

목차

TLS/SSL	3
암호화 종류	3
대칭키	3
공개키	3
해시	3
공개키 인증서 형식	3
인증서 포맷 변경	4
인증서 생성	4
CA 인증서 생성	4
서버 인증서 생성	5
CSR(인증요청서) 서명	5
디피-헬만 파라미터(dhparam) 키 는 무엇인가?	5

TLS/SSL

- [Let's Encrypt / certbot](#)
- [curl 명령어로 인증서 정보 확인](#)
- <https://www.ssllabs.com/> - 웹 보안점검
- <https://sslmate.com/caa/> - CAA 생성기
- DNS CAA 레코드는 무엇일까?
- 디피 헬만 키 (Diffie-Hellman Key)
- Mozilla TLS Cipher Suite
- X.509란?

암호화 종류

대칭키

- DES
- AES
- SEED
- ARIA

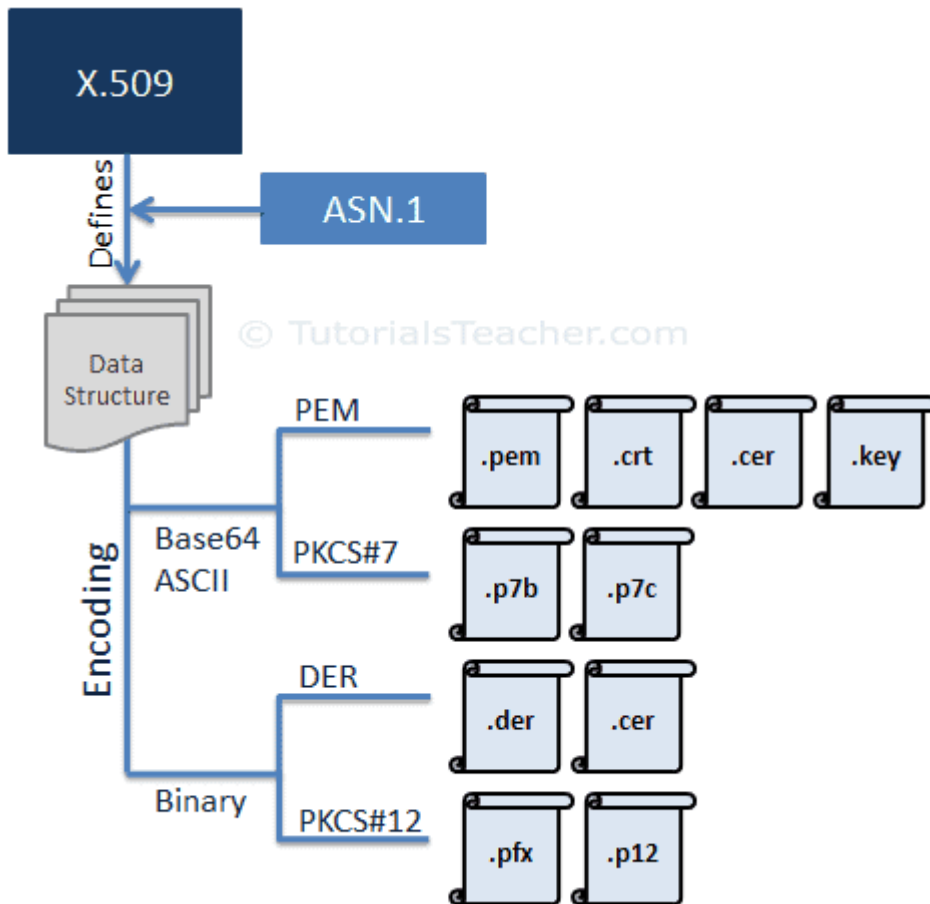
공개키

- RSA
- DSA
- Diffie-Hellman

해시

- MD5
- SHA1
- SHA2 (SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256)
- SHA3

공개키 인증서 형식



<https://www.tutorialsteacher.com/https/ssl-certificate-format>

- PEM(Privacy-enhanced Electronic Mail) : Base64 ASCII로 encode 된 파일로 .pem, .cert, .cer, .key등이 여기에 속한다. pem 파일은 서버 인증서와 중간자 인증서, private key가 해당 파일에 포함된다. crt 혹은 cer 파일로 서버 인증서나 중간자 인증서가 사용되고 개인키는 key파일이 될수있다.
- DER(Distinguished Encoding Rules) : binary 폼으로 .der 이나 .cer 파일들을 포함한다. 해당 인증서는 Java 기반 web 서버에서 주로 사용된다.
- pfx, p12 ... : PKCS#12(Public Key Cryptography Standards #12)

인증서 포맷 변경

```
openssl x509 -in cert.crt -outform der -out cert.der
```

인증서 생성

CA 인증서 생성

```
# key 생성
openssl genrsa -out ca.key 4096
# 인증서 생성
openssl req -x509 -new -nodes -sha512 -days 3650 \
-key ca.key \
```

```
-out ca.crt
```

서버 인증서 생성

```
# key 생성
openssl genrsa -out ia.key 4096

# CSR(인증요청서) 생성
openssl req -sha512 -new \
    -key ia.key \
    -out ia.csr
```

CSR(인증요청서) 서명

```
# 인증요청서 서명
cat > v3.ext <<-EOF
authorityKeyIdentifier=keyid,issuer
basicConstraints=CA:FALSE
keyUsage = digitalSignature, nonRepudiation, keyEncipherment,
dataEncipherment
extendedKeyUsage = serverAuth
subjectAltName = @alt_names

[alt_names]
DNS.1=yourdomain.com
DNS.2=yourdomain
DNS.3=hostname
EOF

openssl x509 -req -sha512 -days 3650 \
    -extfile v3.ext \
    -CA ca.crt -CAkey ca.key -CAcreateserial \
    -in ia.csr \
    -out ia.crt
```

디피-헬만 파라미터(dhparam) 키 는 무엇인가?

디피-헬만 파라미터(이하 dhparam)는 SSL 통신시 암호화를 도와주는 방식중 하나로 dhparam 키를 이용해 암호화 복잡도를 높여 보안을 강화하는것이 목적으로 각종 WAS의 SSL 통신에서 dhparam을 지원합니다. SSL 등급을 매기는 테스트 사이트에서 A등급 이상을 받으려면 이 설정은 필수로 해야합니다.

OpenSSL에서 dhparam 키를 생성하는 명령어는 다음과 같습니다.

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

보통 dhparam 키를 생성하는데 시간이 매우 오래 걸리기 때문에 누군가 만들어놓은 키값을 그대로 가져다 써도 무방하다. 다만 그 누군가는 믿을만한 사람이어쨌다.

모질라 <https://ssl-config.mozilla.org/>에서 공개적으로 제공하는 dhparam 파일이 있다.

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

참조링크

- <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

Last update: **2023/02/07 01:49**

