Cryptography Application TLS / SSL

PacNOG19

28th November - 2nd December 2016

Nadi, Fiji

Issue Date: [31-12-2015]

Revision: [V.1]

APNIC

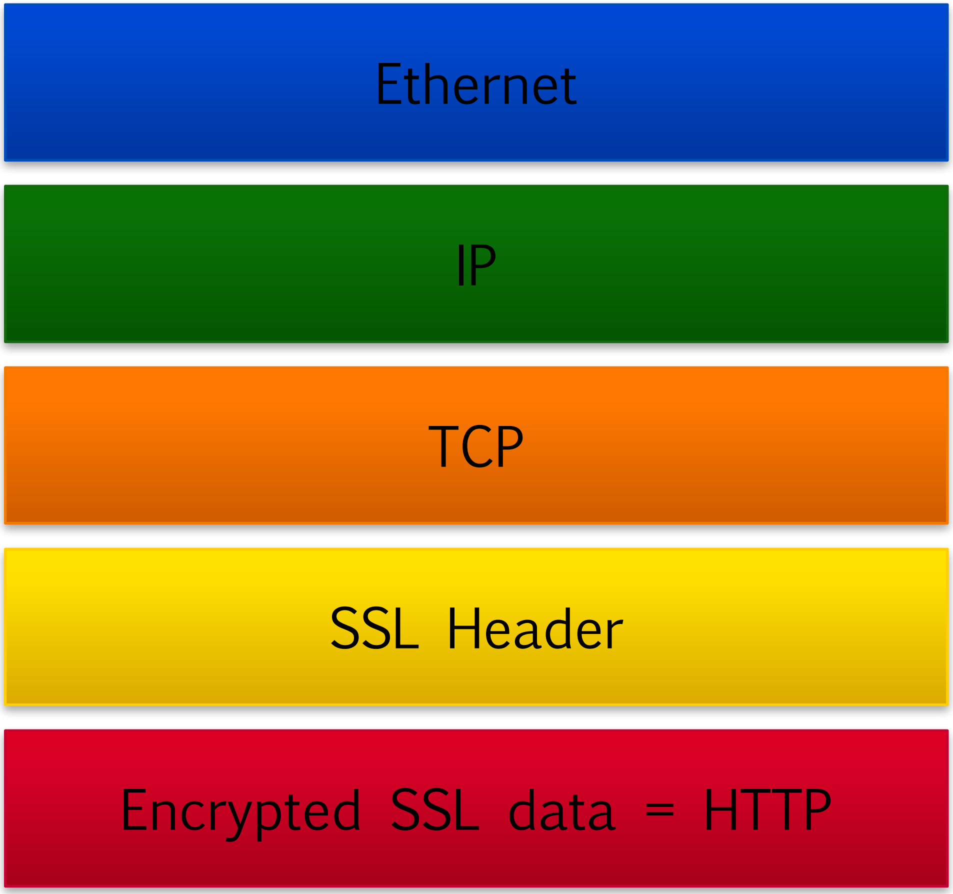
History

- Secure Sockets Layer was developed by Netscape in 1994 as a protocol which permitted persistent and secure transactions.
- In 1997 an Open Source version of Netscape’s patented version was created, which is now OpenSSL.
- In 1999 the existing protocol was extended by a version now known as Transport Layer Security (TLS).
- By convention, the term "SSL" is used even when technically the TLS protocol is being used.

TLS/SSL : What it does

- Encryption
- Integrity
- Authentication

Location of SSL Protocol & TCP Ports



Ethernet

IP

TCP

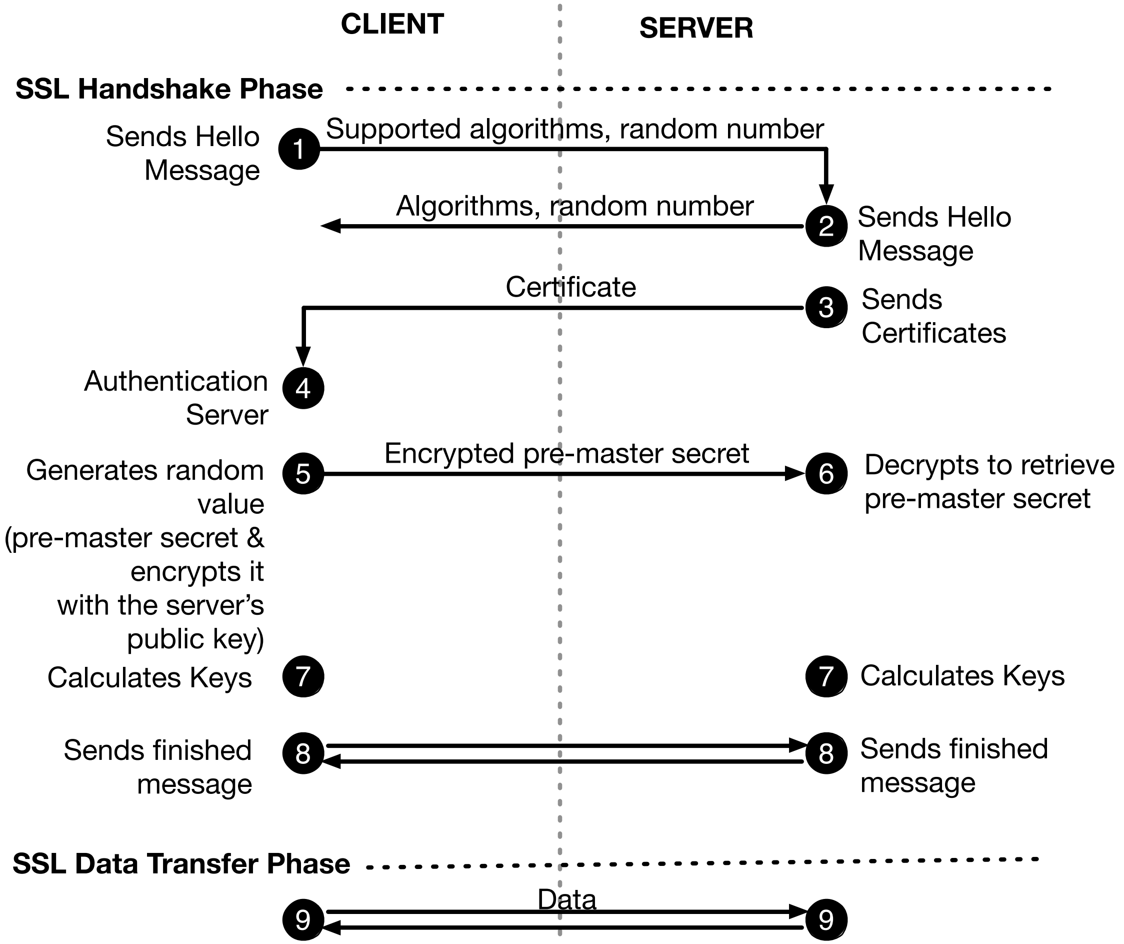
SSL Header

Encrypted SSL data = HTTP

SSL Operations

- Application calls SSL connect routines to set up channel.
- Public Key cryptography is used during handshake to authenticate parties and exchange session key.
- Symmetric Key cryptography (using session key) is used to encrypt data.

How SSL Works



CLIENT

SERVER

SSL Handshake Phase

1 Sends Hello Message

Supported algorithms, random number

2 Sends Hello Message

Algorithms, random number

3 Sends Certificates

Certificate

4 Authentication Server

5 Generates random value (pre-master secret & encrypts it with the server's public key)

Encrypted pre-master secret

6 Decrypts to retrieve pre-master secret

7 Calculates Keys

7 Calculates Keys

8 Sends finished message

8 Sends finished message

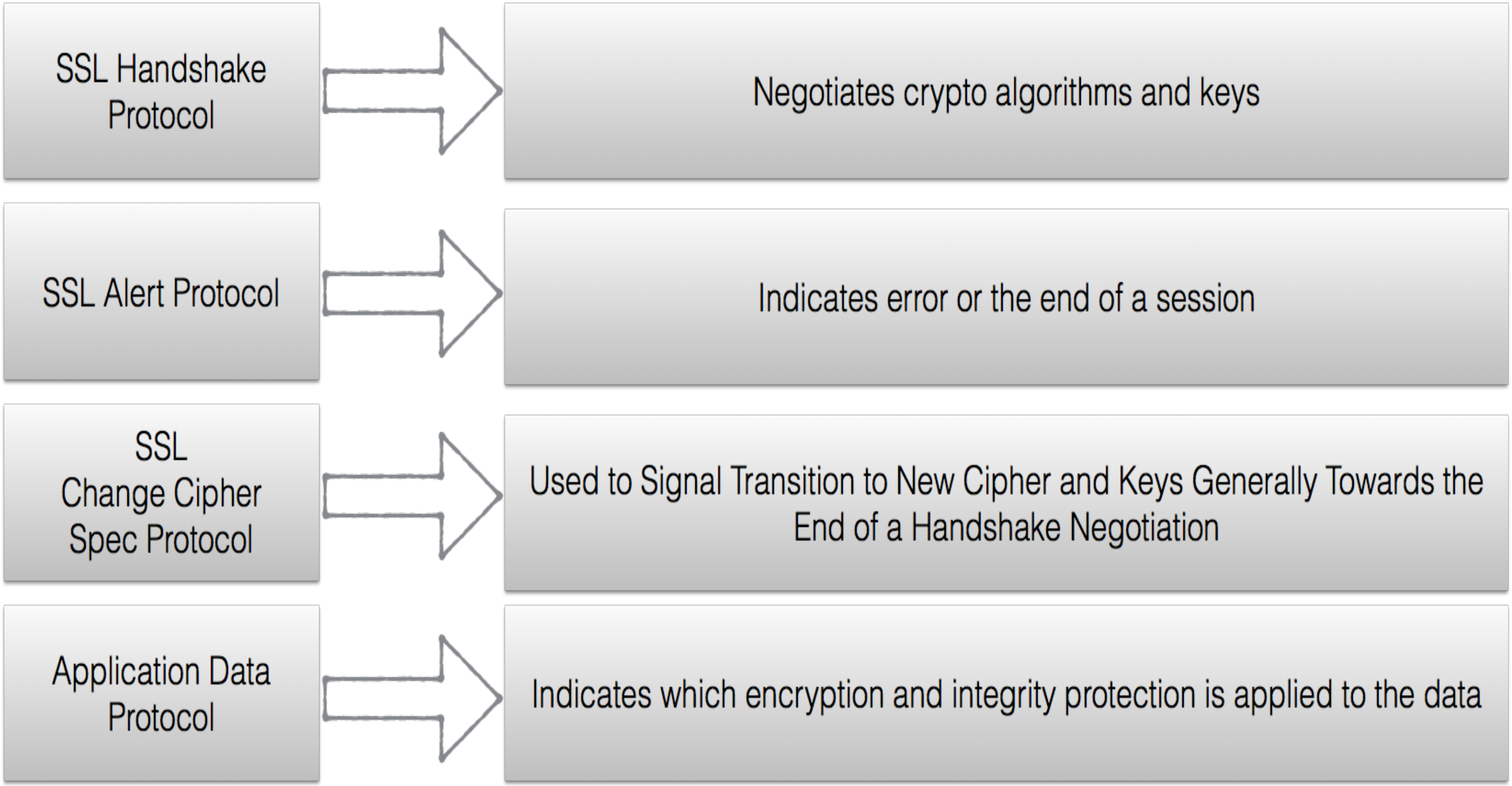
SSL Data Transfer Phase

9

Data

9

SSL Protocol Building Block Functions



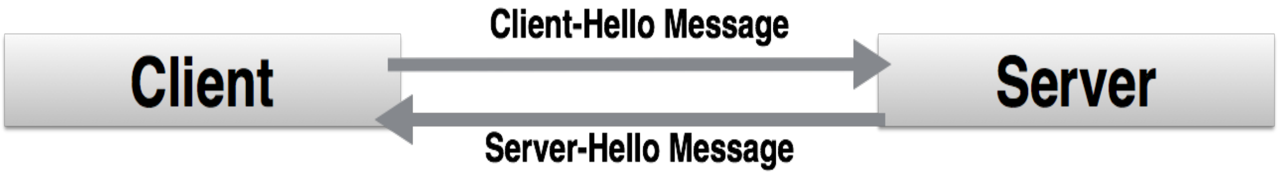
SSL Handshake Protocol → Negotiates crypto algorithms and keys

SSL Alert Protocol → Indicates error or the end of a session

SSL Change Cipher Spec Protocol → Used to Signal Transition to New Cipher and Keys Generally Towards the End of a Handshake Negotiation

Application Data Protocol → Indicates which encryption and integrity protection is applied to the data

SSL Handshake protocol



Key	Cipher	Hash
RSA	RC4	HMAC-MD5
Diffie-Hellman	Triple DES	HMAC-SHA
DSA	AES	

Version	3.3
Random Number	289484848484

Key	Cipher	Hash
RSA	RC4	HMAC-MD5
Diffie-Hellman	Triple DES	HMAC-SHA
DSA	AES	

SSL Alert Protocol

- Alert messages communicate the severity of the message and a description of the alert
- Fatal messages result in connection termination.

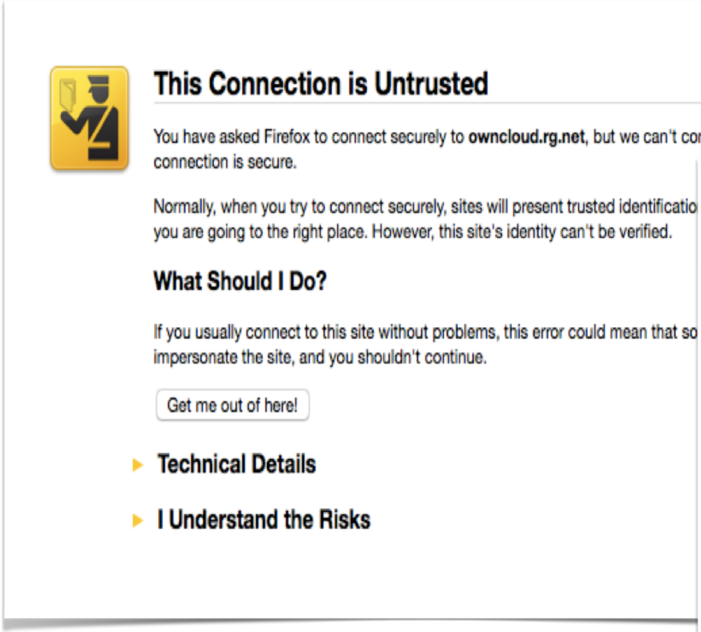
SSL ChangeCipherSpec Protocol

- The ChangeCipherSpec layer is composed of one message that signals the beginning of secure communications between the client and server.

Application Data Protocol

- Application data messages are carried by the record layer and are fragmented, compressed, and encrypted based on the current connection state. The messages are treated as transparent data to the record layer.

Trusted vs Non Trusted Certificate



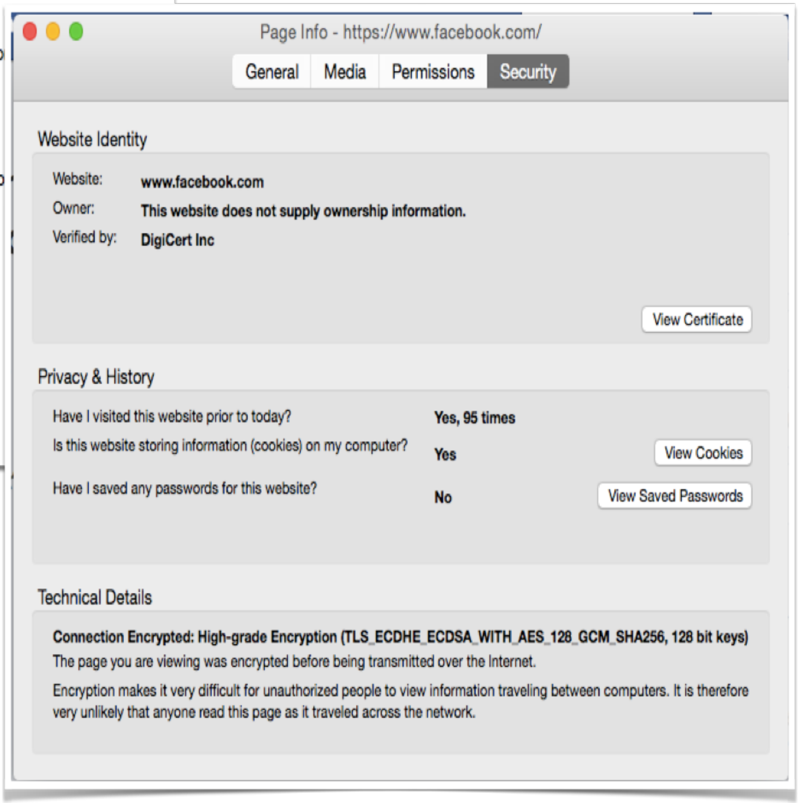
This Connection is Untrusted

You have asked Firefox to connect securely to **owncloud.rg.net**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identificatio you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that so impersonate the site, and you shouldn't continue.



Page Info - https://www.facebook.com/

Website Identity

Website: **www.facebook.com**

Owner: **This website does not supply ownership information.**

Verified by: **DigiCert Inc**

Privacy & History

Have I visited this website prior to today? **Yes, 95 times**

Is this website storing information (cookies) on my computer? **Yes**

Have I saved any passwords for this website? **No**

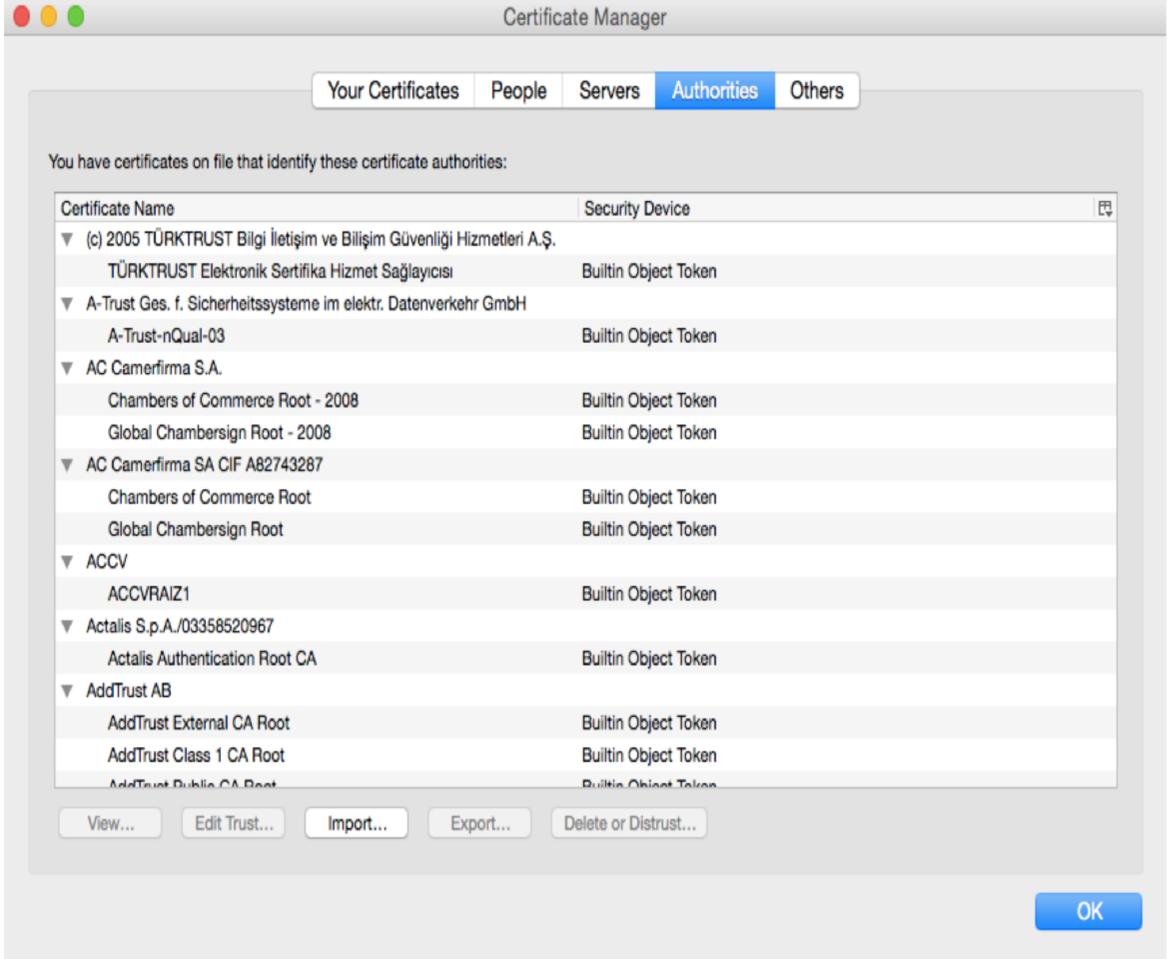
Technical Details

Connection Encrypted: High-grade Encryption (TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256, 128 bit keys)

The page you are viewing was encrypted before being transmitted over the Internet.

Encryption makes it very difficult for unauthorized people to view information traveling between computers. It is therefore very unlikely that anyone read this page as it traveled across the network.

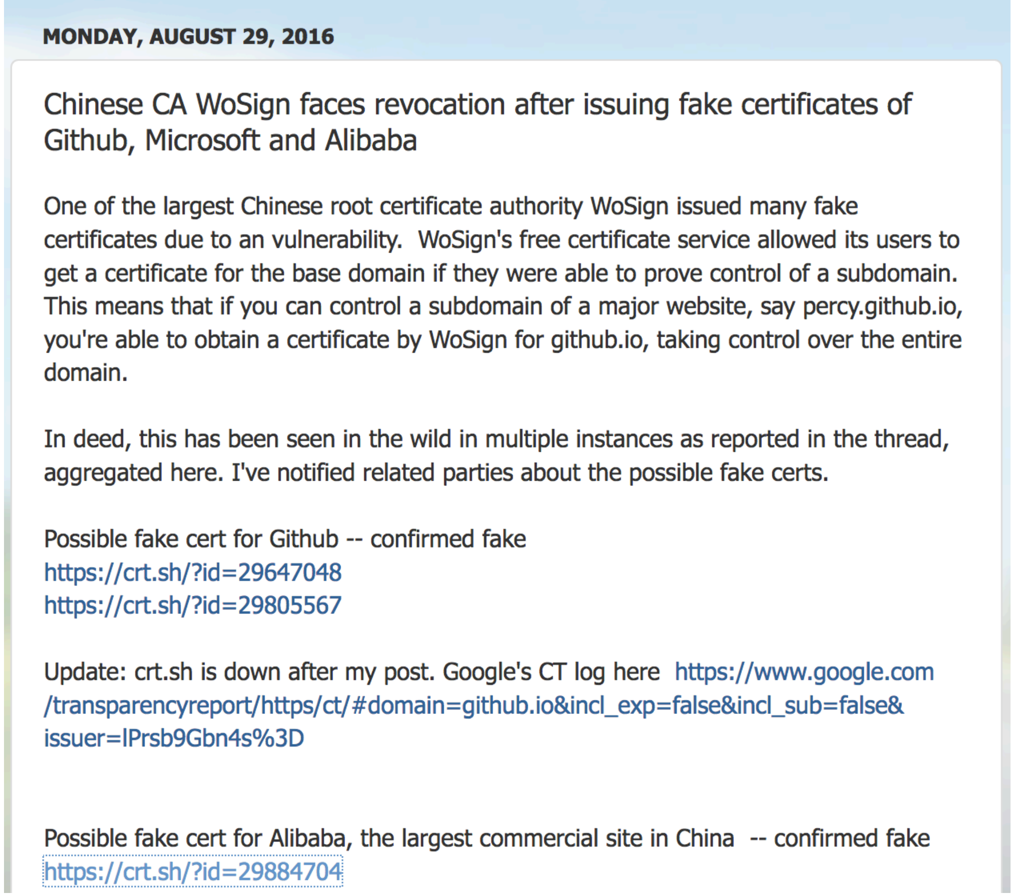
Certificate Authority



You have certificates on file that identify these certificate authorities:

Certificate Name	Security Device
▼ (c) 2005 TÜRKTRUST Bilgi İletişim ve Bilişim Güvenliği Hizmetleri A.Ş.	
TÜRKTRUST Elektronik Sertifika Hizmet Sağlayıcısı	Builtin Object Token
▼ A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH	
A-Trust-nQual-03	Builtin Object Token
▼ AC Camerfirma S.A.	
Chambers of Commerce Root - 2008	Builtin Object Token
Global Chambersign Root - 2008	Builtin Object Token
▼ AC Camerfirma SA CIF A82743287	
Chambers of Commerce Root	Builtin Object Token
Global Chambersign Root	Builtin Object Token
▼ ACCV	
ACCVRAIZ1	Builtin Object Token
▼ Actalis S.p.A./03358520967	
Actalis Authentication Root CA	Builtin Object Token
▼ AddTrust AB	
AddTrust External CA Root	Builtin Object Token
AddTrust Class 1 CA Root	Builtin Object Token
AddTrust Public CA Root	Builtin Object Token

Chinese CA WoSign faces revocation after issuing fake certificates of Github, Microsoft and Alibaba



MONDAY, AUGUST 29, 2016

Chinese CA WoSign faces revocation after issuing fake certificates of Github, Microsoft and Alibaba

One of the largest Chinese root certificate authority WoSign issued many fake certificates due to an vulnerability. WoSign's free certificate service allowed its users to get a certificate for the base domain if they were able to prove control of a subdomain. This means that if you can control a subdomain of a major website, say percy.github.io, you're able to obtain a certificate by WoSign for github.io, taking control over the entire domain.

In deed, this has been seen in the wild in multiple instances as reported in the thread, aggregated here. I've notified related parties about the possible fake certs.

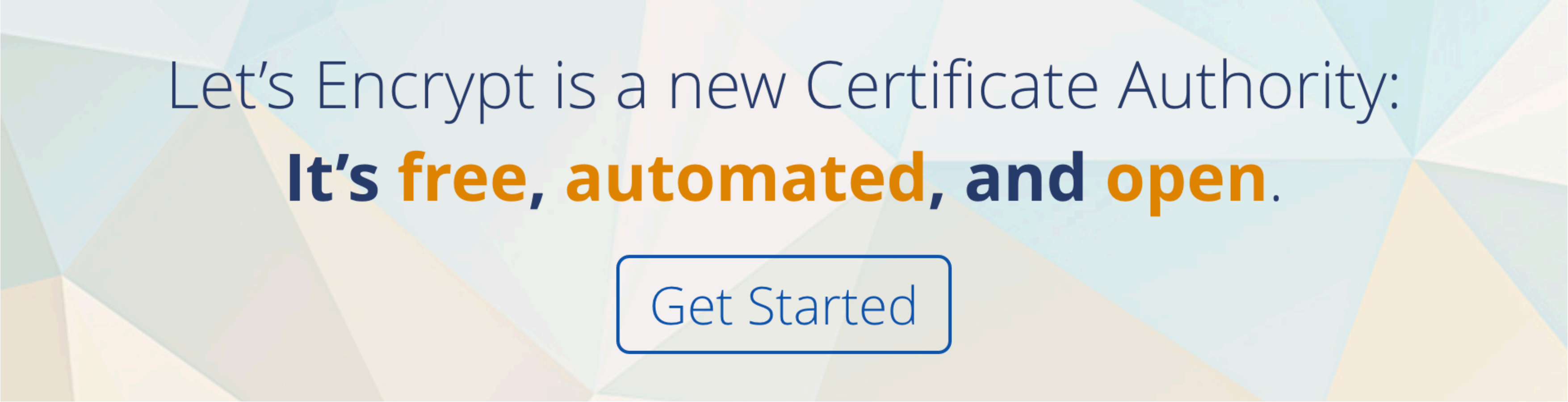
Possible fake cert for Github -- confirmed fake
https://crt.sh/?id=29647048
https://crt.sh/?id=29805567

Update: crt.sh is down after my post. Google's CT log here https://www.google.com/transparencyreport/https/ct/#domain=github.io&incl_exp=false&incl_sub=false&issuer=IPrsb9Gbn4s%3D

Possible fake cert for Alibaba, the largest commercial site in China -- confirmed fake
https://crt.sh/?id=29884704

https://groups.google.com/forum/m/#!topic/mozilla.dev.security.policy/k9PBmyLCi8I/discussion

Introducing Let'sEncrypt



Let's Encrypt is a new Certificate Authority:

It's free, automated, and open.

https://letsencrypt.org/

Introducing Let’sEncrypt

- Which browsers and operating systems support Let’s Encrypt
  - https://community.letsencrypt.org/t/which-browsers-and-operating-systems-support-lets-encrypt/4394
- Check your browser
  - https://wiki.apnictraining.net

LAB