인증서가 발급되면 담당자의 이메일을 통해 세개의 인증서가 전달된다.
하나는 웹 서버인증서([인증받은 도메인 이름으로 된].crt) 이고,
나머지는 루트인증서(TrustSign_Root.cer)와
체인인증서(TrustSign_Chain.cer)이다. 파일을 메모장(Notepad)으로
열어보면 모두 다음과 같은 형식으로 되어 있다.

```
-----BEGIN CERTIFICATE-----
MIISDOIUIkmIsRRIkSIIWLISdsSKJIaIOSISLKjwBgNVBAg
AALOJdIwjam4gQ2FwZTESMBAGA1UEBxMJQ2FwZSBUb3duMR
QwEgYDVQQKEwHLOWDvcnR1bmIOaTEYMBYGKi2UECxMPT25s
aW5IIFNIcnZpY2VzMRowGAYDVQQDExF3d3cuZm9yd2FyZC5
jby56YTBaMAOGCSqGSIb3DQEHHKJWAAkImLKSuIjSOIjsfB
Wu5WLHD/G4BJ+PobiC9d7S6pDvAjuyC+dPAnLOd91tXdm2j
19OD1kgDoSp5ZyGSgwJh2V7diuuPIHDAgEDoAAwDQYJVVjk
ksohvcNAQEEBQADQQBf8LSLKknIskISSLIworrr334ZmXD1
AvUjuDPCWzFupRIIIiq7UR8ZOwiJUUsIIkfq/IuuIIz6oq6
htdJkIil/wdhh
-----END CERTIFICATE-----
```

1. 기존에 생성하였던 파일이름.kdb, 파일이름.rdb, 파일이름.sth 파일을 CSR 생성과정중에 생긴 drive:\IBM\IBM HTTP SERVER\ssl 디렉터리에 이동시킨다. 또, 메일로 수취한 웹 서버인증서([인증받은 도메인 이름으로 된].crt)와 루트인증서(TrustSign_Root.cer), 체인인증서(TrustSign_Chain.cer)도 같은 경로에 이동시킨다.
2. NT 환경이라면 시작 > 프로그램 > IBM HTTP Server > Start Key Management 유틸리티를 선택한다.
   Unix 의 경우에는 drive:/IBM/IBM HTTP SERVER/ikeyman 을 실행시킨다.
3. Open(열기) -> 파일이름.kdb 를 연다. 이때 암호를 입력한다.

< 루트인증서(TrustSign_Root.cer) 설치 >

4. Key Database content(키 데이터베이스 내용) 프레임에서 Signer Certificates(서명자 증명서)를 선택한 후 Add(추가) 버튼을 클릭한다.
5. File dialog box 가 뜨면 File Type(데이터 유형)을 Base64-encoded ASCII data 로 선택한다. 그리고, Browse(찾아보기)를 클릭하여 루트인증서(TrustSign_Root.cer)를 찾아 선택하고 OK(확인)를 클릭한다.
6. Label dialog box 가 보이면 Label 이름(ex. Root)을 적당히 입력 후 OK 를 클릭한다.

Comodo Korea
국제표준인증 제휴기관

7. 서명자 증명서의 목록에 루트인증서가 확실히 추가 되었는지 확인한다.

< 체인인증서(TrustSign_Chain.cer) 설치 >

8. Key Database content(키 데이터베이스 내용) 프레임에서 Signer Certificates(서명자 증명서)를 선택한 후 Add(추가) 버튼을 클릭한다.
9. File dialog box 가 뜨면 File Type(데이터 유형)을 Base64-encoded ASCII data 로 선택한다. 그리고, Browse(찾아보기)를 클릭하여 체인인증서(TrustSign_Chain.cer)를 찾아 선택하고 OK(확인)를 클릭한다.
10. Label dialog box 가 보이면 Label 이름(ex. Chain)을 적당히 입력후 OK 를 클릭한다.
11. 서명자 증명서의 목록에 체인인증서가 확실히 추가 되었는지 확인한다.

< 웹 서버인증서([인증받은 도메인 이름으로 된].crt) 설치 >

12. Personal Certificates(개인 증명서)를 선택하고 Receive(수신)를 클릭한다.
13. File dialog box 가 뜨면 File Type(데이터 유형)을 Base64-encoded ASCII data 로 선택한다. 그리고, Browse(찾아보기)를 클릭하여 웹 서버인증서([인증받은 도메인 이름으로 된].crt)를 찾아 선택하고 OK(확인)를 클릭한다.
14. 설치가 완료되었으면 인증서를 정확히 설치했는지 확인한다. 우측에 있는 '보기/편집' 버튼을 클릭하면 키 정보를 확인할 수 있다.
15. Management Utility 를 빠져나온다.

< httpd.conf 수정 >

16. drive:\IBM\IBM HTTP SERVER\conf 디렉터리에 있는 httpd.conf 파일을 연다.
17. 파일의 내용 중에 아래와 같이 되어 있는 부분을 찾는다.

Keyfile drive:/IBM/IBM HTTP SERVER/ssl/keyfile.kdb

'Keyfile' 이라는 키워드로 찾으면 쉽게 찾을 수 있을 것이다. 여기서 파일이름.kdb 의 경로를 적어주면 된다.
예를 들어 이 가이드에서는 drive:/IBM/IBM HTTP SERVER/ssl/ 디렉터리에 파일이름.kdb 라는 이름으로 저장되어 있으므로 이렇게 변경한다.

Comodo Korea
국제표준인증 제휴기관

Keyfile drive:/IBM/IBM HTTP SERVER/ssl/파일이름.kdb

18. IBM HTTP Server 를 stop/start 해준다.
19. 웹브라우저를 통해 https:// 로 해당 사이트에 접속하여 SSL 이 잘 구동되었는지 확인한다.

< .kdb 파일 백업하기 > 20..kdb

파일을 꼭 백업해 둡니다.
<키 데이터베이스 파일은 꼭 백업을 해두셔야 하며, 백업을 하지 않아 발생하는 문제에 대해서는 재발급 비용이 추가될 수 있습니다.>