

TLS/SSL

- <https://sslmate.com/caa/> - CAA

Let's Encrypt / certbot

- <https://certbot.eff.org/docs/using.html> Certbot Manual
- Let's Encrypt(CertBot) SSL with HAProxy
- HAProxy SSL
- Let's Encrypt(CertBot) Wildcard Certificates

certbot

```
certbot dns . 가 http
    http 가
    *.domain.com
    dns
http my.domain.dom let's encrypt
    --standalone . dns
    TXT
--preferred-challenges dns 가 . --manual http dns
```

- (dhparam) 가?

- (dhparam) SSL WAS SSL dhparam dhparam
 . SSL A .

OpenSSL dhparam .

```
openssl dhparam -out dhparam.pem <KEY-SIZE>
# KEY-SIZE 2048 4096
```

dhparam 가 가

<https://ssl-config.mozilla.org/>

dhparam .

- <https://ssl-config.mozilla.org/ffdhe2048.txt>
- <https://ssl-config.mozilla.org/ffdhe4096.txt>

- <https://rsec.kr/?p=242>
- <https://waspro.tistory.com/479>

- [DNS CAA](#) [?](#)

From:

<https://atl.kr/dokuwiki/> - **AllThatLinux!**

Permanent link:

https://atl.kr/dokuwiki/doku.php/tls_ssl?rev=1608360959

Last update: **2020/12/19 06:55**

