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

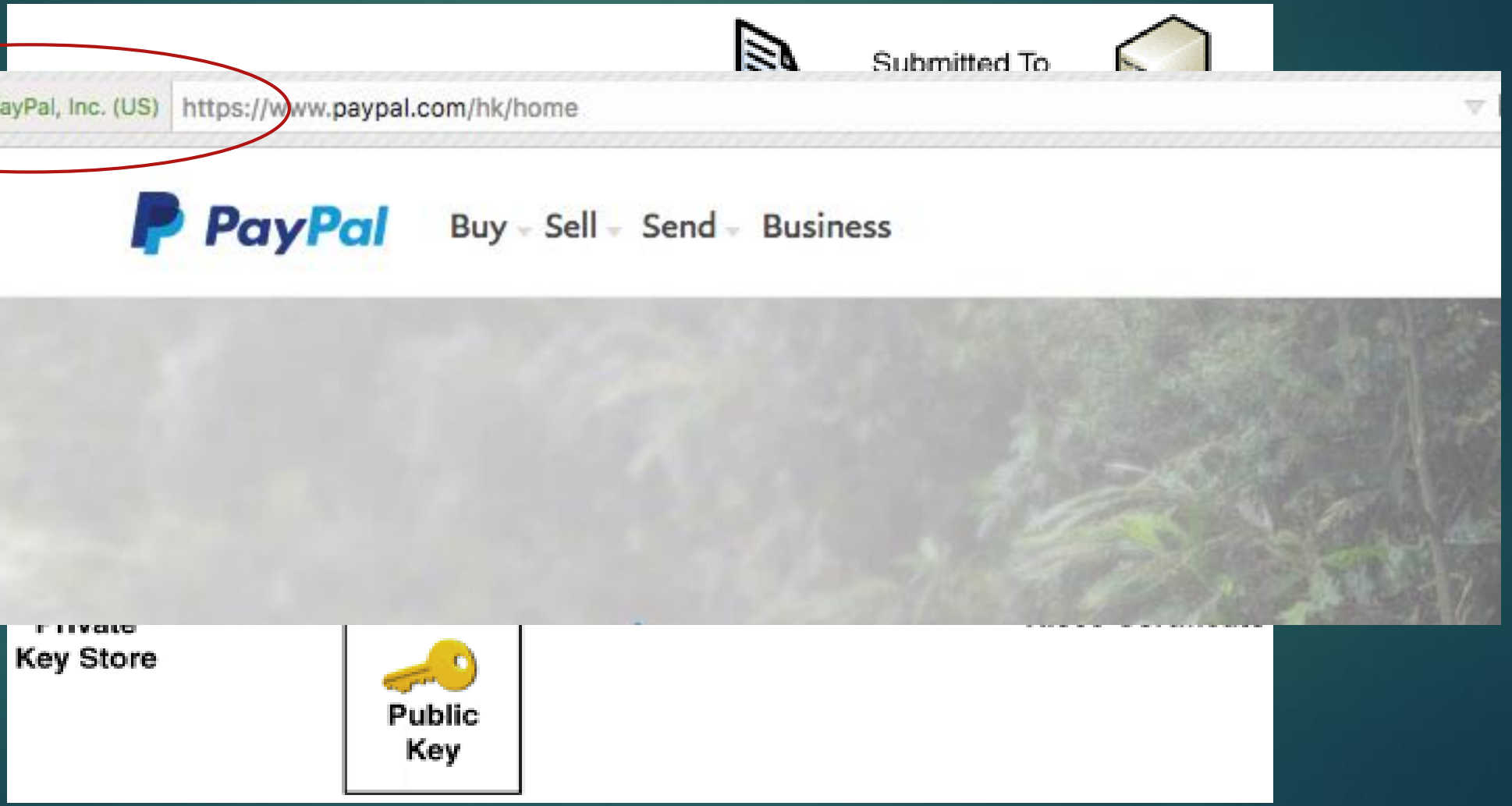
- Request
  & Obtain SSL Cert
- Traditional CA

Let's Encrypt

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

- Reference
- Final words

Request & Obtain SSL Cert



Reference: https://msdn.microsoft.com/en-us/library/ff647097.aspx

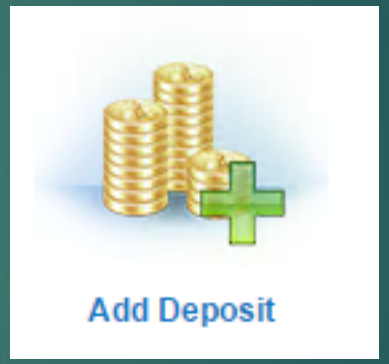
Traditional CA

- 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 CSR

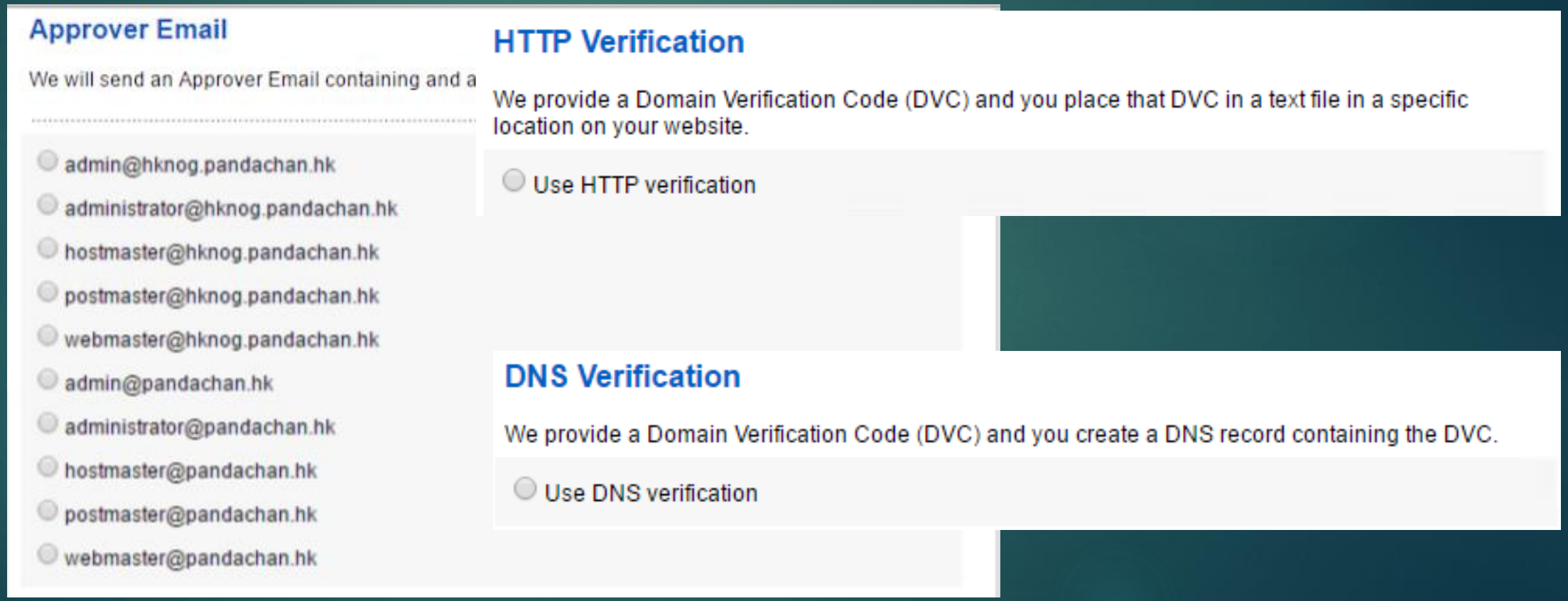
```
[root@hknog-panda ssl]# openssl req -new -key hknog.pandachan.hk.key -out hknog.pandachan.hk.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few 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

Traditional CA – Obtain and Renew SSL Cert

- Validate your domain



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

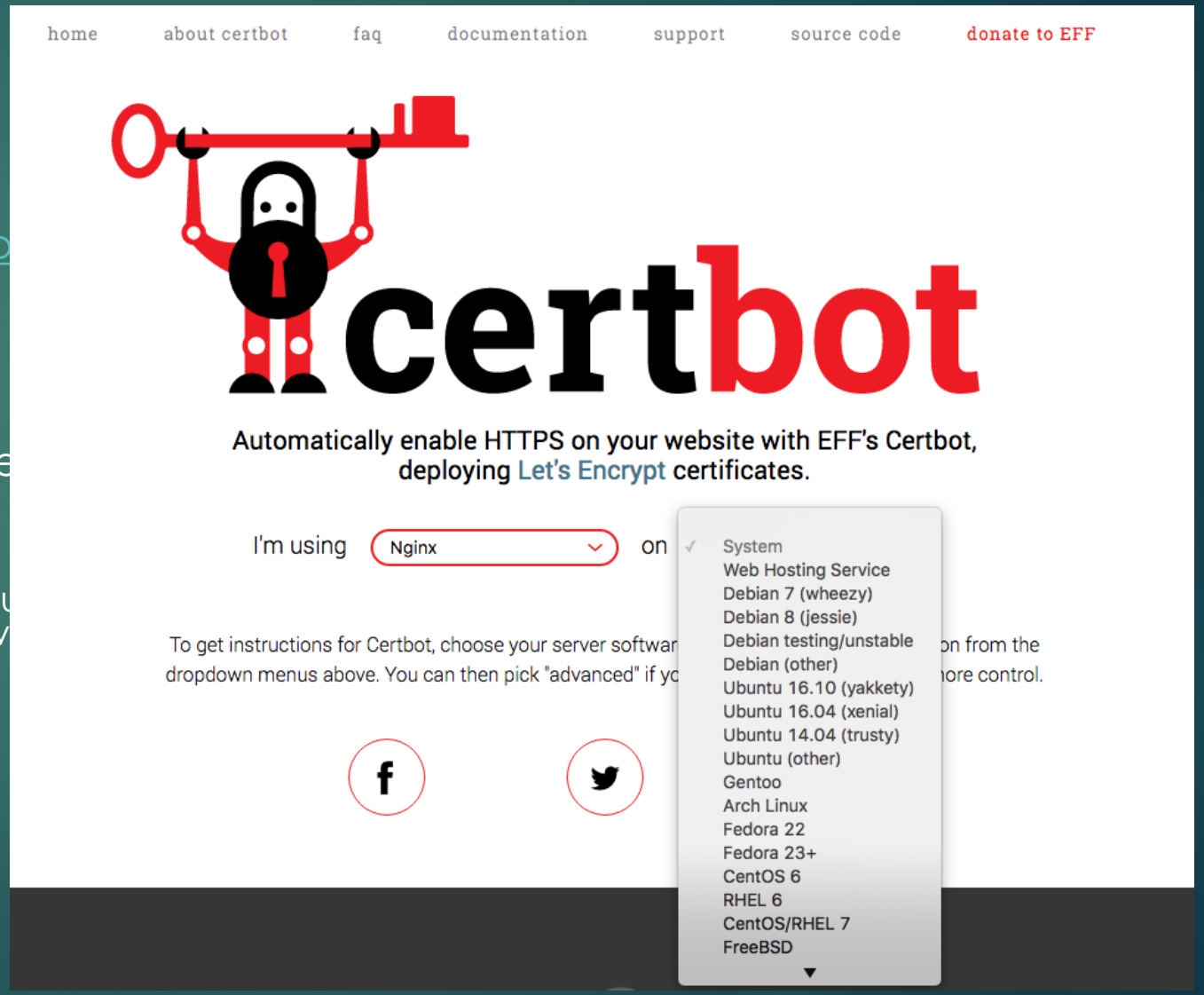
- SSL CA
- Initiative from the Electronic Frontier Foundation (EFF)
- Some major sponsor: Mozilla, Cisco, Akamai, Facebook

- 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://certbo
   (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/ww
     hknog2017.pandachan.hk
   - cert.pem
   - chain.pem
   - fullchain.pem
   - privkey.pem



Let's Encrypt – Renew SSL Cert

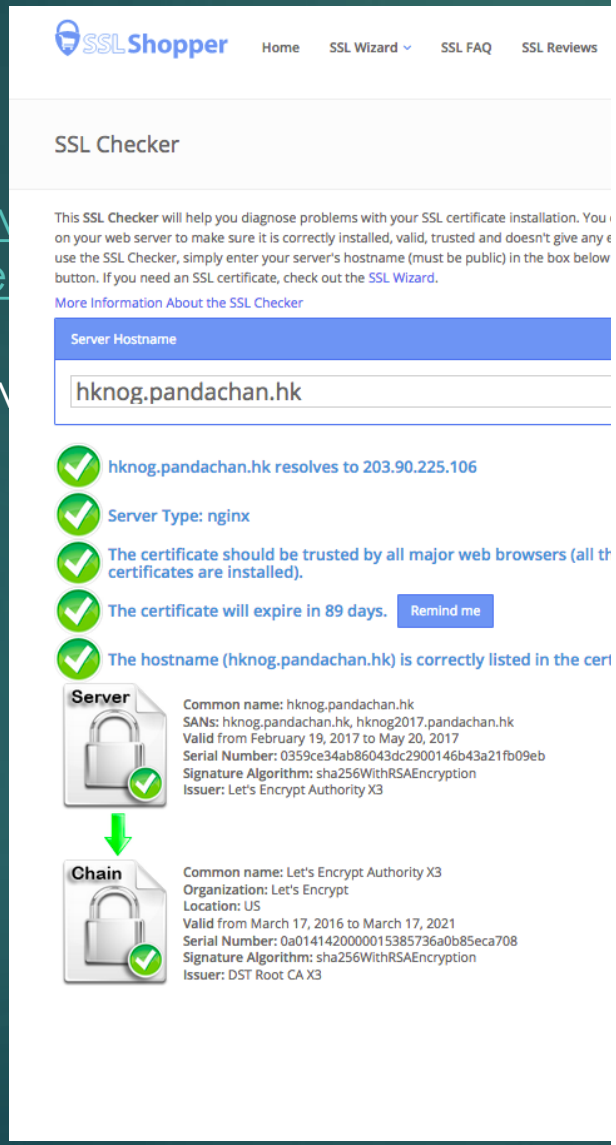
- # certbot renew

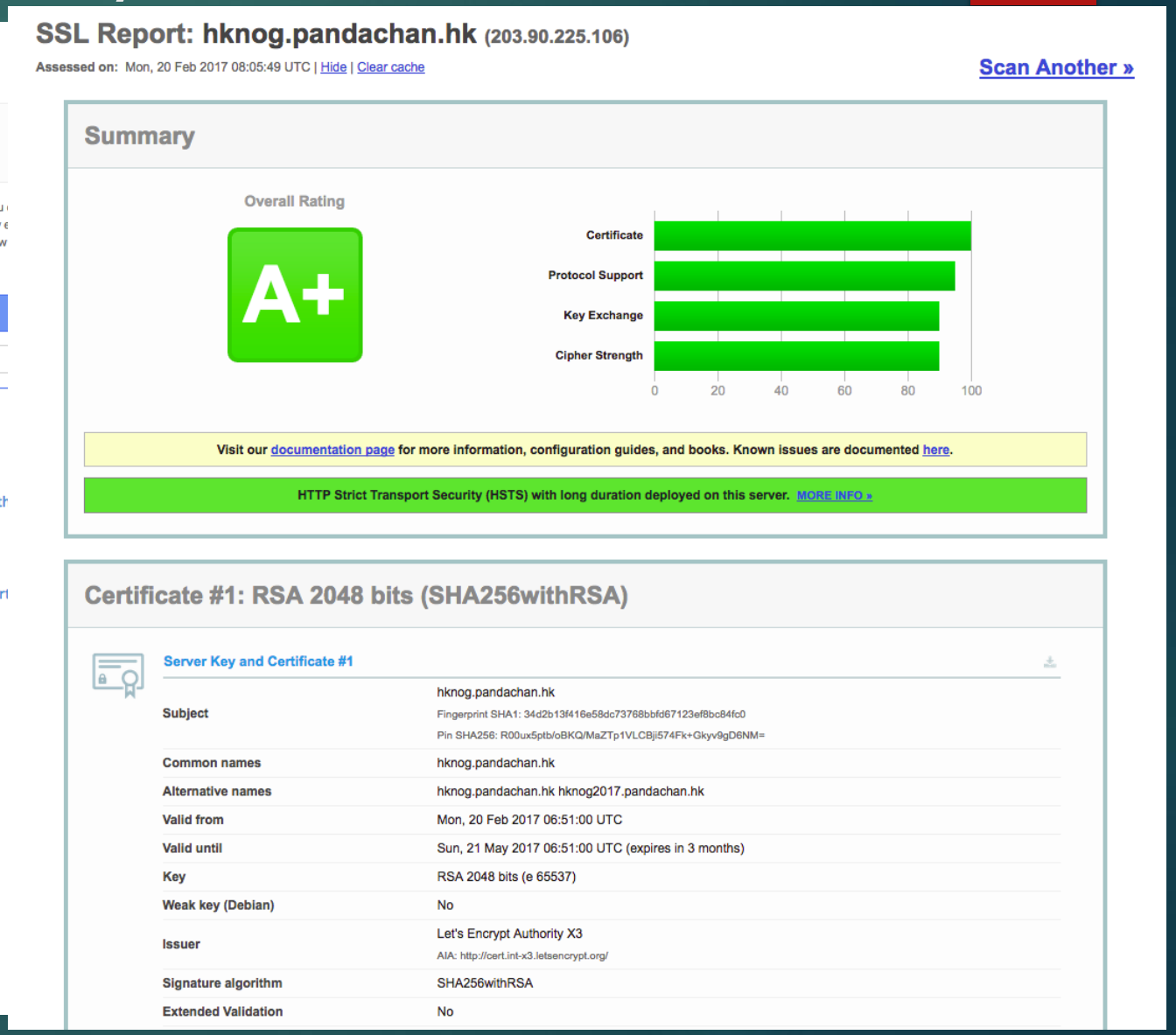
Let's Encrypt – Obtain SSL Cert

- 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

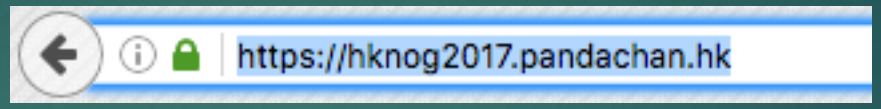
- https://v
  checke
- https://v





Let's Encrypt – Limitation

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

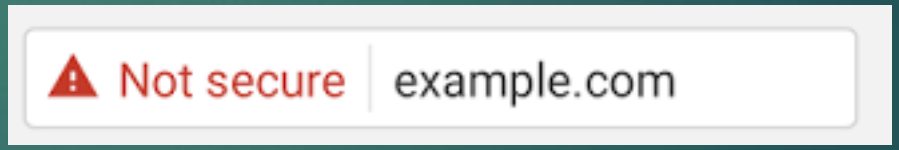


Reference

- 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