Limited | https://ztbrowser.com

Extended Validated (Private Organization)

Org: ZoTrus Technology Limited

SN: 91440300MA5GY4X4XH

Loc: Shenzhen, China

Identified by ZT Browser

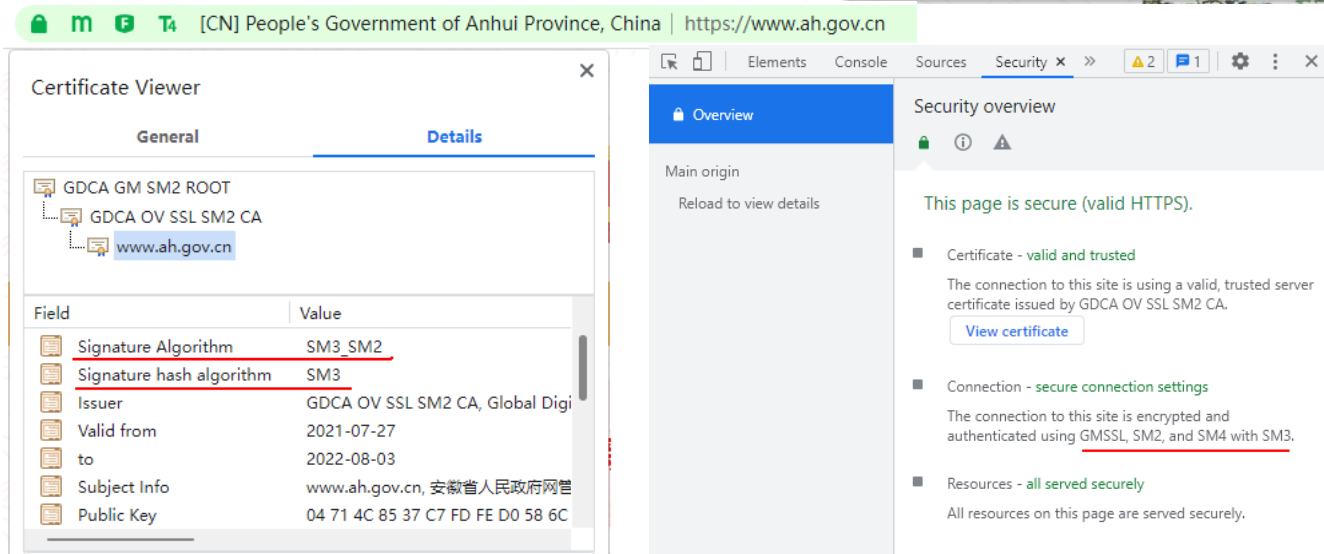
Learn more

No validated identity, no security



ZT Browser other features

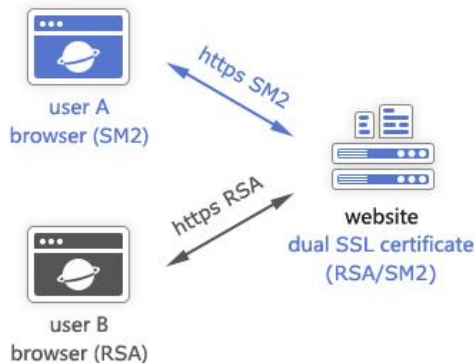
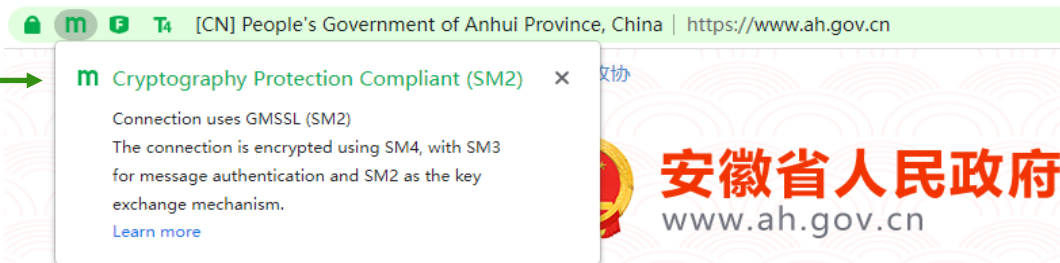
Special for China market
- SM2 algorithm support





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-adaptation.

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.