

|                                                          |   |
|----------------------------------------------------------|---|
| <b>TLS/SSL</b>                                           | 3 |
| <i><b>Let's Encrypt / certbot</b></i>                    | 3 |
| certbot                                                  | 3 |
| -            ( <i><b>dhparam</b></i> )                가? | 3 |



# TLS/SSL

- <https://www.ssllabs.com/> -
- <https://sslmate.com/caa/> - CAA
- DNS CAA ?
- (Diffie-Hellman Key)
- Cipher Suite

## 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 dns_*. --dns-credentials *.pem --dns-key *.key --dns-tls http://10.10.10.10:443
```

- http `*.domain.com` 가
- 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  
SSL A dhparam

OpenSSL dhparam

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

dhparam

가

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>

From:

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

Permanent link:

[https://atl.kr/dokuwiki/doku.php/tls\\_ssl?rev=1616069260](https://atl.kr/dokuwiki/doku.php/tls_ssl?rev=1616069260)

Last update: **2021/03/18 12:07**

