

Copyright 2015 By KICA. All Right Reserved.

Tomcat v5.0+ CSR 생성가이드

Win32, Linux 공통 문서

한국정보인증 KICASSL



- CSR 생성 시 주의사항

- ① 키스토어(개인키 포함) 생성
- ② CSR(Certificate Signing Request) 생성

- “개인키와 CSR은 반드시 일치 하여야 합니다.”
 - 여러 번 개인키를 생성했다면 맨 마지막 개인키를 이용하셔야 합니다.
 - **개인키와 발급 신청한 CSR이 다르면 인증서 설치가 불가능합니다.**
 - 동일한 개인키는 복원 및 재생성을 할 수 없으므로 보관에 주의가 필요합니다.
- “개인키가 발급한 SSL 인증서와 매칭 오류 시 표시 메시지/로그”
 - “키와 인증서가 매칭 되지 않습니다” 등과 같은 **매칭 오류 메시지가 로그/표시됨. (키워드 : matching)**
 - > CSR 생성 시 사용한 개인키 파일로 다시 설정하시거나 재발급 하셔야합니다.
 - “중개(체인)을 검증을 실패 하였습니다” 등과 같은 **체인 오류 메시지가 로그/표시됨. (키워드 : chain)**
 - > 중개 인증서 관련 설정 내용에 확인이 필요합니다.
 - 1) Keystore 등 import가 필요한 웹 서버는 중개인증서를 import 여부 확인
 - 2) 중개인증서 경로를 별도로 설정하는 웹 서버는 중개인증서 경로 및 파일 위치 확인
- “1개의 서버에서 여러 도메인 사용시 주의사항”
 - https(SSL)을 사용하는 포트는 중복 및 공용 사용이 불가합니다.
 - 2개의 인증서를 설치 시 2개의 포트가 필요하며, 포트 공유를 하려면 “와일드카드 인증서”, 또는 “멀티도메인 인증서” 상품을 사용하셔야 합니다.
 - 와일드카드 SSL인증서 (*.kicassl.com), 멀티도메인 SSL인증서는 포트 공유가 가능한 SSL 인증서 입니다.
 - 멀티도메인 인증서 설치 후 인증서에 도메인을 추가 신청 시 인증서는 재설치 해야 합니다.

- 단일 / 멀티 / 와일드카드 도메인 SSL 인증서에 따른 신청 방법의 차이점
 - 설명 내용 중 상품별 주의사항과 차이점을 따로 해당 부분에 추가 설명 하였습니다.
 - 내용 중 상품 종류별 추가 설명이 없으면 예제와 동일하게 진행하시길 바랍니다.

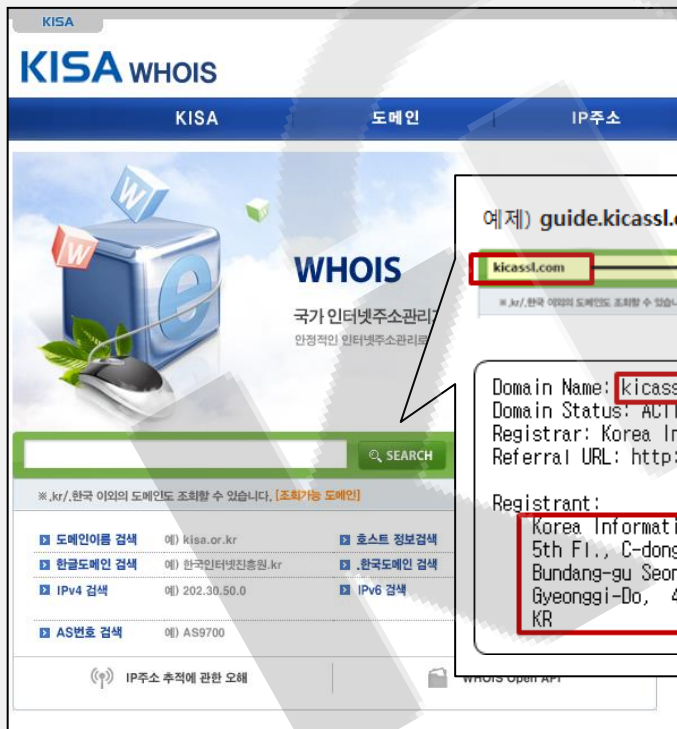
상품 종류	매뉴얼과 차이점
단일 도메인	매뉴얼 설명대로 진행해주시길 바랍니다. 한 서버에 복수로 인증서 설치 시 단일 도메인 인증서는 포트 공유 불가능
멀티 도메인	인증서 신청 시 해당 멀티 인증서에 포함될 나머지 도메인들을 추가 도메인 기입란에 빠짐없이 입력하여 신청해 주시기 바랍니다. 그 외 다른 내용은 동일합니다. 또한 포트 공유가 가능합니다
와일드카드 도메인	CSR 생성 시 Common Name에 *기본도메인 으로 도메인을 입력합니다. (예: *.kicassl.com) 즉 SSL 인증서를 사용할 웹 서버의 Full domain name에 *.kicassl.com 과 같이 서브도메인 구역에 "*"를 입력하여 생성합니다. 그 외 다른 내용은 동일합니다. 또한 포트 공유가 가능합니다.

① 키스토어(개인키 포함) 생성 [도메인 등록 정보 확인]

- SSL 인증서 CSR 생성시 기입 내용
 - 도메인 등록 정보 확인

※ 꼭 도메인 등록정보와 사업자등록증정보와 일치해야 합니다.
도메인의 등록자(실사용자)의 업체정보를 기입해야 합니다.

예) 도메인 등록자 A – 유지보수 및 대행자 B일 때, “A” 정보 기입



예제) guide.kicassl.com 도메인에 대한 Whois 등록정보 검색화면

Domain Name: **kicassl.com**

Domain Status: ACTIVE

Registrar: Korea Information Certificate Authority, Inc. dba DomainCA.com

Referral URL: http://www.DomainCA.com

Registrant:

Korea Information Certificate Authority, Inc.
5th Fl., C-dong, Pangyo Digital Center, 624, Sampyeong-dong
Bundang-gu Seongnam Si
Gyeonggi-Do, 463400
KR

도메인 검색 시
'www', 'guide' 등은 제외하고
kicassl.com 만 검색.

CSR 생성시 필요한 정보

① 키스토어(개인키 포함) 생성 [도메인 등록정보와 영문 사업자등록증 정보의 일치 확인]

- SSL 인증서 CSR 생성시 기입 내용
 - 영문 사업자등록증 정보와 도메인 등록정보와 일치 확인

[앞 장, 도메인 등록정보 기준]

SSL 인증서 신청 시 필요한 내용

- 1) Country Name : (Ex : KR)**
영문 대문자 두 자리의 국가코드
- 2) State : (Ex : Gyeonggi-Do)**
영문의 시/도
- 3) Locality : 영문의 구/군/시**
(Ex : Seongnam-Si Bundang-gu)
- 4) Organization Name : 영문의 회사명**
(Ex : Korea Information Certificate Authority, Inc)
- 5) Org~ Unit Name : (Ex : SSL Team)**
담당부서 영문 명칭
- 6) Common Name :**
인증서를 발급받을 대상의 URL
(Ex : guide.kicassl.com)
만일 와일드카드 상품 일 시 "*.kicassl.com"

발급번호 Issuance number	사업자등록증명 Certificate for Business Registration (법인사업자) (Corporate Taxpayer)		처리기간 Processing period
6416-683-7517-223	한국정보인증주식회사 Korea Information Certificate Authority Inc.		즉 시 Immediately
사업자등록번호 Business registration number	110-81-41568		
성명(대표자) Name of representative	고성학 Koh Sung Hak		
주민(법인)등록번호 Resident(Corporation) registration number	경기도 성남시 분당구 판교로 242 (삼평동, 판교디지털센터 C 동 5층) (Sangpyeong-dong, Sang-am-dong, 16FL), 242, Pangyo-ro, Bundang-gu Seongnam-si, Gyeonggi-do, Korea		
사업장소재지 Address			

※ 꼭 도메인 등록정보와 사업자등록증정보와 일치해야 합니다.
도메인의 등록자(실사용자)의 업체정보를 기입해야 합니다.

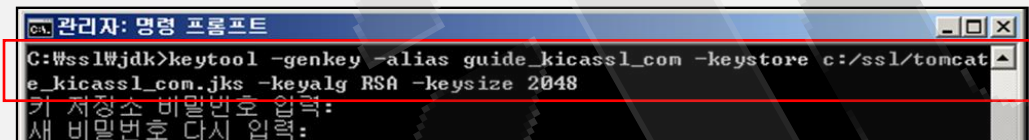
예) 도메인 등록자 A - 유지보수 및 대행자 B일 때, "A" 정보 기입

① 키스토어(개인키 포함) 생성

- keytool(JAVA)를 이용하여 JKS(Java Keystore) 생성

- prompt> `keytool -genkey -alias [개인키 별칭] -keystore [생성할 JKS 파일명 및 경로] -keyalg RSA -keysize 2048`

- (1) -genkey : 키스토어와 개인키 생성 옵션
- (2) -alias : 개인키 별칭
- (3) -keystore : 생성할 JKS 파일명 및 경로
- (4) -keyalg : 사용할 키 알고리즘 (RSA)
- (5) -keysize : RSA 알고리즘의 키 사이즈 (2048)



Linux계열은 경로를 리눅스 경로로 변경하여 입력하시길 바랍니다

- 종략 - (다음 장 계속)

※ 위에 결과로 생성된 개인키를 기반으로 CSR과 인증서가 발급되므로 꼭 백업이 필요하며, 보관에 유의하셔야 합니다.

만일, JDK버전이 1.4.2 보다 낮다면 SHA-2 인증서를 사용할 수 없습니다.

따라서 웹서버와 JDK를 업데이트 하신 후 진행해주시길 바랍니다.

만일, SHA-2 인증서를 사용할 수 없는 환경이라면, SHA-2 인증서 설치 후 접속 시 “**페이지를 표시할 수 없습니다.**” 오류 메시지가 표시됩니다.

인증서 만료일 기준 2016년 12월 31일 이전인 인증서만 **SHA-1** 인증서가 발급 가능하며, 별도로 문의해주셔야 합니다.

① 키스토어(개인키 포함) 생성

- keytool(JAVA)를 이용하여 JKS(Java Keystore) 생성
 - 앞 장에 이어서 키스토어 생성 정보 입력

```

관리자: 명령 프롬프트

      앞 장 내용

키 저장소 비밀번호 입력:
새 비밀번호 다시 입력:
이름과 성을 입력하십시오.
[Unknown]: guide.kicassl.com
조직 단위 이름을 입력하십시오.
[Unknown]: SSL Team
조직 이름을 입력하십시오.
[Unknown]: Korea Information Certificate Authority, Inc.
구/군/시 이름을 입력하십시오?
[Unknown]: Seongnam-Si Bundang-Gu
시/도 이름을 입력하십시오.
[Unknown]: Gyeonggi-Do
이 조직의 두 자리 국가 코드를 입력하십시오.
[Unknown]: KR
CN=guide.kicassl.com, OU=SSL Team, O="Korea Information Certificate Authority, Inc.", L=Seongnam-Si Bundang-Gu, ST=Gyeonggi-Do, C=KR<가> 맞습니까?
[아니오]: y

<guide_kicassl_com>에 대한 키 비밀번호를 입력하십시오:
<키 저장소 비밀번호와 동일한 경우 Enter 키를 누름>
    
```

SSL 인증서 요청자 정보

- 1) Country Name : (Ex : KR)
영문 대문자 두 자리의 국가코드
- 2) State : (Ex : Gyeonggi-Do)
영문의 시/도
- 3) Locality : 영문의 구/군/시
(Ex : Seongnam-Si Bundang-gu)
- 4) Organization Name : 영문의 회사명
(영문 사업자 등록증에 기입된 명칭)
(Ex : Korea Information Certificate Authority, Inc)
- 5) Org~ Unit Name : (Ex : SSL Team)
담당부서 영문 명칭
- 6) Common Name :
인증서를 발급받을 대상의 URL
(Ex : guide.kicassl.com)
만일 와일드카드 상품 일 시 "*.kicassl.com"
그 외의 입력 값은 생략 (Enter 키)

키 저장소 비밀번호와 동일하게 개인키 비밀번호를 설정해야 함.

※ 위에 결과로 생성된 JKS를 기반으로 CSR과 인증서가 발급되므로 꼭 키스토어 파일 백업이 필요하며, 보관에 유의하셔야 합니다.

② CSR(Certificate Signing Request) 생성 [가입하는 키스토어 파일은 꼭 보관하셔야 합니다]

- keytool(JAVA)를 이용하여 CSR파일 생성

- **keytool -certreq -alias** [지정한 개인키 별칭] **-file** [생성할 CSR 파일명 및 경로] **-sigalg SHA256WithRSA** **-keystore** [위 지정한 개인키가 있는 JKS 파일명 및 경로]

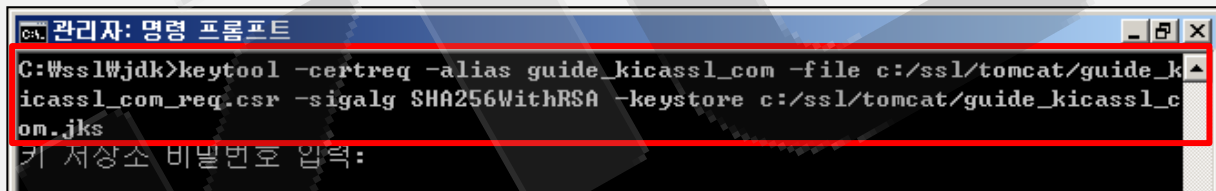
(1) -certreq : CSR 파일을 생성 옵션

(2) -alias : 개인키 별칭

(3) -file : 생성할 CSR 파일명 및 경로

(4) -sigalg : 사용할 서명 알고리즘 (SHA256WithRSA)

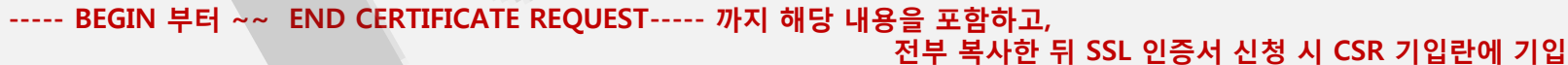
(5) -keystore : 생성한 JKS 파일명 및 경로



```
C:\Wssl\jdk>keytool -certreq -alias guide_kicassl_com -file c:/ssl/tomcat/guide_kicassl_com_req.csr -sigalg SHA256WithRSA -keystore c:/ssl/tomcat/guide_kicassl_com.jks
키 저장소 비밀번호 입력:
```

- **생성된 CSR파일(guide_kicassl_com_req.csr)의 내용**

- 앞 매뉴얼을 수행하면 base64 인코딩하여 "-req"에 지정한 경로로 파일이 저장됩니다.



감사합니다

신뢰세상
A World of Trust

한국정보인증(주) SSL (Korea Information Certificate Authority, Inc.)

E-mail. webmaster@kicassl.com