

Let's Encrypt

2017/02/24

By UDomain

Let's Encrypt

by UDomain



SHARER

- ▶ UDomain Web Hosting Company Ltd. (<https://www.udomain.hk/>)

Panda Chan (pandachan@udomain.hk)
System Engineer
Linux Server

- ▶ HK local company providing hosting services
- ▶ Multinational corporations, government departments, SMEs and individuals users all over the world

Let's Encrypt

by UDomain



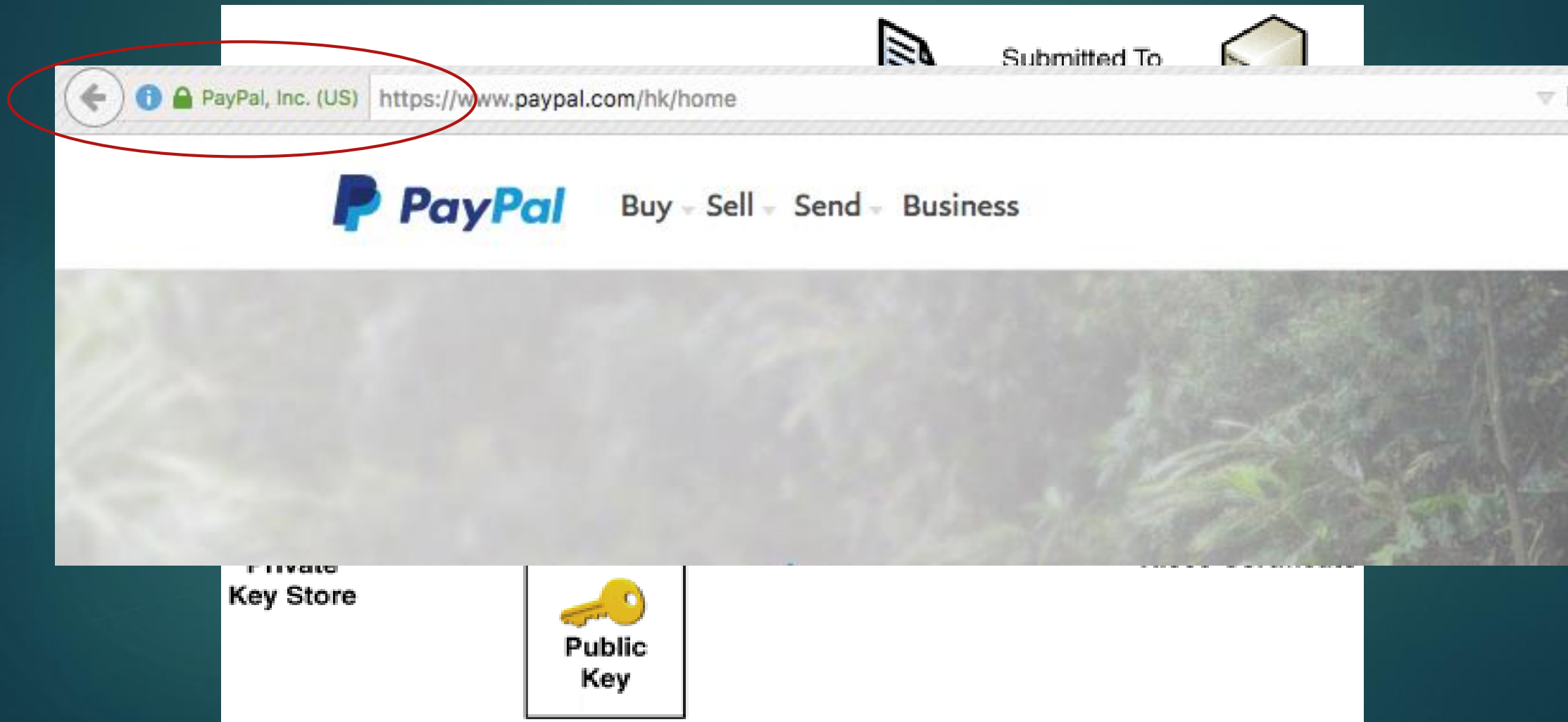
- Request & Obtain SSL Cert
- Traditional CA

Let's Encrypt

- Introduction
- Obtain SSL Cert
- Renew SSL Cert
- Verify Result
- Limitation

- Reference
- Final words

Request & Obtain SSL Cert



Traditional CA

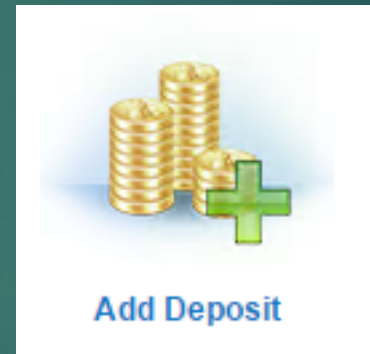
- ▶ GlobalSign (<https://www.globalsign.com/>)
- ▶ Symantec (<https://www.symantec.com/>)
- ▶ Comodo (<https://www.comodo.com/>)

Traditional CA

– Obtain and Renew SSL Cert

First of all:

- ▶ Register account in CA
- ▶ Add payment method
- ▶ Prepaid money



Traditional CA

– Obtain and Renew SSL Cert

- ▶ Generate private key

```
[root@hknog-panda ssl]# openssl genrsa -out hknog.pandachan.hk.key 2048
Generating RSA private key, 2048 bit long modulus
..+++
```

```
.....
e is 65537)
```

- ▶ Gen CSF

```
[root@hknog-panda ssl]# openssl req -new -key hknog.pandachan.hk.key -out hknog.pandachan.hk.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:HK
State or Province Name (full name) []:HK
Locality Name (eg, city) [Default City]:Hong Kong
Organization Name (eg, company) [Default Company Ltd]:UDomain
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []:hknog.pandachan.hk
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

Traditional CA

– Obtain and Renew SSL Cert

- ▶ Provide CSR to CA

Enter Your CSR here:

```
-----BEGIN CERTIFICATE REQUEST-----  
MIICojCCAYoCAQAwXTElMAkGA1UEBhMCSEsxCzAJBgNVBAGM  
DA1Ib25nIEtvmcxEADA0BgNVBAoMB1VEb21haW4xGzAZBgNV  
bmRhY2hhbi5oazCCASIwDQYJKoZIhvcNAQEBBQADggEPADCC  
c7qEaB67SB09Y8m55Wl/DpIjLqyam7TFMaTrbJcm9mtFIQ56  
K5J8tdDdQ+I1KI kz0E9vP7wFz2vZBkTyAfHdU0vWG09R4MyU  
h8PyBMBbHK57VbcW0htqyQNNbY0NqjfhTNXNF3UZnJSY5jtf  
lkIJAiaqyGg/diuf30MZFsAPBzYhj0Q5kBf8HgiczW9Ib72Y  
EiTJCJy/YmbU8IuripanovqRoPqj8ZRuvUA0tRQbxQL6KAfH  
6sE8W+6FiHmU6t8CAwEAAaAAMA0GCSqGSIb3DQEBCwUAA4IB  
del4+JaEvSwrRcBDrthjeiQ34ulCgGwhQ43e4M3w7Mrs7T+o  
EB7dvMC8LO8Y/zvZmbHuLqAQvdNBkWXNAMfbXVfh3ScFNR32  
9nQ+PFinhhxugaxaN6NIByGIUPjhlYsPT+ovAauA1CkLDd+H  
xofFOVzKdiVKUz0uU+BI6Jax5Eps9JSeoPgOH3xA0Iizhyob  
U3q2A7l4qJTJLAz16Dc/rrp3zeE1IS4rVbdhErR8ln6V31VZ
```


Traditional CA

– Obtain and Renew SSL Cert

- ▶ Validate your domain

Approver Email

We will send an Approver Email containing and a

- admin@hknog.pandachan.hk
- administrator@hknog.pandachan.hk
- hostmaster@hknog.pandachan.hk
- postmaster@hknog.pandachan.hk
- webmaster@hknog.pandachan.hk
- admin@pandachan.hk
- administrator@pandachan.hk
- hostmaster@pandachan.hk
- postmaster@pandachan.hk
- webmaster@pandachan.hk

HTTP Verification

We provide a Domain Verification Code (DVC) and you place that DVC in a text file in a specific location on your website.

- Use HTTP verification

DNS Verification

We provide a Domain Verification Code (DVC) and you create a DNS record containing the DVC.

- Use DNS verification

Traditional CA

– Obtain and Renew SSL Cert

- ▶ Retrieve SSL cert from email or CA control panel
- ▶ Install to server

Traditional CA

– Obtain and Renew SSL Cert

- ▶ Step for renew
 - ▶ Provide CSR to CA
 - ▶
 - ▶
 - ▶
 - ▶ Install to server

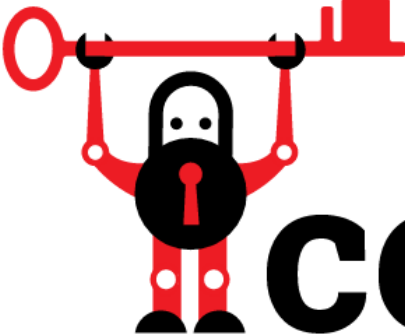
Let's Encrypt - Introduction

- ▶ SSL CA
 - ▶ Initiative from the Electronic Frontier Foundation (EFF)
 - ▶ Some major sponsor: Mozilla, Cisco, Akamai, Facebook
-
- Secure solution (of course!)
 - Free solution (issue, renew, SANs)
 - Automated solution (cmd => schedule job)
-
- Try to encrypt as much WWW traffic as possible

Let's Encrypt – Obtain SSL Cert

1. Enable EPEL
2. Install certbot (<https://certbot.eff.org/>)
(yum install certbot)
3. Generate Private Key
+ Generate CSR
+ Provide CSR to CA
+ CA validation (Challenge)
+ Obtain SSL
+ Install to Server
 - ▶ # certbot certonly --register-u
/var/www/vhosts/hknog/www
hknog2017.pandachan.hk
 - ▶ cert.pem
 - ▶ chain.pem
 - ▶ fullchain.pem
 - ▶ privkey.pem

home about certbot faq documentation support source code donate to EFF




certbot

Automatically enable HTTPS on your website with EFF's Certbot, deploying Let's Encrypt certificates.

I'm using on

- System
- Web Hosting Service
- Debian 7 (wheezy)
- Debian 8 (jessie)
- Debian testing/unstable
- Debian (other)
- Ubuntu 16.10 (yakkety)
- Ubuntu 16.04 (xenial)
- Ubuntu 14.04 (trusty)
- Ubuntu (other)
- Gentoo
- Arch Linux
- Fedora 22
- Fedora 23+
- CentOS 6
- RHEL 6
- CentOS/RHEL 7
- FreeBSD

To get instructions for Certbot, choose your server software from the dropdown menus above. You can then pick "advanced" if you want more control.



Let's Encrypt – Renew SSL Cert

▶ # certbot renew

Let's Encrypt – Obtain SSL Cert

- ▶ Server Environment

- ▶ CentOS7
- ▶ Nginx
- ▶ IPv4 only
- ▶ With SNI (Server Name Indication) enabled
- ▶ Disabled SSLv2 SSLv3 TLSv1.0
- ▶ Left only TLSv1.1 & TLSv1.2 to avoid POODLE, BEAST
- ▶ IP: 203.90.225.106

- ▶ Demo Now

Let's Encrypt – Verify Result

▶ <https://www.ssllabs.com/sslcheck/>

▶ <https://www.ssllabs.com/sslcheck/>

SSL Shopper Home SSL Wizard SSL FAQ SSL Reviews

SSL Checker

This SSL Checker will help you diagnose problems with your SSL certificate installation. You can use the SSL Checker, simply enter your server's hostname (must be public) in the box below button. If you need an SSL certificate, check out the [SSL Wizard](#).

[More Information About the SSL Checker](#)

Server Hostname

- ✓ [hknog.pandachan.hk](#) resolves to 203.90.225.106
- ✓ Server Type: nginx
- ✓ The certificate should be trusted by all major web browsers (all the certificates are installed).
- ✓ The certificate will expire in 89 days. [Remind me](#)
- ✓ The hostname ([hknog.pandachan.hk](#)) is correctly listed in the certificate

Server

Common name: hknog.pandachan.hk
SANs: hknog.pandachan.hk, hknog2017.pandachan.hk
Valid from February 19, 2017 to May 20, 2017
Serial Number: 0359ce34ab86043dc2900146b43a21fb09eb
Signature Algorithm: sha256WithRSAEncryption
Issuer: Let's Encrypt Authority X3

Chain

Common name: Let's Encrypt Authority X3
Organization: Let's Encrypt
Location: US
Valid from March 17, 2016 to March 17, 2021
Serial Number: 0a014142000015385736a0b85eca708
Signature Algorithm: sha256WithRSAEncryption
Issuer: DST Root CA X3

SSL Report: hknog.pandachan.hk (203.90.225.106)

Assessed on: Mon, 20 Feb 2017 08:05:49 UTC | [Hide](#) | [Clear cache](#) [Scan Another »](#)

Summary

Overall Rating

A+

Certificate 100
Protocol Support 95
Key Exchange 90
Cipher Strength 90

Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).

HTTP Strict Transport Security (HSTS) with long duration deployed on this server. [MORE INFO »](#)

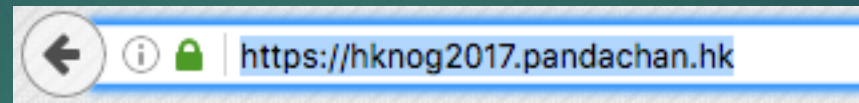
Certificate #1: RSA 2048 bits (SHA256withRSA)

Server Key and Certificate #1

Subject	hknog.pandachan.hk Fingerprint SHA1: 34d2b13f416e58dc73768bbfd67123ef8bc84fc0 Pin SHA256: R00ux5ptb/0BKQ/MaZTp1VLCBj574Fk+Gkyv9gD6NM=
Common names	hknog.pandachan.hk
Alternative names	hknog.pandachan.hk hknog2017.pandachan.hk
Valid from	Mon, 20 Feb 2017 06:51:00 UTC
Valid until	Sun, 21 May 2017 06:51:00 UTC (expires in 3 months)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	Let's Encrypt Authority X3 AIA: http://cert.int-x3.letsencrypt.org/
Signature algorithm	SHA256withRSA
Extended Validation	No

Let's Encrypt – Limitation

- ▶ 90 days
- ▶ No EV (Green Bar SSL)
- ▶ No *

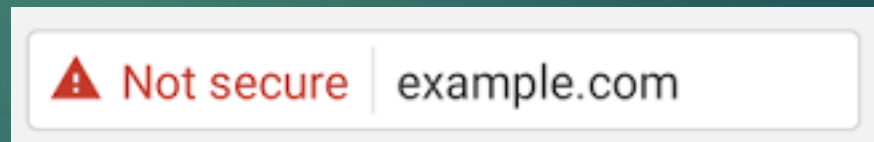


Reference

- ▶ Let's Encrypt - <https://letsencrypt.org/>
- ▶ CertBot - <https://certbot.eff.org/faq/>
- ▶ SSL Model: <https://www.sslshopper.com/what-is-ssl.html>
- ▶ Requesting and obtaining a certificate from a CA: <https://msdn.microsoft.com/en-us/library/ff647097.aspx>
- ▶ EV Cert - <https://www.sslshopper.com/cheapest-ev-ssl-certificates.html>
- ▶ ACME (Automated Certificate Management Environment):
https://en.wikipedia.org/wiki/Automated_Certificate_Management_Environment

Final Words

- ▶ Achieving higher Google ranking by using HTTPS
<https://webmasters.googleblog.com/2014/08/https-as-ranking-signal.html>
 - ▶ taking into account whether sites use secure, encrypted connections as a signal in our search ranking algorithms
- ▶ Showing Not Secure in Google Chrome
<https://security.googleblog.com/2016/09/moving-towards-more-secure-web.html>
 - ▶ Beginning in January 2017 (Chrome 56), we'll mark HTTP pages that collect passwords or credit cards as non-secure, as part of a long-term plan to mark all HTTP sites as non-secure.
- ▶ All websites with HTTPS
- ▶ Further questions or discussion
pandachan@udomain.hk



▶ END