Certificate Transparency

Trust Services Forum - CA Day 2019

Ryan Sleevi / sleevi@google.com

Agenda

- What is Certificate Transparency?
- Status in Browsers
- Use by Certificate Authorities
- Real World Certificate Transparency
- Certificate Transparency for CABs
- Non-TLS Certificates and CT

What is Certificate Transparency?

CT as a Technology

- Defined in RFC 6962
- Cryptographically-verifiable, append-only, auditable log of issued certificates
  - A ledger
  - A blockchain
  - A database
  - An audit log
- Protocol for recording and reviewing certificate issuance practices

CT as an Ecosystem

- Not a single ecosystem, but many ecosystems, some overlapping, each serving different needs
- Key Participants:
    - CAs
    - Logs
    - Compliance Checkers

CT in the Web's PKIs

- >30 public, world-readable/writable logs, from 4 different operators
    - Constantly adding more
- Contain TLS server certificates intended to be used in various Web browsers
- **Important**: Any data in a TLS certificate trusted by a browser is treated as public data

Status in Browsers

Status in Browsers

Google Chrome

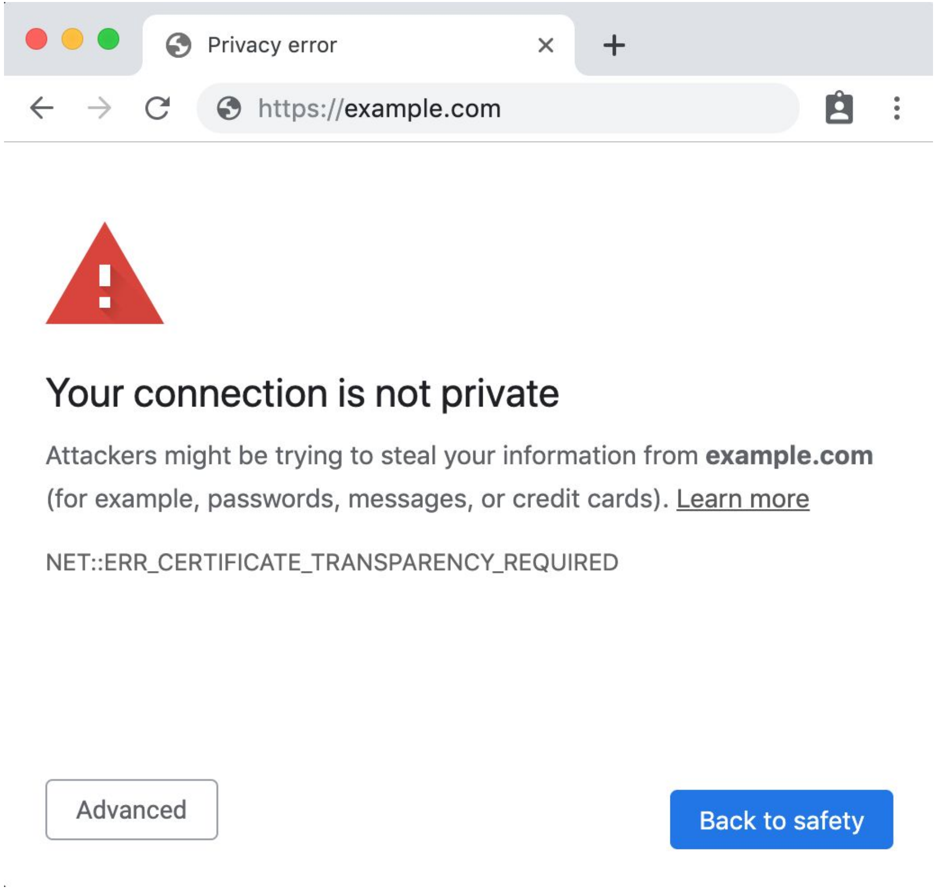
Google Chrome requires that all Extended Validation (EV) certificates issued after 1 Jan 2015 be CT Qualified in order to be recognized as EV, and that all publicly-trusted TLS certificates issued after 30 April 2018 be CT Qualified in order to be recognized as valid.

- *Certificate Transparency in Chrome*

Apple

Publicly trusted Transport Layer Security (TLS) server authentication certificates issued after October 15, 2018 must meet Apple's Certificate Transparency (CT) policy to be evaluated as trusted on Apple platforms.

- *Apple’s Certificate Transparency Policy*



Your connection is not private

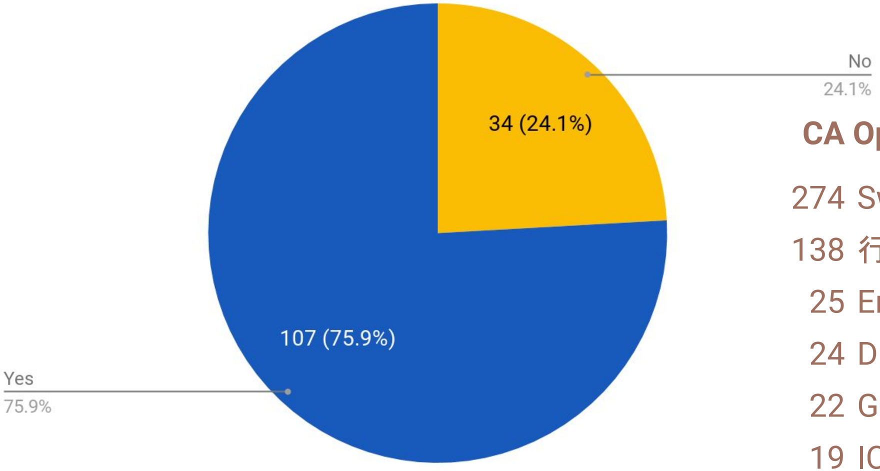
Attackers might be trying to steal your information from **example.com** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERTIFICATE_TRANSPARENCY_REQUIRED

Use by Certificate Authorities

Certificates issued May 2018, measured July 2018

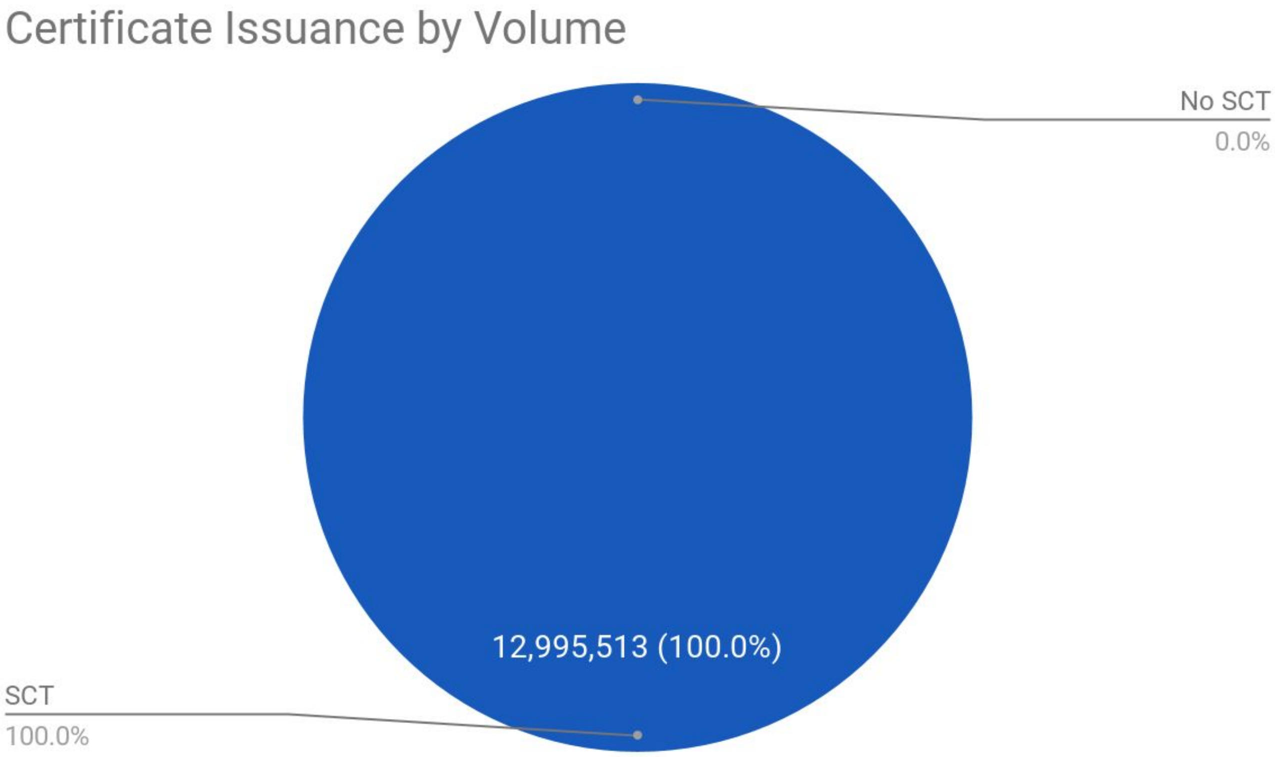
CAs with >1 Non-Compliant Certificate



CA Operators where not all certs have SCTS:

274	SwissSign AG
138	行政院 (Taiwan GRCA)
25	Entrust, Inc.
24	DigiCert Inc
22	Government of Korea
19	ICP-Brasil
18	Dreamcommerce S.A.
17	Unizeto Technologies S.A.
16	NetLock Kft.
11	GlobalSign nv-sa
7	Microsoft Corporation
7	MULTICERT
7	T-Systems International GmbH
5	SCEE
4	Amazon
3	Deutsche Post
3	certSIGN
2	Entrust
2	QuoVadis Limited
2	U.S. Government
2	Southern Company Services, Inc.
1	...12 more...

Certificates issued May 2018, measured July 2018



> “We find that CT has so far been widely adopted with minimal breakage and warnings.”

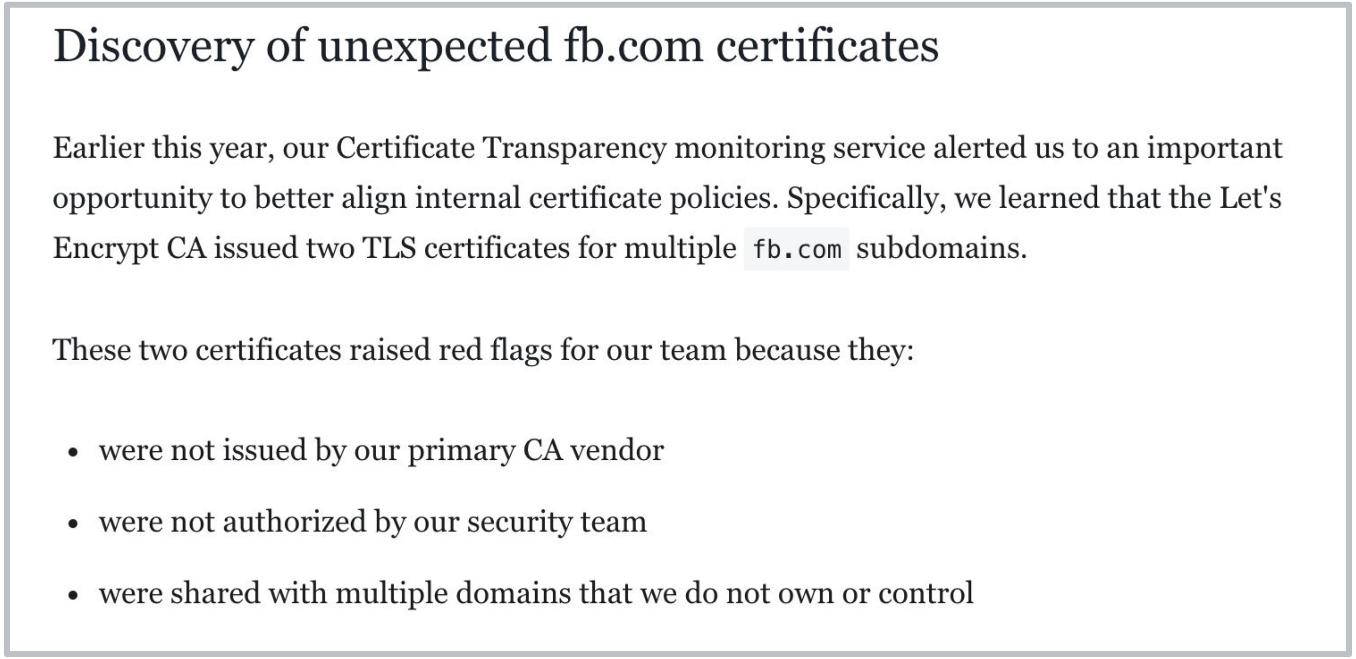
[Does Certificate Transparency Break the Web? Measuring Adoption and Error Rate]()

Proceedings of the IEEE Symposium on Security & Privacy (2019)

Real World Certificate Transparency

Detect Unauthorized Certificates

Facebook



Discovery of unexpected fb.com certificates

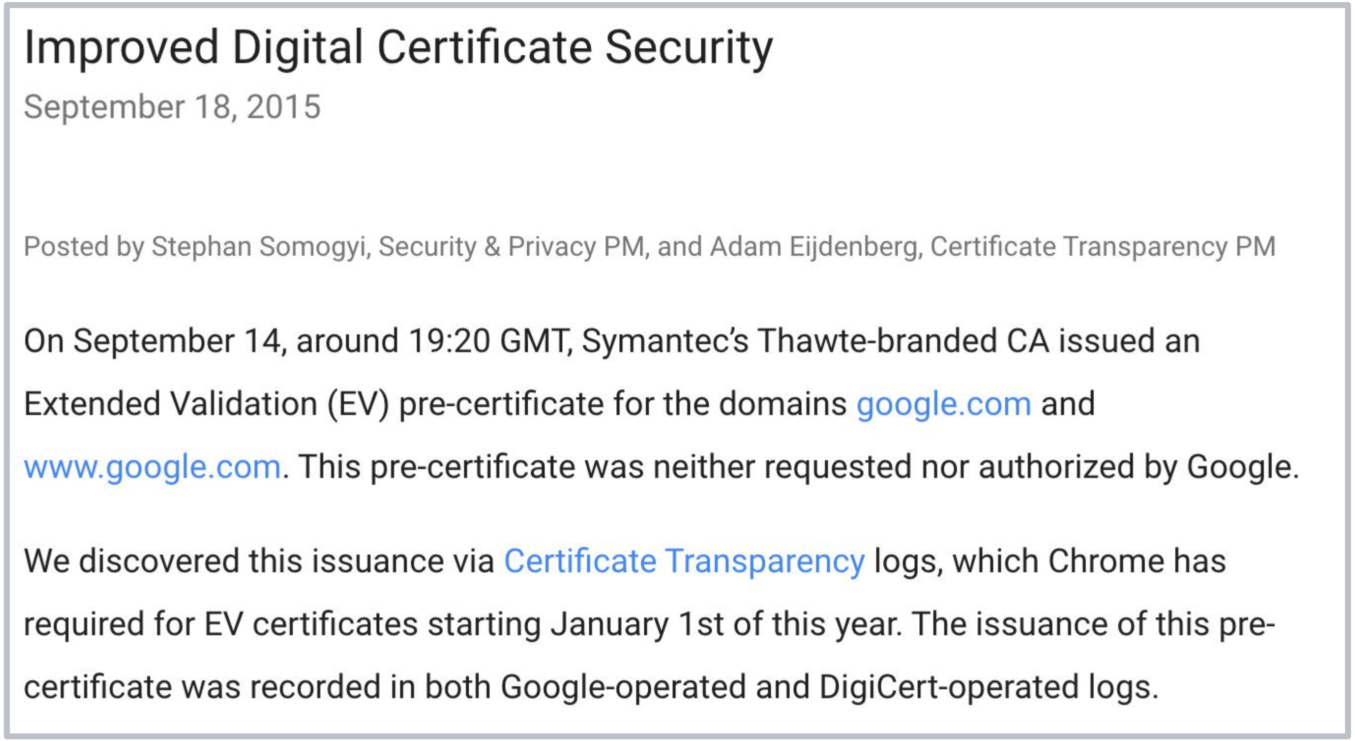
Earlier this year, our Certificate Transparency monitoring service alerted us to an important opportunity to better align internal certificate policies. Specifically, we learned that the Let's Encrypt CA issued two TLS certificates for multiple `fb.com` subdomains.

These two certificates raised red flags for our team because they:

- were not issued by our primary CA vendor
- were not authorized by our security team
- were shared with multiple domains that we do not own or control

Source: Early Impacts of Certificate Transparency, facebook.com

Google



Improved Digital Certificate Security

September 18, 2015

Posted by Stephan Somogyi, Security & Privacy PM, and Adam Eijdenberg, Certificate Transparency PM

On September 14, around 19:20 GMT, Symantec's Thawte-branded CA issued an Extended Validation (EV) pre-certificate for the domains google.com and www.google.com. This pre-certificate was neither requested nor authorized by Google.

We discovered this issuance via Certificate Transparency logs, which Chrome has required for EV certificates starting January 1st of this year. The issuance of this pre-certificate was recorded in both Google-operated and DigiCert-operated logs.

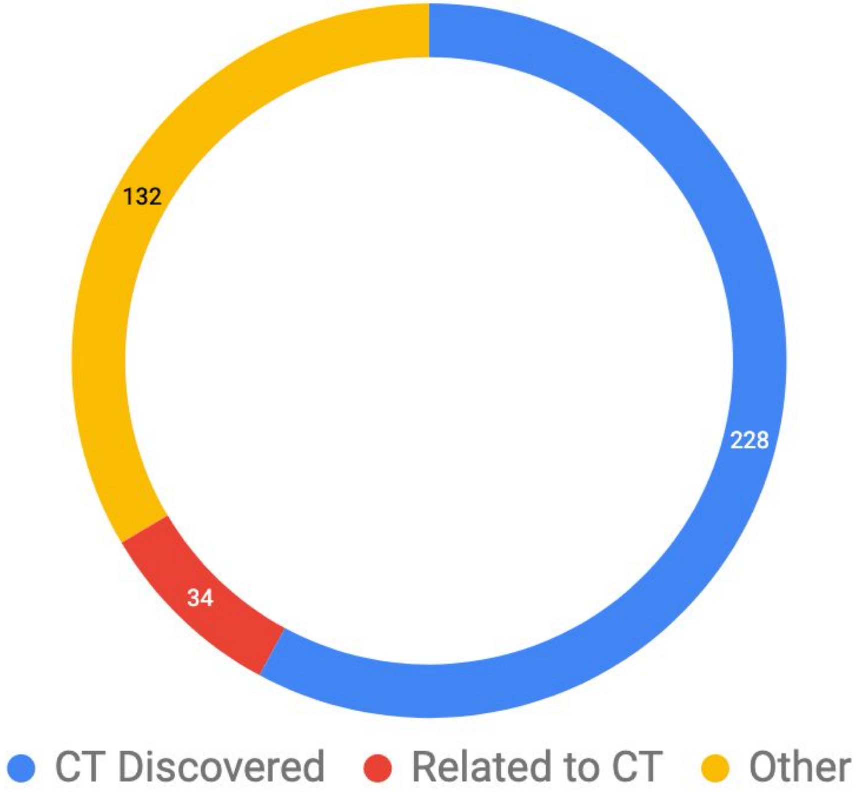
Source: Improved Digital Certificate Security, security.googleblog.com

Detect Problematic Certificates

Problematic Certificates

- Don’t follow the Certification Practices Statement
- Don’t follow the Certificate Profile
- Don’t follow the Trust Framework Requirements
  - Root Program Requirements
  - Audit Criteria (WebTrust, ETSI ESI)
  - IETF RFCs
- Don’t have the required services (OCSP, CRL, AIA, CP/CPS)

Bugzilla CA Incidents - 2016-01-01 to 2019-09-18



Google

Open Source Problem Detection

CT Search Engines

Censys: Startup spun out of the University of Michigan. A search engine for data from Internet-wide crawls that also incorporates CT Data. From the research team that developed ZLint

crt.sh: From Sectigo, an open-source search engine for Certificate Transparency that also has the ability to execute linters as certificates are found.

Linters

certlint: Developed and open-sourced by Amazon, a C + Ruby linter that compiles the ASN.1 modules to ensure valid DER, as well as CA/Browser Forum-specific checks

ZLint: Developed as part of research at the University of Michigan into problematic certificates, performs comprehensive checks against the policy requirements of the Baseline Requirements.

Internet Scale Search

+

Automated Testing Tools

=

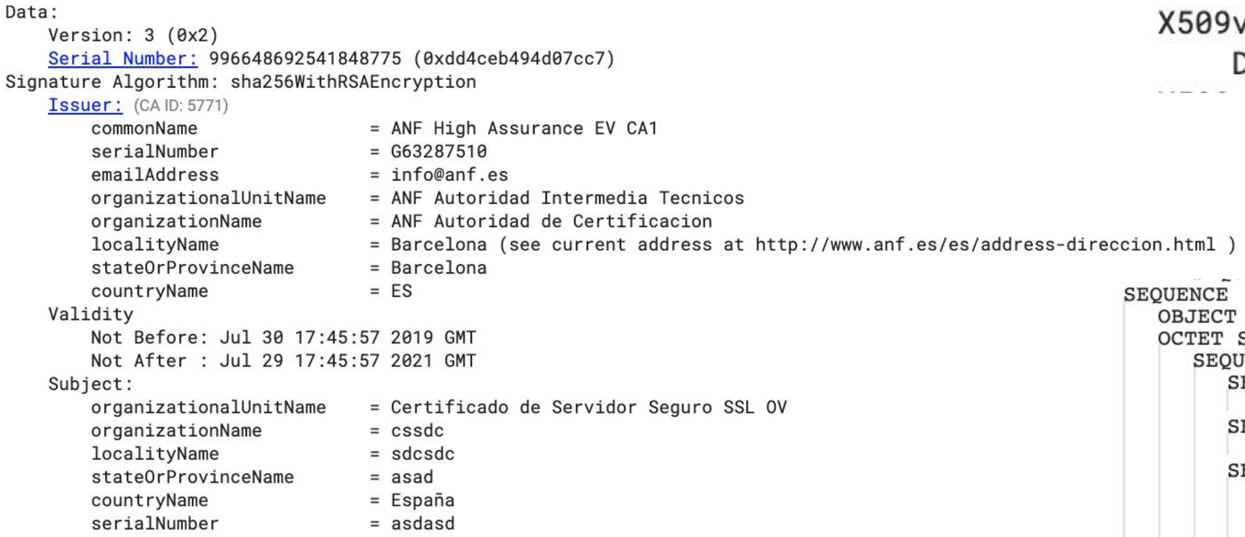
Internet Scale Compliance Issues

Certificate Transparency for CABs

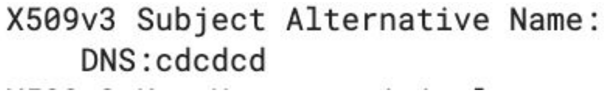
Certificate Transparency = 100% Sampling

Linters = Test Suites

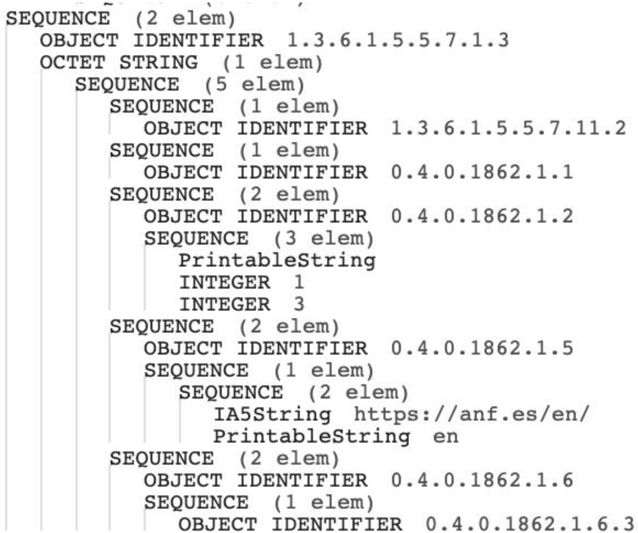
Example of a Problematic Cert



```
Data:
    Version: 3 (0x2)
    Serial Number: 996648692541848775 (0xdd4ceb494d07cc7)
Signature Algorithm: sha256WithRSAEncryption
    Issuer: (CA ID: 5771)
        commonName                = ANF High Assurance EV CA1
        serialNumber              = G63287510
        emailAddress              = info@anf.es
        organizationalUnitName    = ANF Autoridad Intermedia Tecnicos
        organizationName          = ANF Autoridad de Certificacion
        localityName              = Barcelona (see current address at http://www.anf.es/es/address-direccion.html )
        stateOrProvinceName       = Barcelona
        countryName               = ES
    Validity
        Not Before: Jul 30 17:45:57 2019 GMT
        Not After : Jul 29 17:45:57 2021 GMT
    Subject:
        organizationalUnitName    = Certificado de Servidor Seguro SSL OV
        organizationName          = cssdc
        localityName              = sdcsdc
        stateOrProvinceName       = asad
        countryName               = España
        serialNumber              = asdasd
```



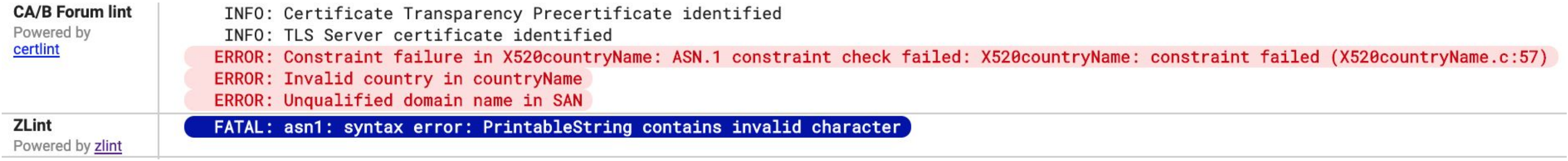
```
X509v3 Subject Alternative Name:
    DNS:cdcdcd
```



```
SEQUENCE (2 elem)
  OBJECT IDENTIFIER 1.3.6.1.5.5.7.1.3
  OCTET STRING (1 elem)
    SEQUENCE (5 elem)
      SEQUENCE (1 elem)
        OBJECT IDENTIFIER 1.3.6.1.5.5.7.11.2
      SEQUENCE (1 elem)
        OBJECT IDENTIFIER 0.4.0.1862.1.1
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 0.4.0.1862.1.2
        SEQUENCE (3 elem)
          PrintableString
          INTEGER 1
          INTEGER 3
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 0.4.0.1862.1.5
        SEQUENCE (1 elem)
          SEQUENCE (2 elem)
            IA5String https://anf.es/en/
            PrintableString en
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 0.4.0.1862.1.6
        SEQUENCE (1 elem)
          OBJECT IDENTIFIER 0.4.0.1862.1.6.3
```

Source: https://crt.sh/?id=1723124144

All Systems Lint



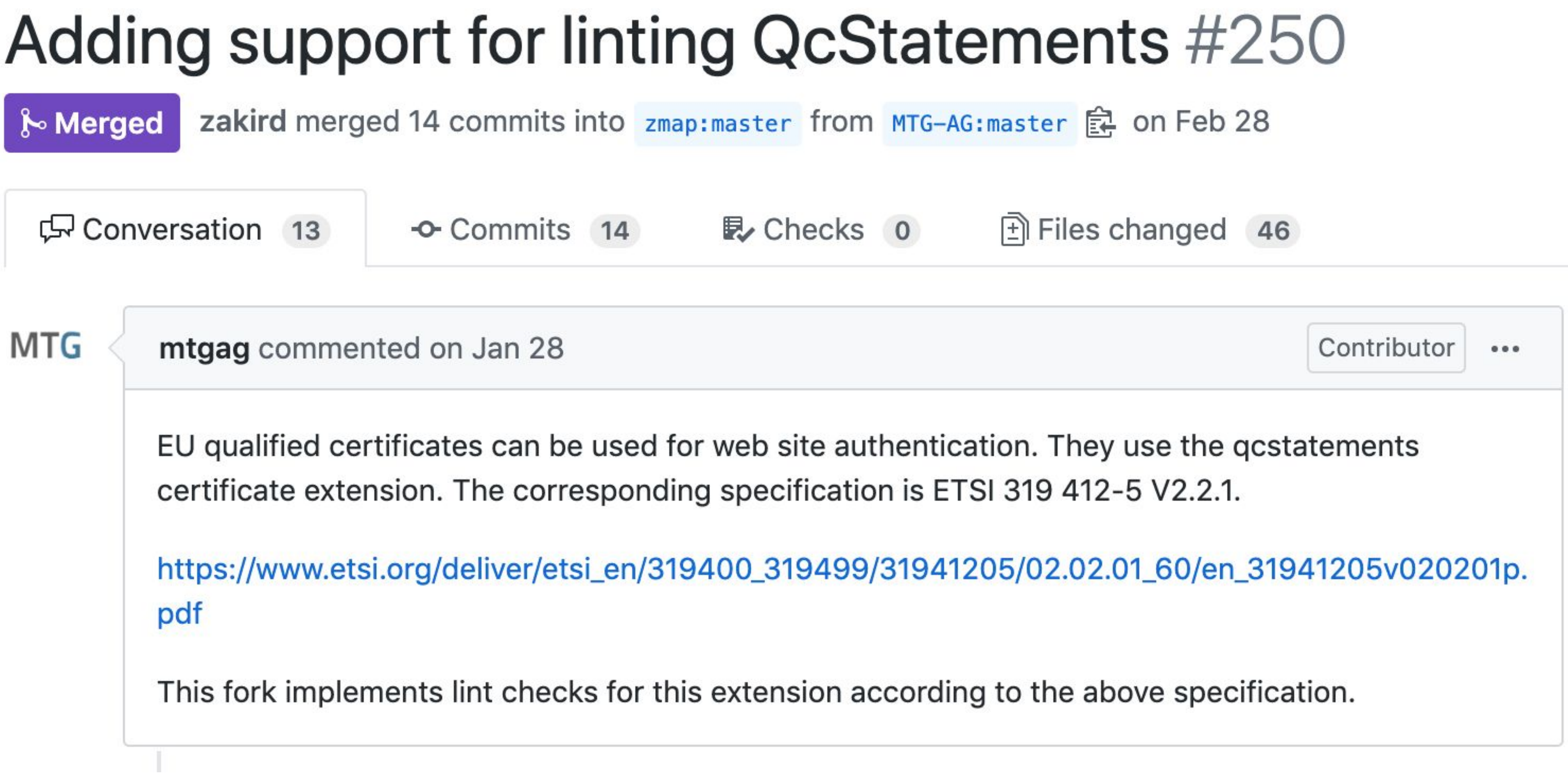
CA/B Forum lint
Powered by certlint

```
 INFO: Certificate Transparency Precertificate identified
 INFO: TLS Server certificate identified
ERROR: Constraint failure in X520countryName: ASN.1 constraint check failed: X520countryName: constraint failed (X520countryName.c:57)
ERROR: Invalid country in countryName
ERROR: Unqualified domain name in SAN
```

ZLint
Powered by zlint

```
FATAL: asn1: syntax error: PrintableString contains invalid character
```

Test for Failure as well as Success



Adding support for linting QcStatements #250

zakird merged 14 commits into `zmap:master` from `MTG-AG:master` on Feb 28

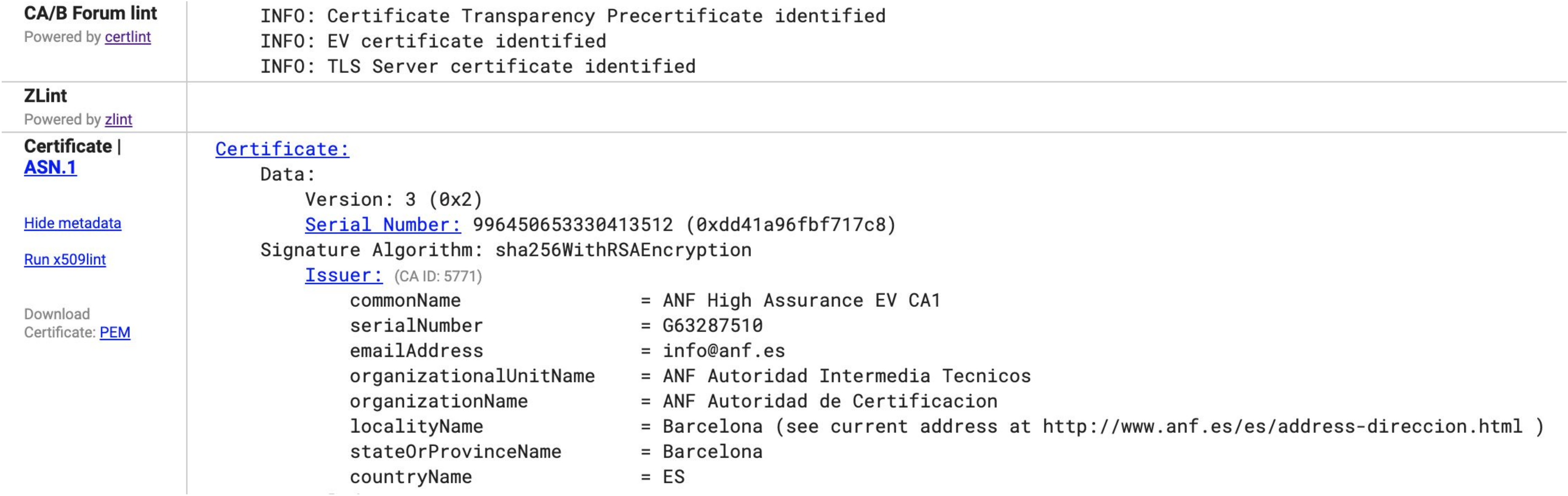
mtgag commented on Jan 28

EU qualified certificates can be used for web site authentication. They use the qcstatements certificate extension. The corresponding specification is ETSI 319 412-5 V2.2.1.

https://www.etsi.org/deliver/etsi_en/319400_319499/31941205/02.02.01_60/en_31941205v020201p.pdf

This fork implements lint checks for this extension according to the above specification.

All Tests Pass?



CA/B Forum lint
Powered by certlint

```
INFO: Certificate Transparency Precertificate identified
INFO: EV certificate identified
INFO: TLS Server certificate identified
```

ZLint
Powered by zlint

Certificate | ASN.1

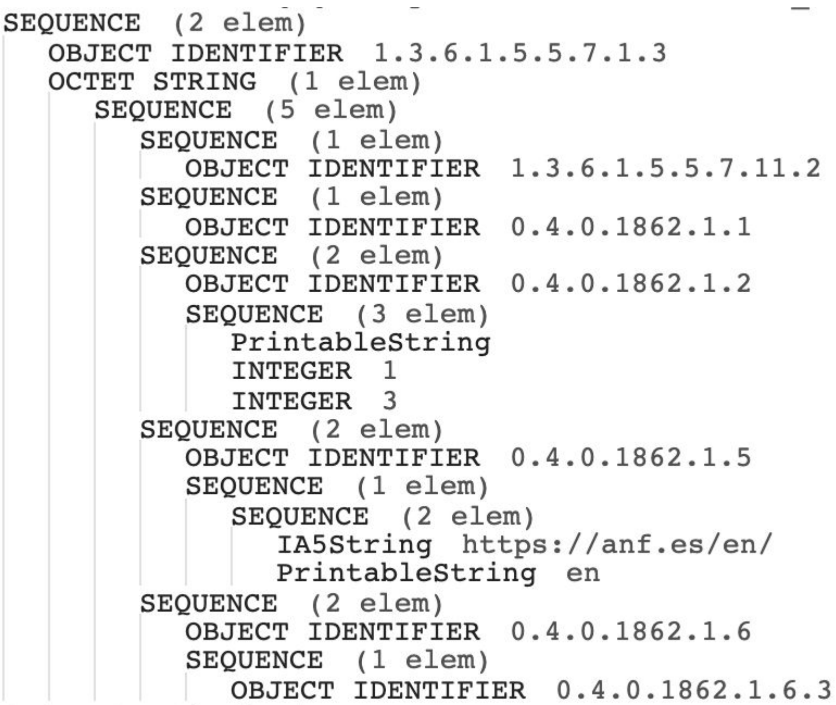
Hide metadata

Run x509lint

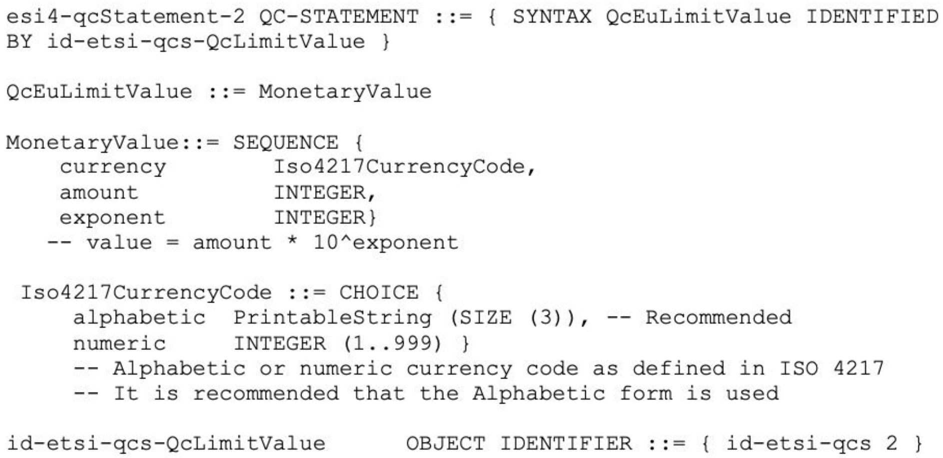
Download Certificate: PEM

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 996450653330413512 (0xdd41a96fbf717c8)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: (CA ID: 5771)
            commonName                = ANF High Assurance EV CA1
            serialNumber              = G63287510
            emailAddress              = info@anf.es
            organizationalUnitName    = ANF Autoridad Intermedia Tecnicos
            organizationName          = ANF Autoridad de Certificacion
            localityName              = Barcelona (see current address at http://www.anf.es/es/address-direccion.html )
            stateOrProvinceName       = Barcelona
            countryName               = ES
```

Not quite

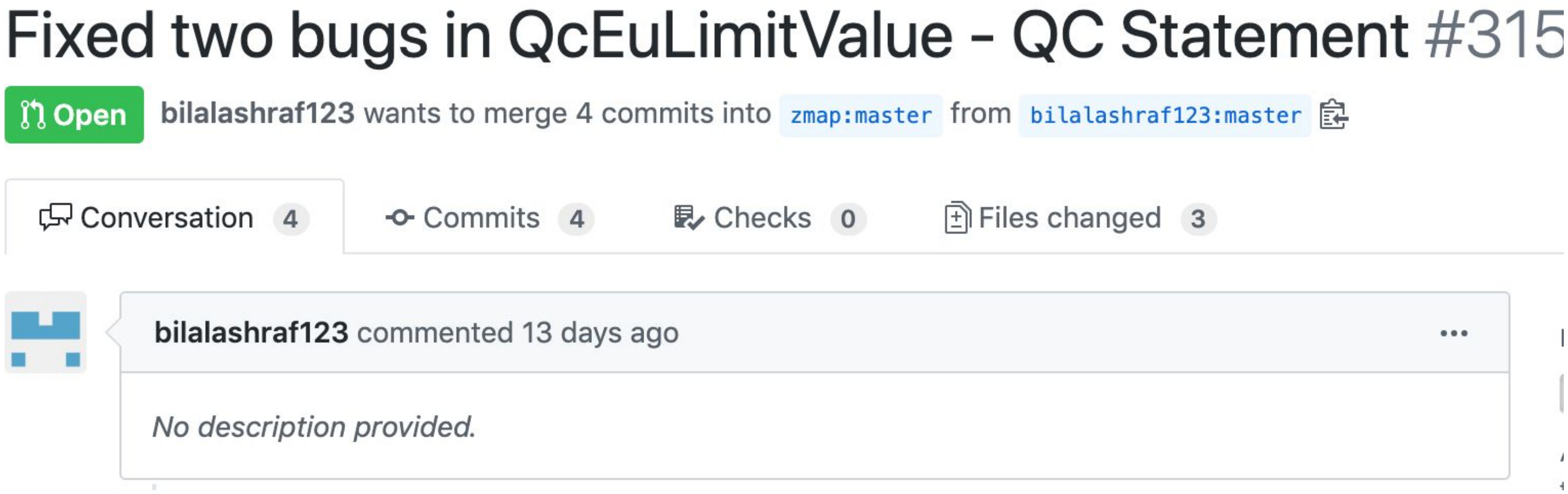


```
SEQUENCE (2 elem)
  OBJECT IDENTIFIER 1.3.6.1.5.5.7.1.3
  OCTET STRING (1 elem)
    SEQUENCE (5 elem)
      SEQUENCE (1 elem)
        OBJECT IDENTIFIER 1.3.6.1.5.5.7.11.2
      SEQUENCE (1 elem)
        OBJECT IDENTIFIER 0.4.0.1862.1.1
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 0.4.0.1862.1.2
        SEQUENCE (3 elem)
          PrintableString
          INTEGER 1
          INTEGER 3
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 0.4.0.1862.1.5
        SEQUENCE (1 elem)
          SEQUENCE (2 elem)
            IA5String https://anf.es/en/
            PrintableString en
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 0.4.0.1862.1.6
        SEQUENCE (1 elem)
          OBJECT IDENTIFIER 0.4.0.1862.1.6.3
```



```
esi4-qcStatement-2 QC-STATEMENT ::= { SYNTAX QcEuLimitValue IDENTIFIED
BY id-etsi-qcs-QcLimitValue }

QcEuLimitValue ::= MonetaryValue

MonetaryValue::= SEQUENCE {
    currency         Iso4217CurrencyCode,
    amount           INTEGER,
    exponent         INTEGER}
   -- value = amount * 10^exponent

 Iso4217CurrencyCode ::= CHOICE {
     alphabetic  PrintableString (SIZE (3)), -- Recommended
     numeric     INTEGER (1..999) }
     -- Alphabetic or numeric currency code as defined in ISO 4217
     -- It is recommended that the Alphabetic form is used

id-etsi-qcs-QcLimitValue      OBJECT IDENTIFIER ::= { id-etsi-qcs 2 }
```

Tests the tests



Fixed two bugs in QcEuLimitValue - QC Statement #315

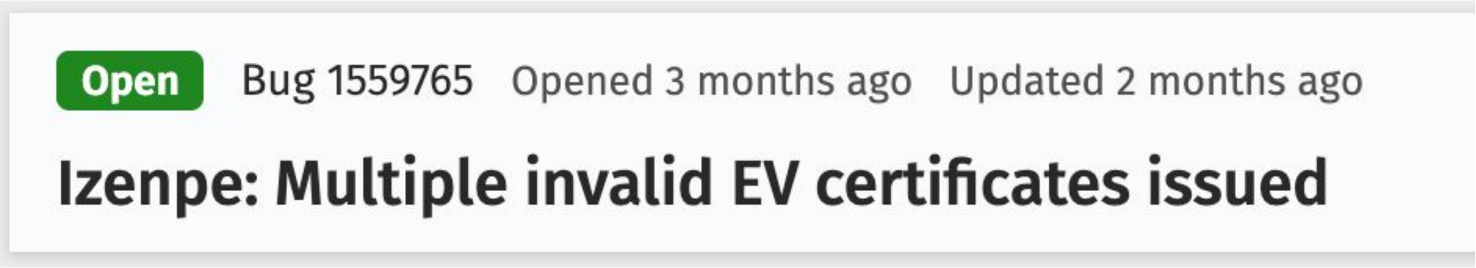
Open bilalashraf123 wants to merge 4 commits into `zmap:master` from `bilalashraf123:master`

bilalashraf123 commented 13 days ago

No description provided.

Test against the CP and CPS

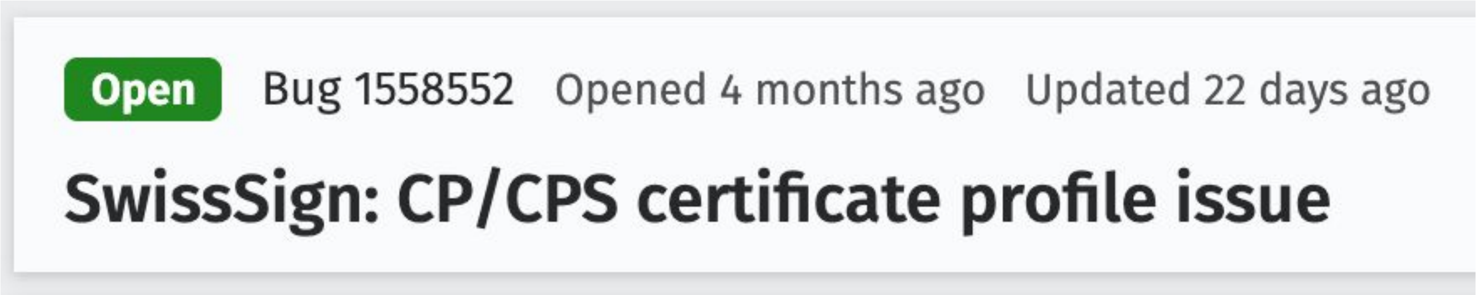
Certificate Profile Misconfiguration



Open Bug 1559765 Opened 3 months ago Updated 2 months ago

Izenpe: Multiple invalid EV certificates issued

Certificate Profile Misconfiguration *(continued)*



Open Bug 1558552 Opened 4 months ago Updated 22 days ago

SwissSign: CP/CPS certificate profile issue

Thanks!