Comodo Korea
국제표준인증 제휴기관

IBM WebSphere HTTP 서버에서 CSR 생성하기

※ 처음 인증서를 설치하는 경우에는 1 단계부터 시작한다.
인증서를 기존에 사용하고 있어서 이미 1~7 단계의 설정이 되어 있다면 곧 바로 8 단계부터 시작한다.

<http.conf 파일의 설정>

1. drive:/IBM/IBM HTTP SERVER/conf 디렉터리로 이동한다
2. 디렉터리 안의 httpd.conf 파일을 httpd.conf.orig 로 변경한다.
3. httpd.conf.sample 파일을 httpd.conf 파일로 변경한다. (이 파일은 SSL 설정이 포함되어 있는 conf 파일이다.)
4. 변경 된 httpd.conf 를 텍스트편집기로 연다. 5.
다음 내용을 주석에서 풀어준다.
   a. #LoadModule ibm_ssl_module modules/IBMModuleSSLencryption-level.dll
   where encryption-level is the appropriate level of encryption for your locale.
   b. #Listen 443
   c. #<VirtualHost host.name.com:443>
   You must also substitute your fully qualified common name in this line.
   d. #SSLEnable
   e. #</VirtualHost>
   f. #SSLDisable
   g. Keyfile "drive:/IBM/IBM HTTP SERVER/ssl/keyfile.kdb".
   Replace the word keys with ssl.
   h. #SSLV2Timeout 100
   i. #SSLV3Timeout 1000

   수정을 마쳤으면 저장하고 나온다.

6. IBM HTTP Server 를 중지한다.
7. IBM HTTP Server 를 가동한다.

<키 데이터베이스 파일 생성>

8. NT 환경이라면 시작 > 프로그램 > IBM HTTP Server > Start Key Management 유틸리티를 선택한다.
Unix 의 경우에는 drive:/IBM/IBM HTTP SERVER/ikeyman 을 실행시킨다.
9. IBM Key Management 창에서 Key Database File(키 데이터베이스 파일) 메뉴를 클릭하여 New(신규)를 선택한다.

Comodo Korea
국제표준인증 제휴기관

10. 입력 창이 뜨면 키 파일의 이름을 지어준다. 파일이름.kdb 를 입력하고 저장하기 원하는 파일 위치를 선택하여 OK(확인)를 클릭한다.
일반적으로 키파일은 drive:/IBM/IBM HTTP SERVER/ssl/ 디렉터리에 저장한다.
11. 암호 입력 프롬프트 창이 나타나면 적당한 암호를 입력한다. 암호의 만기일은 특별한 이유가 없으면 설정하지 않는 것을 권장한다. 주의!! "Stash the password to a file?(암호를 파일에 보관하시겠습니까?)"에 반드시 체크한다. 모두 확인 되었으면 OK(확인)를 클릭한다.

<CSR(인증서명요청)파일 생성>

12.Create(작성) 메뉴를 클릭하여 New Certificate(새 증명서)를 선택한다.
13. 입력 창이 뜨면 반드시 모든 정보를 영문으로 기입한다.

※ 입력예

<주의사항>
① Organization(영문회사명)에는 < > ~ ! @ # $ % ^ * / \ ( ) ? 등의 특수 문자를 넣을 수 없습니다. 사업자 등록증에 기재된 회사명과 일치하는 영문회사명을 넣어 주시기 바랍니다. (예: 사업자 등록증에 '코모도코리아'이면 Comodokorea 으로 넣어주셔야 합니다. Comodo 만 넣으시면 않됩니다.) 또한, 인증서를 설치할 Common Name(인증 받을 도메인 주소)에 해당하는 도메인의 등록정보를 반드시 참조하셔서 해당 등록정보에 기재된 회사명을 참고 하실 수 있겠습니다.
영문 회사명은 소유하고 계신 도메인이 com/net/org 인 경우에는 Network Solutions 에서, kr 인 경우에는 KRNIC 에서 확인할 수 있습니다.
② Common Name(인증 받을 도메인 주소)에는 IP 주소, 포트번호, 경로명, http:// 등을 포함할 수 없습니다.

Key Label(키 레이블) :	키를 구분할 수 있도록 적당한 이름을 지어준다.
Version(버전) :	X509 V3(반드시 X509 V3 를 선택)
Key Size(키크기) :	2048(반드시 2048 를 선택)
Common Name : (인증 받을 도메인주소)	www.comodokorea.co.kr
Organization(영문회사명)	ComodoKorea

Organization(부서)	Digital Certificate Team
Locality(구/군)	Songpa
State/Province(시/도)	Seoul
Zipcode(우편번호)	empty(비워둔다)
Country(국가코드)	KR
Validity Period(유효기간)	empty(비워둔다)

14. 이 작업을 통하여 만들어질 CSR 파일의 적당한 이름을 파일이름.arm 으로 정한다. 파일을 저장할 위치를 선택하여 OK(확인)를 클릭한다. 일반적으로 키파일과 함께 drive:/IBM/IBM HTTP SERVER/ssl/ 디렉터리에 저장한다.
15. 파일이름.arm 을 텍스트편집기로 열어보면 다음과 같은 형식의 암호화된 문서를 볼 수 있다.

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIBnDCCAQUACQAwXjELMAkGA1UEBhMCQ0ExEDOABgNVBAgTBO9ud
GFayW8xEDAOBgNVBAcTBO1vbnRyYWwxDDAKBgNVBAoTA0tGQzEdMB
sGA1UEAxMUd3d3Lmlsb3ZlY2hpY2tlbi5jb2OwgZOwDQYJKoZIhvc
NAQEBBQADgYsAMIGHAoGBALmJA2FLSGJ9iCF8uwfPW2AKkyyKo/e9
aHnnwLLw8WWjhl[ww9pLietwX3bp6Do8/7mwV3jrgQ1OIwarj9iKM
LT6cSdeZOOTNn7vvJaNv1iCBWGNypQv3kVMMzzjEtOl2uGl8VOyeE
7jImYj4HlMa+R168AmXT82ubDR2ivqQwl7AgEDoAAwDQYJKoZIhvc
NAQEEBQADgYEAn8BTcPg4Owo/hGIMU2m39FVvhOM86/ZBkANQCEHx
Mz/zrnydXnvRMKPSE2O8x3Bgh5cGBC47YghGZzdvxYJAT1vbkfCSB
VR9GBxef6/ytkuJ9YnK84Q8x+pS2bEBDnwOD2MwdOSF1sBb1bcFfk
mbpjN2N+hqrrvAOmcNpAgk8nU=
-----END NEW CERTIFICATE REQUEST-----
```

16. 이 CSR 문서를 반드시 첫줄(-----BEGIN NEW CERTIFICATE REQUEST-----)과 끝줄(-----END NEW CERTIFICATE REQUEST-----)이 포함되도록 복사하여 메모장에 붙여넣기 한다. 이 CSR 을 E-mail 로 전송한다.
17. 지금까지의 작업을 통해 다음 4 개의 파일이 만들어졌을 것이다. 파일에 변조 및 이상이 발생할 경우를 대비하여 이 파일들을 안전한 곳에 반드시 백업해둔다. (파일 백업을 하지 않아 발생하는 불이익에 대하여 코모도코리아는 책임을 지지 않습니다.)

    파일이름.kdb
    파일이름.sth

파일이름.rdb
파일이름.arm