

Apache

Apache 서버에서 개인키 및 CSR을 생성하는 방법입니다.



- CSR(Certificate Signing Request)이란 인증서 서명 요청을 의미하며, 인증서 발급을 위한 정보(도메인, 회사명, 담당자 등)를 담고 있는 데이터입니다.
- 본 매뉴얼은 Apache 2.x 기준으로 작성되었습니다.
- Apache 서버에서 SSL 통신을 가능하게 하기 위해서는 OpenSSL과 mod_ssl이 필요합니다.
- 서버에 OpenSSL이 설치되어 있어야 하며, Apache 버전과 mod_ssl 버전 확인 후, 알맞은 OpenSSL을 설치해주시기 바랍니다.
- CSR 생성 방법은 서버 환경에 따라 다를 수 있으며, 본 매뉴얼은 참고용으로 이용 바랍니다.

1. 개인키를 생성합니다.

```
openssl genrsa -des3 -out gabia.key(개인키 파일) 2048
```



- 키 사이즈는 2048만 가능합니다.
- 인증서를 설치할 때 개인키 및 비밀번호가 필요하므로 보관에 유의해주세요.
- 개인키를 분실한 경우, 복원 및 재생성이 불가능합니다.

2. 개인키를 바탕으로 CSR을 생성합니다.

```
openssl req -new -key gabia.key(키 파일) -out gabia.csr(CSR 파일) -sha256
```

3. 인증서 발급을 위한 정보를 입력합니다.

CSR에 입력하는 정보는 신청 도메인 등록 정보(후이즈 정보)를 바탕으로 작성하며, 영문으로 입력합니다.

```

Enter pass phrase for gabikey.pem:
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]:KR
State or Province Name (full name) []:Seoul
Locality Name (eg, city) [Default City]:Songpa-gu
Organization Name (eg, company) [Default Company Ltd]:Gabia
Organizational Unit Name (eg, section) []:Test team
Common Name (eg, your name or your server's hostname) []:www.gabia.com

```

- Country : 국가코드, 대문자로 입력해야 합니다. (한국 : KR)
- State or Province : 시/도
- Locality : 구/군
- Organization : 회사명
- Organization Unit : 부서명
- Common Name : 인증서 도메인 주소를 입력합니다. 와일드카드 인증서는 *.도메인을 입력합니다.

위 필수 정보 외에 추가 속성은 입력하지 않으셔도 됩니다.

4. CSR 파일 내용을 확인합니다.

```
# cat csr.pem
-----BEGIN CERTIFICATE REQUEST-----
MIICsjCCAzoCAQAwbTELMAkGA1UEBhMCs1lxDjAMBgNVBAgMBVNIb3VzMRIwEAYD
VQQHDAITb25ncGetZ3UxDjAMBgNVBAoMBUdhYmIhMRIwEAYDVQQLEA1UZXNOIHRI
YW0xYjAUBgNVBAMMDXZ3dy5nYWJpYS5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IB
DwAwggEKAoIBAQCNpfd3sWAM/eigYkFuMD+AUaSNxOHnaosZpbdM0zw+epeiefWs
DV0hFjM3mDNhhNlnjM2FTIC/3EQ2xWE5VEUZgf7lqVn67p9xM4CKfVEkrVtxpgRI
lIj fZVtqhgi rhkC1xeSJHeGZiEa3whn4zcS3VL/b0wyrDmELewTDEy+/F7fwGmkZ
d7WyllyLINjeGzzjLN3hwe3wEwBUiElv5yJJqaHMHtm0gR7vNo4/rFNXUaA/iFjd
rcYYTXthoeR+50rs7MYHMAD800cl00xhlmAflw2AY4FvXrgs2uspfbii fIZTlpZ/
3vNmtcfKGna4lNP1g3RhGhC1tx/9tzaipeJ/AgMBAAAGgADANBgkqhkiG9w0BAQUF
AAOCAQEAFHCd6rAVLl asaamVuXDdnC8ncctbq5uvawxn7anz2EWG8UkP9Zi ln1Tg
+1yRte4s3hZ0wDYAH4Uwc/WsyKN9/2Rne4y6Gcdn6gVBDfQcBEtKbCHLBGx6Vfp8
kUbmKErzbkxBshDAY7K+vAFxdixJ4yM8U5CZx1y8LmqtmqZ0nC6/Gqq6cyQhH2n7
dLfnQscyKnBjXiukeDoK6DYDNDcd3n8uwkIRIX3Z+/MJsJFnmYKBxiBhdkNm3ISg
w1fL9YMI XDAgGYFYurYnMoRY9S1F0ybxBnJKkpWw0M1CUEDEWZ8Y5d7LQjgruxkb
QMheQB2Mwf1Xg5szUNbFYg4ZF0afPw==
-----END CERTIFICATE REQUEST-----
```

-----BEGIN CERTIFICATE REQUEST----- 부터 -----END CERTIFICATE REQUEST----- 까지 복사하여
SSL 인증서 관리정보를 입력합니다.