# 보안서버 구축가이드(ver 5.1)

# - 2012. 12. 27 -

<ul> <li>Ⅱ. 웹서버 종류별 SSL 구축방법</li></ul>	I. 보안서버 개요 5	
<ul> <li>Ⅲ. 이중화된 웹서버 SSL적용방법</li></ul>	Ⅱ. 웹서버 종류별 SSL 구축방법 11	
<ul> <li>Ⅳ. SSL 적용여부 확인방법</li></ul>	Ⅲ. 이중화된 웹서버 SSL적용방법 96	
<ul> <li>V. 웹페이지 SSL 구현방법</li></ul>	Ⅳ. SSL 적용여부 확인방법 106	
<ul> <li>Ⅵ. 보안서버 구축 시 유의사항</li></ul>	V. 웹페이지 SSL 구현방법 108	
₩I. 보안서버 구축 FAQ	Ⅵ. 보안서버 구축 시 유의사항 113	
[붙임 1] SSL인증서 발급절차	Ⅶ. 보안서버 구축 FAQ 114	
[붙임 2] 보안서버 구축 후 오류발생시 참조사항 119	[붙임 1] SSL인증서 발급절차 115	
	[붙임 2] 보안서버 구축 후 오류발생시 참조사항 119	



# 주 의 사 항

본 가이드 사용 시 다음의 사항에 주의 하시고 활용하시기 바랍니다.

본 가이드는 SSL인증서 방식을 이용한 기술이며 관련내용 등은 개별 웹 사이트 구축 시 나타날 수 있는 고유한 환경이 다를 수 있으므로 실제 환경에서 구축·적용 시 차이가 있을 수 있습니다. 그러므로 각 웹 서버별 기술된 예시 및 내용을 구축·적용 할 때에 는 먼저 각 웹 사이트의 고유한 환경에 맞는지 확인해야만 합니다.

※ 본 가이드의 내용에 대하여 오류 및 보안서버 구축에 있어 의견이
 있을 때에는 gpki@klid.or.kr로 해당 내용을 보내주시거나 문의하시
 면 적극 보완・지원하도록 하겠습니다.

I. 보안서버 개요	· 5
1. 보안서버 정의	<del></del> 5
2. 보안서버 구축 필요성	·· 5
가. 정보유출(Sniffing) 방지 ······	• 5
나. 피싱(Phishing) 방지 및 웹 사이트 신뢰도 향상	• 5
3. 보안서버 적용 범위	·• 6
4. 보안서버 적용 대상	·• 6
5. SSL인증서 신청절차	·• 6
가. 웹서버 종류 확인	•• 6
나. 행정전자서명(SSL인증서) 신청서 작성	•• 6
다. 공문 발송	$\cdot \cdot 7$
라. CSR(Certificate Signing Request) 생성	$\cdot \cdot 7$
마. 인증서 등록 안내 수신(신청 후 2일 이내)	$\cdot \cdot 7$
바. SSL인증서 발급(인증서 등록 후 15일 이내)	$\cdot \cdot 7$
6. 보안서버 구축절차	<del></del> 8
7. 보안서버 설치파일 설명	9
가. CSR (Certificate Signing Request)	• 9
나. CSR 생성시 입력값	• 9
다. 보안서버 구축시 필요한 파일	10
라. 웹서버별 보안서버 구축 관련 파일 형태	10
II. 웹서버 종류별 SSL 구축방법	11
2.1. IIS 6.0 이하 웹서버에서 보안서버 구축하기	11
가. 개인키 생성 및 CSR 생성 방법	11
나. 인증서 설치 방법	17
다. 웹사이트 적용하기	27
라. SSL 인증서 개인키 추출 방법	27
2.2. IIS 7.0 웹서버에서 보안서버 구축하기	34
가. 개인키 생성 및 CSR 생성 방법	34
나. 인증서 설치 방법	37
다. 웹사이트 적용	47
라. SSL 인증서 개인키 추출 방법	48
2.3. Apache 서버에서 보안서버 구축하기	54
가. Linux O/S에 OpenSSL과 Mod_ssl의 설치 방법	54
나. WIN O/S에 OpenSSL 설치 방법 ······	56
다. 개인키 생성 및 CSR생성 방법	58
라. 인증서 설치 방법	61
마. 웹사이트 적용	65
바. SSL 인증서 개인키 추출 방법	
	65
2.4. WebToB 서버에서 보안서버 구축하기	65 <b>66</b>

# <차 례>

나 이즈서 서치 바버	71
다. 원사이트 전유	75
라. 마카이드 ㅋㅎ 라. SSL 이즛서 개이키 추축 방법	75
2.5. iPlanet 서버에서 보안서버 구축하기	76
가. 개인키 생성 및 CSR 생성 방법	76
나. 인증서 설치 방법	78
다. 웹사이트 적용	84
라. SSL 인증서 개인키 추출 방법	84
2.6. Tomcat 서버에서 보안서버 구축하기	87
가. 개인키 생성 및 CSR 생성 방법	88
나. 인증서 설치 방법	90
다. 웹사이트 적용	94
라. SSL 인증서 개인키 추출 방법	94
III. 이중화된 웹서버 SSL 적용방법	96
3.1. IIS 서버의 경우	96
3.2. Apache 서버의 경우	.01
3.3. WebToB 서버의 경우	.02
3.4. iPlanet 서버의 경우1	.04
3.5. Tomcat 서버의 경우	.05
Ⅳ. SSL 적용여부 확인방법	06
4.1. 보안서버 구축여부 확인방법1	.06
4.2. 보안서버 적용전후 보안통신 비교	.07
V. 웹페이지 SSL 구현방법	08
5.1. 전체페이지 암호화하기	.09
5.2. 페이지별 암호화하기	11
5.3. 프레임별 암호화하기	.11
Ⅵ. 보안서버 구축 시 유의사항	13
Ⅶ. 보안서버 FAQ	14
7.1. 제도 관련 FAQ	.14
가. 행정전자서명센터(GPKI)은 어떤 기관인가요?	14
나. 보안서버는 무엇이고, 구축하지 않으면 어떻게 되나요?	14
다. 보안서버는 구축의 의무인가요? 관련 법조항이 뭔가요?	14
붙임1. SSL인증서 발급 절차	15
붙임2. 보안서버 구축 후 오류발생 시 참고사항	19
<제·개정 연 혁> ··································	27

# I 보안서버 개요

### 1. 보안서버 정의

보안서버(SSL)란? 인터넷 상에서 사용자 PC와 웹서버 사이에 송수신되는 개인 정보 를 암호화하여 전송하는 웹서버를 의미합니다. 그러므로 보안서버를 구축하는 것은 웹서버와 사용자 PC간의 신뢰를 형성하고, 웹 브라우저와 웹서버간에 전송되는 데 이터의 암/복호화를 통해 보안채널을 형성하여 안전한 전자거래를 보장합니다.

#### **<u>\* SSL(Secure Sockets Layer)</u>**



### 2. 보안서버 구축 필요성

#### 가. 정보유출(Sniffing) 방지

공용 네트워크(학교, PC방, 회사 등)를 사용하는 PC에서 보안서버가 구축되지 않은 사이트를 접속할 경우, 개인정보가 타인에게 스니핑 툴(Sniffing tool) 등에 의해 손 쉽게 노출될 가능성이 있습니다.

#### 나. 피싱(Phishing) 방지 및 웹 사이트 신뢰도 향상

보안서버가 구축된 사이트를 대상으로 피싱(Phishing) 공격을 시도하기는 상대적으 로 어려워 피싱에 의한 피해를 줄일 뿐만 아니라 이용자의 신뢰를 얻을 수 있어 기 관의 이미지를 부각시킬 수 있습니다.

## 3. 보안서버 적용 범위

개인정보보호법 제2조(정의) "개인정보"란 살아있는 개인에 관한 정보로서 성명, 주 민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특 정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합 하여 알아볼 수 있는것을 포 함한다)를 말한다.

"인터넷에서 사용되는 대표적인 개인정보의 예시로는 로그인시 아이디, 비밀번호, 회원가입시 주민번호, 인터넷뱅킹시 계좌번호, 계좌 비밀번호등이 해당됩니다." 또한 게시판 등에서 사용하는 성명, 이메일, 연락처 등도 개인을 식별할 수 있는 정보로 서 개인정보에 해당됩니다.

#### 개인정보보호법 제24조(고유식별정보의 처리 제한)

③ 개인정보처리자가 제1항 각 호에 따라 고유식별 정보를 처리하는 경우에는 그 고유식별 정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 대통령령으로 정하는 바에 따라 암호화 등 안전성 확보에 필요한 조치를 하여야 한다.

#### ※ 고유식별정보 : 주민번호, 여권번호, 외국인등록번호, 운전면허번호

이러한 개인정보를 안전하게 관리하기 위해서는 해당 개인정보를 포함하고 있는 웹페이지에 대해 보안서버(암호화 통신)를 적용해야 합니다.

### 4. 보안서버 적용 대상

- 행정기관

### 5. SSL인증서 신청절차

가. 웹서버 종류 확인

○ 현재 운용하고 있는 웹사이트의 웹서버의 종류를 확인합니다.

☞ GPKI에서 지원하는 웹서버는 IIS, Apache, WebtoB, iPlanet, Tomcat입니다.

#### 나. 행정전자서명(SSL인증서) 신청서 작성

○ 행정전자서명 인증관리센터 홈페이지(http://www.gpki.go.kr) 중앙 하단부

[인증서신청 관련양식] → [행정전자서명신청서] → [기관용 신청서] 다운로드 후 작성

<sup>☞</sup> 인증서 종류(□ SSL)에 기재(■ 또는, ☑), 인증서관리담당 및 사용 웹서버 정보(예시: IIS6.0, Apache2.1)를 정확하게 작성

#### 다. 공문 발송

○ 행정전자서명 신청서를 첨부하여 [외부조직]

```
[정부산하기관 및 위원회] → [한국지역정보개발원] → [지역정보센터]
→ "정보기반과"로 공문 발송
```

☞ 공문 발송 후, 사전 점검 사항 : 시스템(웹서버)에 https 포트(기본 : 443)가 활성화 되었는지 확인 (방화벽과 L4스위치 등 장비에 해당 포트가 허용 되었는지 확인)

- 라. CSR(Certificate Signing Request) 생성
  - CSR은 SSL인증서를 발급받기 위하여 필요한 웹서버의 정보를 담고 있는
     인증서 신청형식 파일(웹 서버별 CSR 생성방법 참조)
- 마. 인증서 등록 안내 수신(신청 후 2일 이내)

○ 공문접수 후, 신청서 등록 처리 후 기관 담당자에게 발급 안내 메일 및 SMS 발송

#### 바. SSL인증서 발급(인증서 등록 후 15일 이내)

- 행정전자서명 인증관리센터 홈페이지(http://www.gpki.go.kr) [유선인증서 → 발급]
   메뉴에 접속하여 '라' 에서 생성한 CSR 파일을 첨부하여 SSL인증서를 발급
   (다운로드) 받습니다.
- IE8.0버전이나 Windows7을 이용하실 경우 IE의 "도구→ 인터넷옵션 → 보안
   → 신뢰할수 있는 사이트 → 사이트"에 www.gpki.go.kr과 gcert.gpki.go.kr을 등록해야 합니다.
- ☞ 인증서는 C:/gpki/certificate/class1/ 폴더의 domain.p7b 파일입니다.

# 6. 보안서버 구축절차

보안서버(SSL인증서 탑재) 구축 절차는 다음과 같습니다.

① 인증서 파일 웹서버로 이동 (domain.p7b)

행정망에서 받은 domain.p7b 파일을 웹서버로 이동시킵니다.

② 체인인증서內 Root CA, CA131000001, domain 인증서 3개 추출

발급받은 인증서 파일 (\*.p7b)을 웹서버에서 요구하는 형식에 따라 체인 인증서 형태 로 추출합니다.

③ 웹 서버에 설치

※ 웹서버 종류 및 버전에 따른 설치 방식 참조

④ 웹프로그램 적용

웹프로그램 구성에 맞게 **웹프로그램 소스를 수정**하여 암호화 통신 기능이 정상 동작 되도록 구성합니다.

⑤ 웹방화벽 및 개인정보 필터링 시스템에 개인키 적용

웹방화벽 및 개인정보 필터링 시스템을 운영시 **개인키를 추출 또는 복제**하여 해당 시스템에 적용합니다..

<표 1-1> 보안서버(SSL인증서 탑재) 구축 절차

- 유닉스 기반 웹서버를 사용하셔도 3개의 인증서 추출 작업은 WINDOWS O/S에서 작업하신 다음 이동하셔도 됩니다.
- ② 웹프로그램 적용시 HTTP를 사용하고 있는 링크 및 폼전송 URL을 HTTPS로 변경하셔야 하며 HTTPS를 사용하는 페이지에 HTTP가 포함되면 '보안경고'가 발생합니다.
- 보안서버 설치 적용 후 웹서버 접속 시 발생되는 오류나 문의사항은 행정전자서명 인증센터 홈페이지(<u>www.gpki.go.kr</u>) 자료실의 기술자료 및 FAQ를 참조하시거나, 안내센터로 문의하시기 바랍니다.
   (전화: 02-818-3021, e-Mail : gpki@klid.or.kr )

- 8 -

# 7. 보안서버 설치파일 설명

#### 7. CSR (Certificate Signing Request)

CSR은 Certificate Signing Request(인증서 서명요청)의 약자로, 인증서 발급을 위해 필요한 정보를 담고 있는 인증서 신청형식 데이터입니다. CSR에 포함되는 내용으로는 개인키 생성 단계에서 만들어지는 개인키(Private Key)와 공개키(Public Key)의 키쌍 중에서 공개키가 포함되며 인증서가 적용되는 도메인에 대한 정보 등이 포함됩니다. 바른 CSR을 생성하기 위해서는 해당 도메인 정보를 정확히 넣어주셔야 합니다. 또한 개인키 및 CSR의 생성을 여러번 수행하셨을 경우 사용하실 개인키와 일치하는 CSR을 이용하여 SSL 인증서를 발급절차에 따라 발급받으시면 됩니다.

만약, 알려주신 CSR의 내용이 사용할 개인키가 아닌 다른 개인키를 이용하여 생성되 었을 경우, 발급된 인증서가 개인키와 일치하지 않아 '키쌍이 맞지 않는 오류'가 발생 합니다. 이 문제를 해결하기 위해서는 개인키 생성 및 CSR 생성 과정부터 다시 시작해 서 해당 인증서를 재발급 받아야 합니다.

항목 웹서버	IIS	아파치	톰켓	WebToB	iPlanet
별칭	사용	-	사용	-	-
비트길이	2048	2048	2048	2048	2048
조직(O)	Government of Korea				
조직단위 (OU)	Group of Server				
사이트명 (CN)	도메인명	도메인명	도메인명	도메인명	도메인명
국가(C)	KR	KR	KR	KR	KR
지역(ST)	GPKI	-	-	-	-
시군구(L)	GPKI	-	-	-	-
이메일	-	-	-	-	-

나. (	CSR	생	성지	입	력	값
------	-----	---	----	---	---	---

※ CSR 생성시 비어있는 항목(-)에 값을 입력하시면 발급시 에러코드(114)가 발생합니다.

다. 보안서버 구축시 필요한 파일

형태	저장 파일	내용	비고
개인키 파일	개인키	인증서를 해독하는 개인키, 비밀키 저장	
CSR 파일	domain.csr	p7b 파일을 받기위한 인증 요청 파일	임시
	Root CA 인증서	인증서 체인의 맨 위에 있는 신뢰된 최상 위 인증서	Root CA
p7b 파일	CA Chain 인증서	인증서 발급기관이 서명한 일련의 계층적 인증서	CA131000001
	서버 인증서	개인키를 기반으로 생성된 인증서	domain.go.kr

※ 보안서버 구축시 웹서버에 설정하는 파일은 개인키 파일과 p7b파일 2개이며 CSR 파일은 p7b파일 발급 받기 위한 임시 신청 파일입니다.

(인증서 복제시 개인키 파일과 p7b파일 2개만 있으면 됩니다)

※ Apache,WebtoB서버의 p7b→pem 변환작업은 OpenSSL 프로그램을 이용합니다. -11 -1 -1

\*

개인기								
				Root CA 인증서				
CSR	$\rightarrow$	P7B	$\rightarrow$	CA Chain 인증서				
	(발급)		(변환)	서버 인증서				

### 라. 웹서버별 보안서버 구축 관련 파일 형태

항목 웹서버	IIS	아파치	톰켓	WebToB	iPlanet
개인키	내장	파일	내장	파일	내장
Root CA 인증서	파일	파일	파일	-	입력
CA Chain 인증서	파일	파일	파일	파일	입력
서버 인증서	파일	파일	파일	파일	입력

※ 인증서를 다른곳에서 사용하려면 개인키를 복제해야 하는데 IIS, 톰켓, iPlanet은 파일형태가 아니기 때문에 별도로 '개인키 내보내기' 작업을 통해 파일로 변환 시켜야 합니다.

# Ⅱ 웹서버 종류별 SSL 구축방법

# 2.1. IIS 6.0 이하 웹서버에서 보안서버 구축하기

#### 가. 개인키 생성 및 CSR 생성 방법

- ① [웹사이트 속성] 메뉴를 선택합니다.
  - "시작 → 프로그램 → 관리도구 → 인터넷 서비스 관리자 → 웹사이트 →
     마우스 오른쪽 버튼 클릭 후 속성"을 선택합니다.



② 등록정보 화면에서 "디렉터리 보안" 탭을 클릭한 후 서버 인증서를 클릭합니다.

cho,klid,or,kr 등록 정보		? ×
에 사이트	벡터리 정 오류	문서 ASP,NET
익명 액세스 및 인증 제어		
이 리소스에 대해 역명 액세스를 가능하게 하고 인종 방법을 편집합니다.	[ 편집	(E)
- _ IP 주소 및 도메인 이름 제한		
· · · · · · · · · · · · · · · · · · ·		
	편집	3(D
보안 통신		
이 리소스에 액세스할 때 보안 통신을 요구	서버 인	증서( <u>S</u> )
	인증세	보기(⊻)
	편집	H( <u>D</u> )
확인 취소	적용( <u>A</u> )	도움말

③ 웹 서버 인증서 마법사를 시작합니다.

- 다음(N) 버튼을 클릭하여 계속 진행합니다.



- "새 인증서를 만듭니다(C)"를 선택한 후, 다음(N) 버튼을 클릭합니다.



- "요청을 준비하지만 나중에 보냅니다"를 선택합니다.

IIS 인증서 마법사			×
요청 연기 또는 즉시 요청 요청을 준비했다가 나중에 보내거나 즉시 보낼 수 :	있습니다.		
인증서 요청을 준비했다가 나중에 보낼지, 아니면	즉시 보낼지를	선택하십시오.	
● 요청을 지금 준비하지만 나중에 보냅니다(P).			
○ 온라인 인증 기관에 요청을 즉시 보냅니다(S).			
	< 뒤로( <u>B</u> )	다음( <u>N</u> ) >	취소

- 인증서를 만들 이름을 입력하시기 바랍니다.

이름은 인증서의 별칭이므로 쉬운 것으로 선정, **임의로 입력**하시기 바랍니다. 인증서 키의 길이는 **2,048**로 하시면 됩니다.

IIS 인증서 마법사	×
이름 및 보안 설정 새 인증서에는 이를 및 특정 비트 길이가 있어야 합니다.	
새 인증서 미름을 입력하십시오. 미름은 쉽게 기억하고 참조할 수 있어야 합니다. 미름(M): [웹 사이트]	
암호화 키의 비트 길이는 인증서의 암호화 강도를 결정합니다. 비트 길이가 길수록 보안은 강해지지만 성능은 감소됩니다. 비트 길이(님):	
[2048 ▼] IT SGC(Server Gated Cryptography) 인증서(내보내기 버전만)(S) IT 이 인증서에 대해 암호화 서비스 공급자(CSP) 선택(P)	
< 뒤로( <u>B</u> ) [다음( <u>N</u> ) > 취	소

- 조직 및 조직 구성단위를 입력합니다.
- 대 소문자, 띄어쓰기 철자를 정확히 입력하여야 합니다.
- ※ 조직(O) : **<Government of Korea**> 라고 입력합니다.

조직	구성단위(U)	:	<group< th=""><th>of</th><th>Server&gt;</th><th>라고</th><th>입력합니다.</th></group<>	of	Server>	라고	입력합니다.
----	---------	---	---	----	---------	----	--------

IIS 인증서 마법사	×
조직 정보 인증서에는 다른 조직과 구별되도록 귀하의 조직에 대한 정보가 있어야 합니다.	
조직 이름 및 조직 구성 단위를 선택하거나 입력하십시오. 일반적으로 회사의 공식 이름 또는 부서 이름입니다. 자세한 내용은 인증 기관의 웹 사이트를 참조하십시오. 조직( <u>0</u> ):	
Government of Korea	
조직 구성 단위(山): Group of Server	
< 뒤로( <u>B</u> ) 다음( <u>N</u> ) > 취소	

- 도메인 이름을 입력하시기 바랍니다.

※ SSL인증서를 적용할 도메인 이름을 입력하면 됩니다.

예) 단일 인증서 : www.klid.or.kr (www를 꼭 붙이세요) 와일드카드 인증서 : \*.klid.or.kr

IIS 인증서 마법사	×
사이트 일반 이름 웹 사이트 일반 이름은 정식 도메인 이름입니다.	
귀하의 사이트의 일반 미를을 입력하십시오. 서비가 인터넷에 있으면 올바른 DNS 미를을 사용하십시오. 서비가 인트라넷에 있으면 그 컴퓨터의 NetBIOS 미를을 사용할 수 있습니 다.	
일반 이름이 바뀌면 새 인증서를 받아야 합니다.	
일반 미름( <u>C</u> ):	
www.klid.or.kr	
< 뒤로( <u>B</u> ) 다음( <u>N</u> )> 취소	

- 지역 정보(구/군/시)를 입력합니다.
- ※ 국가/지역은 default로 KR(대한민국)입니다. 시/도와 구/군/시에 "GPKI"를 입력 후 다음(N) 버튼을 활성화시켜 계속 진행하시면 됩니다.

IIS 인증서 마법사	×
<b>지역 정보</b> 인증 기관에는 다음 지역 정보가 필요합니다.	
국가/지역( <u>C</u> ):  KR (대한민국)	
GPKI	]
	3
시/도 및 구/군/시는 공식 이름이어야 하며 약어를 사용하면 안 됩니다.	
< 뒤로( <u>B</u> ) 다음( <u>N</u> ) >	취소

- 인증서 요청 파일(CSR)을 저장합니다. default 이름을 사용하시면 됩니다.

X
찾아보기(B),,,
음( <u>N</u> ) > 취소

- 등록한 내용을 다시 한 번 **확인**합니다.

IIS 인증서 마법사 요청 파일 요약 요청 파일을 생성하기로 했;	음니다.	×
다음 요청을 생성하려면 [[ 파일 이름: c:\certreq.t 요청에는 다음 정보가 포함!	음]을 누르십시오, xt 텍니다.	~
발급 대상 미를 국가/지역 시/도 구/고/시 조직 구성 단위	www.klid.or.kr 웹 사이트 KR Government of Korea Group of Server	
	< 뒤로(B) [대용(N)	> 취소

- 인증서 요청 파일(CSR) 생성을 완료합니다.



④ SSL인증서 발급

☞ 보안서버 구축가이드 'SSL 인증서 발급절차 안내'에 따라 해당 신청서를 작성하여 공문을 보내시고 인증센터에서 '인증서 등록후' 이메일이나 휴대폰 문자메시 지로 전송되는 발급안내 내용을 확인하신 후 행정전자서명 인증관리센터 홈페이지 (www.gpki.go.kr) [유선인증서>발급] 메뉴에서 발급하면 됩니다.

<붙임1 SSL인증서 발급 절차 참고>

### 나. 인증서 설치 방법

- ① 발급받은 인증서를 확인합니다.
  - C:\GPKI\certificate\class1 디렉터리에 해당 <*cn name : domain*>.p7b 파일이 있는지 확인합니다. (예: www.gpki.go.kr.p7b)
- ② pkcs#7 ⇒ cer 변환
  - 인증서 파일 <p7b filename>을 윈도우 환경에서 더블클릭하여 파일을 open합 니다. 아래와 같은 창이 열립니다.

📟 민증서					
파일(E) 동작( <u>A</u> ) 보기( <u>V</u> ) 도움말( <u>H</u> )					
	]				
한 인증서 - 현재 사용자 금- 급 C:₩DOCUMENTS AND SE 인증서	발급 대상 A (131000001) (140, kid, or, kr (150, kid, or, kr (150, kr) (150, kr)	부모 Ra C, Ra	급자 bot CA A131000001 bot CA	<u>만료 날짜</u> 2012-03-28 2010-08-01 2012-04-21	
	•				Þ
C:₩DOCUMENTS AND SETTINGS	₩ADMINISTRATOR₩H	탕 화면₩CHO,			

- 인증서를 선택(예: CA131000001) 후 마우스 우측 버튼을 클릭하여 "모든작업(K) - 내보내기"를 클릭합니다.

<mark>'a certmgr - [인증시 - 파일₩C:₩GPKI₩CE</mark> 파일(F) 동작(A) 보기( <u>V</u> ) 도움말(H) ← → 1 12 114 『참 12 12 12 12 11	ERTIFICATE WCLASS I WTES	T2,GPKI,GO.KB,P7B₩인증서		<u>_   ×</u>
할 인증서 - 파일 □ C:₩GPKI₩CERTIFICATE₩CLASSI₩TE └ 인증서	발급 대상 / Image: Construction of the second	I 발급자 Root CA Root CA 열기 내보내기	만료 날자 2010-07-21 2012-04-21 2010-04-08	용도 (모두> (모두> 시비 민증
	<u> </u>			<u> </u>

- "DER로 인코딩된 X.509바이너리(.CER)"을 선택하여 인증서를 저장합니다.

사용	할 형식을 선택하신시오
	● DER로 인코드된 X 509 바이너리(CER)(D)
	이며 기구도 전포드린 지903(JEFING) 이 암호화 메시지 구문 표준 - PKCS #7 인증서 (,P7B)( <u>C</u> )
	□ 가능하면 인증 경로에 있는 인증서 모두 포함(!)
	○ 개인 정보 교환 - PKCS #12(,PFX)( <u>P</u> ) ■ 가능하면 인증 경로에 있는 인증서 모두 포함(U)
	■ 강력한 보호 사용(Internet Explorer 5.0, NT 4.0 SP4 미상 필요)(E)
	🗖 내보내기가 완료되면 개인 키 삭제(区)

- ☞ 3개 인증서(RootCA인증서, CA인증서, SSL인증서)를 모두 "DER로 인코딩된 X.509바이너리(.CER)"으로 변환하여 저장합니다.
- ③ 3개 인증서중 SSL인증서를 웹 사이트에 적용합니다.
  - "시작 → 프로그램 → 관리도구 → 인터넷 서비스 관리자 → 웹사이트 → 마우스
     오른쪽 버튼 클릭 후 속성"을 선택합니다.



- 등록정보 화면에서 "디렉터리 보안" 탭을 클릭한 후 서버 인증서를 클릭합니다.

cho,klid,or,kr 등록 정보	? ×
웹 사이트 ISAPI 필터 홈 디릭 디렉터리 보안 HTTP 헤더 사용자 지	렉터리 문서  정 오류 ASP,NET
의명 액세스 및 인증 제어 이 리송숭엖 대행 원명 액세수를 가능하게 하고 한중 방법을 편집합니다.	편집(E)
- 	
응 IP 중소난 원터넷 독세인 민류를 사용하여 미리소스에 대한 독세스를 취가하거나 거 부합니다.	편집(1)
보안 통신 이 리솔수에 액세수할 때 보안 통신을 요구 아고 클라이언트 인증서를 사용합니다.	<mark>서버 인증서(<u>S</u>)</mark> 인증서 보기(⊻) 편집(₽)
 확인 취소	적용( <u>A</u> ) 도움말

- 다음(N) 버튼을 클릭하여 계속 진행한다.



- 다음(N) 버튼을 클릭하여 계속 진행한다.

IIS 인증서 마법사		×
<b>보류 중인 인증서 요청</b> 보류 중인 인증서 요청은 인증 기관이 아직 응답하	지 않은 요청입니다.	
인증서 요청을 보류 중입니다. 어떻게 하시겠습니지 ☞ <u>보류 중인 요청을 처리한 다음 인증서를 설치할</u> ☞ 보류 중인 요청을 삭제합니다( <u>D</u> ).	H? <u>[[[[KP]]</u> ]	
	< 뒤로( <u>B</u> ) 다음( <u>N</u> ) >	취소

- (와일드카드)SSL인증서 파일(\*.p7b)에서 내보낸 SSL인증서(도메인인증서)를 선택한 후, 다음(N) 버튼을 클릭하여 계속 진행하시면 됩니다.



- 이제 SSL인증서의 설치가 완료되었습니다.

IIS 인증서 마법사		×
	웹 서버 인증서 마법사 완료	
	웹 서버 인증서 마법사를 성공적으로 완료했습니다.	
	현재 이 서버에 인증서가 설치되었습니다.	
	마법사를 다시 사용하여 지금 만든 새 인증서를 나중에 갱신 하거나 바꾸거나 삭제할 수 있습니다.	
	마법사를 끝내려면 [마침]을 누르십시오.	
	< 뒤로(B) <b>마침</b> 휘소	

④ SSL인증서 설치가 완료되었으면, IIS 서버를 재 구동 시킵니다. - 시작 → 실행 → "cmd" 명령 입력 후 확인 버튼을 클릭 합니다.

실행			<u>?×</u>
	프로그램, 폴더, 문서, 9	또는 인터넷 리소스 (	비름을 입력하십시오.
열기( <u>0</u> ):	eme		
	확인	취소	찾아보기( <u>B</u> )

- "iisreset /restart" 명령 입력후 엔터를 치면 IIS 서버의 서비스가 재구동 됩니다.



- ⑤ 3개 인증서중 RootCA 인증서 및 CA 인증서를 웹 서버에 설치하기 위하여 mmc 콘솔 창을 실행합니다.
  - 시작 → 실행 → "mmc" 명령 입력 후 확인 버튼 클릭 → 파일 → 스냅인 추가/ 제거를 선택합니다.

🚡 콘솔1	
파일(F) 동작(A) 보기(V) 즐겨찾기(Q) 칭 새로 만들기(N) Ctrl+ 열기(Q) Ctrl+	(W) 도움말(H) 이
저장( <u>S</u> ) Ctrl+ 다른 이름으로 저장( <u>A</u> )	
스냅인 추가/제거( <u>M</u> ) Ctrl+	현재 보기에서 표시할 항목이 없습니다.
1 C:\WINDOWS\\Certmgr.msc 2 C:\WINDOWS\\inetsrv\iis.msc 3 C:\WINDOWS\\inetsrv\iis.msc 4 C:\WINDOWS\\inetscompmgmt.msc	
끝내기( <u>X</u> )	
스냅인 콘솔에서 스냅인을 추가하거나 제거하도록	설정합니다.

- 스냅인 추가/제거 창에서 추가(D) 버튼을 클릭합니다.

스냅인 추가/제거 ? 🔀
독립 실행형   확장
콘솔에서 독립 실행형 스냅인을 추가 또는 제거하려면 이 페이지를 사용하십시오.
스냅인 추가 대상( <u>S</u> ): 🔄 콘솔 루트 🔹 🗾
추 <b>가(<u>D</u>)</b> 제거( <u>B</u> ) 정보( <u>B</u> )
확인 취소

- 인증서를 선택한 후 추가(A) 버튼을 클릭합니다.

독립 실행형 스냅인 추가	? ×
사용 가능한 독립 실행형 스냅인:	
스냅인	공급업체 🔺
🖏 서비스	Microsoft Corporation
📓 성능 로그 및 경고	Microsoft Corporation
💽 웹 주소에 연결	Microsoft Corporation
🚽 🗃 이동식 저장소 관리	Microsoft Corporation
💼 이벤트 뷰어	Microsoft Corporation
🔽 이덴신 서비스	Microsoft Corporation, I
교민증사	Microsoft Corporation 🛛 🗖
📢 인터넷 정보 서비스	Microsoft Corporation
🚊 장치 관리자	Microsoft Corporation
্রিসিয়াতা সালা সালা	Microsoft Corporation
설명 인증서 스냅인은 인증서 저장소의 내 에서 찾아보게 합니다.	용을 사용자 자신, 서비스 또는 컴퓨터
	추가( <u>A</u> ) 닫기( <u>C</u> )

- 스냅인 관리할 인증서 대상을 "컴퓨터 계정"으로 체크한 후 다음(N) 버튼을 클릭합니다.

인증서 스냅인		×
이 스법인이 항상 관리할 인증서 대상: 이 내 사용자 계정( <u>M</u> ) 이 서비스 계정(S) 이 <u>컴퓨터 계정(C)</u>		
	< 뒤로(B) <b>다음(<u>N</u>) &gt;</b>	·····································

- 마침 버튼을 클릭한 후 스냅인 추가/제거 창에서 확인 버튼을 클릭한다.

	_
이 스냅인이 관리할 컴퓨터를 선택하십시오.	
○ 로컬 컴퓨터: (이 콘솔이 실행되고 있는 컴퓨터)(L)	
○ 다른 컴퓨터(▲):           찾아보기(且)	
□ 명령줄에서 시작할 때 선택된 컴퓨터를 변경할 수 있음. 사용자가 콘솔을 저장할 때만 해당(₩)	
< 뒤로( <u>B</u> ) 마침 취소	
스냅인 추가/제거 ?	×
독립 실행형   확장	
콘솔에서 독립 실행형 스냅인을 추가 또는 제거하려면 이 페이지를 사용하십시오.	
콘솔에서 독립 실행형 스냅인을 추가 또는 제거하려면 이 페이지를 사용하십시오. 스냅인 추가 대상( <u>S</u> ): 🔄 콘솔 루트	
콘솔에서 독립 실행형 스냅인을 추가 또는 제거하려면 이 페이지를 사용하십시오. 스냅인 추가 대상(S): 🔄 콘솔 루트 🔹 📷	
콘솔에서 독립 실행형 스냅인을 추가 또는 제거하려면 이 페이지를 사용하십시오. 스냅인 추가 대상(§): 🔄 콘솔 루트 💿 📷	
콘솔에서 독립 실행형 스냅인을 추가 또는 제거하려면 이 페이지를 사용하십시오. 스냅인 추가 대상(S): 🔄 콘솔 루트 💌 💌	
콘솔에서 독립 실행형 스냅인을 추가 또는 제거하려면 이 페이지를 사용하십시오. 스냅인 추가 대상(S): 🔄 콘솔 루트 💌 📷	
콘솔에서 독립 실행형 스냅인을 추가 또는 제거하려면 이 페이지를 사용하십시오. 스냅인 추가 대상(S): 🔄 콘솔 루트 💌 📧	
본솔에서 독립 실행형 스냅인을 추가 또는 제거하려면 이 페이지를 사용하십시오. 스냅인 추가 대상(S): 중국을 루트 중 중 (중) (로컬 컴퓨터) 중 (문질 컴퓨터) 중 (문질 컴퓨터) 중 (문질 문질 문	

- ⑥ 3개 인증서중 RootCA 및 CA 인증서를 웹 서버에 설치합니다.
  - "신뢰된 루트 인증기관 → 마우스 오른쪽 버튼 클릭 후 모든 작업 → 가져오기"를 선택합니다.

🚡 콘솔1			
파일( <u>F</u> ) 동작( <u>A</u> ) 보기(⊻)	즐겨찾기( <u>0</u> ) 창( <u>₩</u> ) 도움말( <u>H</u> )		
⇐ → 🗈 🖬 💼 🙆 [	2 🛛 🕄 💷		
🌇 콘솔 루트₩인증서(로컬 컴	뜪터)₩신뢰된 루트 인증 기관		_ 🗆 🗵
- 콘솔 루트 - ഈ 인증서(로컬 컴퓨터) 개인 시뢰된 루트 인증 이증서	개체 유형		
☞ 🙆 엔터프라이즈 신로	모든 작업( <u>K</u> ) ▶ 인증서 찾기( <u>C</u> )	1	
<ul> <li>□ ····································</li></ul>	보기( <u>V</u> ) · · · · · · · · · · · · · · · · · · ·		
표~ 🛄 공급 업체 루트 인 🗍	새 작업 창 보기( <u>T</u> )		
⊕ <mark>`</mark> 인증서 등록 요청 ⊕ <b>`</b> SPC	새로 고침(E) 목록 내보내기( <u>L</u> )		
	도움말( <u>비</u> )		
•			
인증서를 저장소에 추가합니다			

- (와일드카드)SSL인증서 파일(\*.p7b)에서 내보낸 RootCA인증서를 선택한 후 다음 버튼을 클릭하여 계속 진행합니다.

인증서 가져오기 마법사	×
<b>가져올 파일</b> 가져올 파일을 지정하십시오,	
파일 이름( <u>F</u> ): [C:₩Documents and Settings₩Administrator₩H	탕 화면₩GPKICA.c
참고: 다음 형식으로 한 파일에 두 개 이상의 인증서 개인 정보 교환- PKCS #12 (,PFX,,P12)	 I가 저장될 수 있습니다.
암호화 메시지 구문 표준- PKCS #7 인증서(.P76 Microsoft 일련 인증서 저장소(.SST)	8)
	뒤로( <u>B</u> ) 다음( <u>N</u> ) > 취소

- 다음 버튼을 클릭하여 계속 진행합니다.

인증서 가져오기 마법사	×
<b>인증서 저장소</b> 인증서 저장소는 인증서를 저장하는 시스템 영역입니다.	
Windows가 자동으로 인증서 저장소를 선택하거나 사용자가 인증서 위치를 지정할 수 있습니다.	
· 이 이중세 종료 기준으로 이중세 저장소를 자동으로 선택(U)	
☑ 모든 인증서를 다음 저장소에 저장(P)	
인증서 저장소:	
신뢰된 루트 인증 기관 찾아보기( <u>B</u> )	
< 뒤로( <u>B</u> ) 다음( <u>N</u> ) > 취소	

- 그러면, 인증서 설치가 완료됩니다. (와일드카드)SSL인증서 파일(\*.p7b)에서 내보낸 CA인증서를 설치하기 위해서는 ⑥번을 반복하면 됩니다.

인증서 가져오기 마법사		×
	인증서 가져오기 마법사 완료	
	인증서 가져오기 마법사를 완료했습니다.	
	다음 설정을 지정했습니다.	
STATES INCOME	사용자가 선택한 인증서 저장소 신뢰된 루트 인증 기관 내용 인증서	
	파일 이름 C:₩Documents and Settin	
	< 뒤로( <u>B</u> ) 마침 취소	
		100

⑦ 이제 SSL인증서의 설치가 완료되었으며, 웹 브라우저를 통해 SSL인증서 설치
 정상 유무를 확인할 수 있습니다. (예. https://cho.klid.or.kr)

ØSL인증서 테스트 - Windows Internet Explorer	
G → e https://cho.klid.or.kr/	▼ 🔒
파일(E) 편집(E) 보기(V) 즐겨찾기(A) 도구(I) 도움말(H) 삶 삶 《 SSL인증서 테스트	💐 웹 사이트 ID
SSL인증서 테스트	MOGAHA Govt of Korea 에서 이 사이트를 확인한 결과: cho.klid.or.kr 서비에 대한 연결이 암호화되었습니다. 신뢰할 수 있는 사이트
	인증서 보기

#### 다. 웹사이트 적용하기

웹사이트 이용시 암호화통신이 가능하도록 웹 프로그램을 수정합니다. ☞ 구축가이드 V장을 참조

### 라. SSL 인증서 개인키 추출 방법

※ 웹방화벽 및 개인정보 필터링에 적용시 필요

- ① mmc 콘솔 창을 실행합니다.
  - 시작 → 실행 → "mmc" 명령 입력 후 확인 버튼 클릭 → 파일 → 스냅인 추가/ 제거를 선택합니다.

à	[1] 동작(A) 보기(Y) 물겨찾기(Q) 창()	() 도움말(出)
H	새로 만들기(NL) Ctrl+N 열기(Q) Ctrl+O 저장(S) Ctrl+S 다른 이름으로 저장(A)	>
	스냅인 추가/제거( <u>M</u> ) Ctrl+M 옵션( <u>P</u> )	
	1 C:#WINDOWSWWservices.msc 2 C:#WINDOWSWWinetsrvWiis.msc 3 C:#WINDOWSWWcertmgr.msc 4 C:#WINDOWSWWdevmgmt.msc	_
-	끝내기(X)	

- 스냅인 추가/제거 창에서 추가(D) 버튼을 클릭합니다.

스냅인 추가/제거	? 🗙
독립 실행형 확장	
콘솔에서 독립 실행형 스냅인을 추가 또는 제거하려면 이 페이지를 사용하십	시오.
스냅인 추가 대상( <u>S</u> ):	
설명	
추가( <u>D</u> ) 제거( <u>B</u> ) 정보( <u>B</u> )	
확인 <b>취</b>	소

- 인증서를 선택한 후 추가(A) 버튼을 클릭합니다.

독립 실행형 스냅민 추가	?	
사용 가능한 독립 실행형 스냅인:		
스냅인	공급업체	^
🗑 이벤트 뷰어	Microsoft Corporation	
💁 인덱싱 서비스	Microsoft Corporation, I	
· · · · · · · · · · · · · · · · · · ·	Microsoft Corporation	
🖥 인터넷 정보 서비스	Microsoft Corporation	
🚊 장치 관리자	Microsoft Corporation	
🛒 정책의 결과 집합	Microsoft Corporation	
📃 컴퓨터 관리	Microsoft Corporation	
플폴더	Microsoft Corporation	-
g≟ ActiveX 컨트롤	Microsoft Corporation	~
설명 인증서 스냅인은 인증서 저장소의 에서 찾아보게 합니다.	내용을 사용자 자신, 서비스 또는 컴퓨터	H
	추가( <u>A</u> ) 닫기( <u>C</u> )	

- 스냅인 관리할 인증서 대상을 "컴퓨터 계정"으로 체크한 후 다음(N) 버튼을 클릭합니다.

인증처 스냅인	X
이 스냅인이 항상 관리할 인증서 대상: ○ 내 사용자 계정( <u>M</u> ) ○ 서비스 계정( <u>S</u> ) ④ <u>컴퓨터 계정(C)</u>	
< 뒤:	로(B) 다음(N)> 취소

- 기본 선택 유지 후 마침 버튼을 클릭 합니다.

컴퓨터 선택 🛛 🔀
이 스냅인이 관리할 컴퓨터를 선택하십시오. 이 스냅인이 항상 관리할 대상: ④[로컬 컴퓨터: (이 콘솔이 실행되고 있는 컴퓨터)(L)
○다른 컴퓨터(A): 찾아보기(B)
□명령줄에서 시작할 때 선택된 컴퓨터를 변경할 수 있음. 사용자가 콘솔을 저장할 때만 해당(₩)
< 뒤로( <u>B</u> ) 마침 취소

- 마침 버튼을 클릭한 후 스냅인 추가/제거 창에서 확인 버튼을 클릭 합니다.

스냅인 추가/제거 ?	×
독립 실행형 확장	
콘솔에서 독립 실행형 스냅인을 추가 또는 제거하려면 이 페이지를 사용하십시오.	
스냅인 추가 대상(S): 🔄 콘솔 루트 🛛 💌 🛍	
📾 인증서(로컬 컴퓨터)	
설명	
추가( <u>D</u> )] 제거( <u>B</u> ) 정보( <u>B</u> )	
확인 취소	

② 개인키를 내보냅니다.

 "개인" → "인증서" → 발급 대상항목 확인 후 오른쪽 버튼을 클릭 하여 내보내기를 클릭합니다.

- 개인키 내보내기를 선택합니다.

🐕 콘솔) - [콘솔 루트₩민중서(로컬	컴퓨터)₩개민₩민중서]		
1월 파일(E) 동작(A) 보기(V) 즐겨찾. ▲ → 18 00 ¥ Ba ¥ 6명 Ba	시(U) 왕(W) 도움망(H) (에 (m)		X
- 군술 루트       - 군술 루트       - 귀약       - 귀약       - 관람된 루트 인증 기관       - 연태프라이즈 신뢰       - 중개 인증 기관       - 신뢰된 게시자       - 신뢰된 게시자       - 신뢰된 게시자       - 신뢰된 가지 않은 인증서       - 신뢰된 사용자       - 신뢰된 사용자       - 인증서 등록 요청       - SPC	방금 대상 / 문 WWW Code (4 년 년 모든 작업(火) 작가(민) 목사(오) 숙정(민) 도움말(빈)	발급자 CA131000001 열기 서 키로 인증서 요청 같은 키로 인증서 요청 제 키로 인증서 정신 같은 키로 인증서 정신 내보내기	만료 날자 2012-05-17
	<		>
인증서를 내보냅니다.			

- 다음버튼을 클릭 합니다.

인증처 내보내기 마법차	
	인증서 내보내기 마법사 시작
	이 마법사를 사용하면 인증서, 인증서 신뢰 목록, 인증서 해지 목록을 인증서 저장소에서 디스크로 복사할 수 있습니다.
	인증서는 인증 기관이 발급하는 것으로 사용자 신분을 확인 합니다. 인증서에는 데이터를 보호하거나 보안된 네트워크 연결을 하는 데 필요한 정보가 들어 있습니다. 인증서 저장소 는 인증서를 저장하는 시스템 영역입니다.
	계속하려면 [다음]을 클릭하십시오,
	< 뒤로( <u>B</u> ) 다음( <u>N</u> ) > 취소

- "예, 개인키를 내보냅니다(Y)"를 선택합니다.

인증처 내보내기 마법사	×
<b>개인 키 내보내기</b> 인증서와 함께 개인 키를 내보낼 수 있습니다.	
개인 키에는 암호가 설정되어 있습니다. 인증서와 함께 개인 키를 내보내려면 뒤 페이지에 서 암호를 입력해야 합니다.	
인증서와 함께 개인 키를 내보내시겠습니까?	
⊙ 예, 개인 키를 내보냅니다(♡).	
○ 마니오, 개인 키를 내보내지 않습니다( <u>0</u> ).	
< 뒤로( <u>B</u> ) 다음( <u>N</u> ) > 취소	

- 별도의 선택 없이 기본 선택으로 다음 버튼을 클릭 합니다.

민증처 내보내기 마법사 🛛 🔀
<b>파일 내보내기 형식</b> 인증서를 여러 형식으로 내보낼 수 있습니다.
사용할 형식을 선택하십시오. OER로 인코드된 X 509 바이너리(.CER)(D) 64 기수로 인코드된 X 509(.CER)(S) O암호화 메시지 구문 표준 - PKCS #7 인증서 (.P7B)(C) · 가능하면 인증 경로에 있는 인증서 모두 포함(I) · 개인 정보 교환 - PKCS #12(.PFX)(P) · 가능하면 인증 경로에 있는 인증서 모두 포함(U) · 강력한 보호 사용(Internet Explorer 5.0, NT 4.0 SP4 미상 필요)(E) · 내보내기가 완료되면 개인 키 삭제(K)
< 뒤로( <u>B</u> ) 다음( <u>N</u> ) > 취소

- 비밀번호를 지정합니다. (자릿수 제한 없음)

인증서 내보내	1기 마법사	K
<b>암호</b> 보안을 -	유지하려면 암호를 사용하며 개인 키를 보호해야 합니다.	
암호를 1	입력하고 확인하십시오.	
암호	:( <u>P</u> ):	
***	*****	
암호	ː 확인( <u>C</u> ):	
***	*****	
(c		
-	< 뒤로( <u>B</u> ) 다음( <u>N</u> ) > 취소	J

- 내보낼 파일 이름을 지정합니다.

인증처 내보내기 마법사	×
<b>내보낼 파일</b> 내보낼 파일 이름을 지정하십시오. 	
파일 이름(E):	
C:₩ssl₩gpkikey.pfx 찾아보기( <u>B</u> )	
< 뒤로( <u>B</u> ) 다음( <u>N</u> ) > 취소	

- 마침 버튼을 클릭 합니다.

인증처 내보내기 마법사		×
	인증서 내보내기 마법사 완료	
	인증서 내보내기 마법사를 완료했습니다.	
	다음 설정을 지정했습니다.	
	파일 이름 C:₩gpki,pfx 키 내보내기 예	
	인종 경로에 있는 인증서 모두 포함 아니오 파악 형실 Personal Informatic	
and the second		
	<	
-	(위로(B) 마침 취소	J

# 2.2. IIS 7.0 웹서버에서 보안서버 구축하기

### 가. 개인키 생성 및 CSR 생성 방법

- ① 서버인증서 메뉴를 선택합니다.
  - "시작 → 제어판 → 관리도구 → IIS Manager → 서버이름 선택 → 오른쪽의 " 서버 인증서"를 선택합니다.



② "작업메뉴"에서 "인증서 요청 만들기"를 선택합니다.

<ul> <li>IIS(인터넷 정보 서비스) 관리자</li> <li>○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○</li></ul>	-		
파일(F) 보기(V) 도움말(H)			
연결 2 JOOYA-PC(jooya-PC₩jooya) - ② 응용 프로그램 물 ▲ ·③ 사이트	이 기능을 사용하여 웹 서 웹 사이트에 사용할 수 있 관리할 수 있습니다.	너 버가 SSL에 대해 구성된 는 인증서를 요청하고	작업 가져오기 인증서 요청 만들기 인증서 보장 완료
> 😝 Default Web Site	이름	발급 대상	도네한 원동지 만들기 자체 서명된 인증서 만들기 ② 도움말

③ CSR 생성에 필요한 정보를 입력합니다.

이즈서에 깊이하 저님은 1	기정하시지 이 지/도 미 그/구/지도 고시 이르이르 지정체	
인당시에 필요한 영모들 / 약어를 사용하면 안 됩니다 일반 이름(M):	18하십시오. 지/도 및 구/군/지근 중작 이름으도 지정해 가. www.gpki.go.kr	
조직(0):	Government of Korea	
조직 구성 단위(U):	Group of Server	
구/군/시(L)	GPKI	
시/도(S):	GPKI	
국가/지역(R):	KR	

- "암호화 서비스 공급자 속성"창에서, 'Microsoft RSA Schannel Cryptographic Provider' 및 '2048bit'로 선택

인증서 요청	-W-X-
암호화 서비스 공급자 속성	
암호화 서비스 공급자와 비트 길이를 선택합니다. 암호화 키의 비트 길이는 인증서의 암호화 강도를 결정합니다. 비트 길이가 길수록 보안은 강해지지만 성능은 저하됩니다. 악호화 서비스 공급자(5):	
Microsoft RSA SChannel Cryptographic Provider	
비트 길이(B).	
2048 -	
이전(P) 다음(N) 미침	(F) 취소

- 파일이름을 지정하고 인증서 요청 파일(CSR) 생성을 완료합니다.

인증서 요청	S X
파일 이름	
인증서 요청에 사용할 파일 이름을 지정하십시오. 이 정보는 서명을 위해 인증 기관에 전송 될 수 있습니다.	
인증서 요청 파일 이름 지정(R):	
cer.txt	
이전(P) 다음(N) 마침(F)	위소

④ SSL인증서 발급 ☞ 행정전자서명 인증관리센터 홈페이지(www.gpki.go.kr)에서 발급하면 됩니다.

<붙임1 SSL인증서 발급 절차 참고>
## 나. 인증서 설치 방법

- ① 발급받은 인증서를 확인합니다.
  - C:\GPKI\certificate\class1 디렉토리에 해당 <cn name : domain>.p7b 파일이 있는지 확인합니다. (예: www.gpki.go.kr.p7b)
- ② pkcs#7 ⇒ cer 변환
  - 인증서 파일 <p7b filename>을 윈도우 환경에서 더블클릭하여 파일을 open 합니다. 아래와 같은 창이 열립니다.



- 인증서를 선택(예: CA131000001) 후 마우스 우측버튼을 클릭하여
- "모든작업(K) 내보내기"를 클릭하여 "인증서 내보내기 마법사 시작"합니다.



- "DER로 인코딩된 X.509바이너리(.CER)"을 선택합니다.

인증서 내보내기 마법사	X
파일 내보내기 형식	
인증서를 여러 형식으로 내보낼 수 있습니다.	
사용할 형식을 선택하십시오.	
◎ DER로 인코딩된 ×.509 바이너리(.CER)(D)	
◎ Base 64로 인코딩된 X,509(,CER)(S)	
◎ 암호화 메시지 구문 표준 - PKCS #7 인증서 (. <b>P7</b> B)(C)	
□ 가능하면 인증 경로에 있는 인증서 모두 포함(I)	
⑦개인 정보 교환 - PKCS #12(.PFX)(P)	
□ 가능하면 인증 경로에 있는 인증서 모두 포함(U)	
□ 내보내기가 완료되면 개인 키 삭제(K)	
□ 확장된 속성 모두 내보내기(A)	
◎ Microsoft 일련 인증서 저장소(,SST)(T)	
<u>인증서 파일 형식</u> 에 대해 자세히 알아봅니다.	
< 뒤로(B) 다음(N) > 추	소

- 내보낼 파일 이름을 지정합니다.

인증서 내보내기 마법사	×
내보낼 파일 내보낼 파일 이름을 지정하십시오.	
파일 미름(F):	
ca.cer/	찾아보기(R)
	< 뒤로(B) 다음(N) > 취소

☞ 3개 인증서(RootCA인증서, CA인증서, SSL인증서)를 모두 "DER로 인코딩된 X.509바이너리(.CER)"으로 변환하여 저장합니다.

- 내보내	격과르	화이	하니다
- 네모핸	겉서글	41	입어다.

열기 		X
() ♥ ▶ 컴퓨터	▶ 로컬 디스크 (C:) ▶ ssl ▼ ↔ 검색	Q
🖣 구성 👻 🧱 보기 👻	- 개 풀더	?
<ul> <li>즐겨찾기 링크</li> <li>''' 죄근 위치</li> <li>''' 바탕 화면</li> <li>''' 컴퓨터</li> <li>''' 문서</li> <li>''' 음악</li> <li>''' 최근에 변경된 파일</li> <li>'''' 경색</li> <li>''' 공용</li> </ul>	이를 수정한 날짜 유형 크기 국 ca.cer 국 ppki.cer 국 rootca.cer	
파일	이름(N): gpki.cer    (*.cer 열기(0)    취소	•

- ③ 3개 인증서중 SSL인증서를 웹 사이트에 적용합니다.
  - "시작 → 제어판 → 관리도구 → IIS Manager → 서버이름 선택 → 오른쪽의 "서버 인증서"를 선택합니다.
  - "작업"메뉴에서 "인증서 요청 완료"를 선택합니다.

작업

가져오기...

온라인 도움말

오 도움말

인증서 요청 만들기... 인증서 요청 완료... 도메인 인증서 만들기... 자체 서명된 인증서 만들기...

- 내보낸 인증서(gpki.cer)를 선택 후 이름을 입력 합니다.

인증서 요정 완료	2 ×
인증 기관 응답 지정	
인증 기관의 응답이 포함된 파일을 검색하여 이전에 만든 인증서 요청을 완료하십시오. 인증 기관의 응답이 포함된 파일 이름(R):	
C:#ssl₩gpki.cer	
이름(Y):	
www.gpki.go.kr	
확인	취소

- 적용결과를 확인 합니다.

			작업
에 전 전	57		가져오기
이 기능을 사용하여 원 리할 수 있습니다.	』서버가 SSL에 대해 구성된 웹 사이	트에 사용할 수 있는 인증서를 요청하고 관	인증서 요청 만들기 인증서 요청 완료
이름	발급 대상	발급자	도메인 인증서 만들기
www.gpki.go.kr	www.gpki.go.kr	CA131000001	자체 서명된 인증서 만들
			보기 내보내기 경신 ※ 제거
			도움말 온라인 도움말

④ "작업"메뉴의 "바인딩"을 선택합니다.

📬 IIS(인터넷 정보 서비스) 관리자		
S S S S S S S S S S S S S S S S S S S	}0 트 → www.gpki.go.kr →	
파일(F) 보기(V) 도움말(H)		
연결 2	🔵 Default Web Site 홈	작업
JOOYA-PC(jooya-PC\fooya) 응용 프로그램 물 이 에 사이트	유는 방법: 영역 · () · · · · · · · · · · · · · · · · ·	사용 궁한 편집 사이트 편집 바인딩 행 기본 설정 응용 프로그램 보기 가상 디렉터리 보기
	기본 문서 디렉터리 로깅 검색	웹 사이트 관리 <b>☆ 다시 시작</b> ▶ 시작

- 추가버튼을 클릭 합니다.

종류	호스트 이름	포트	IP 주소	바인딩 정보	추가(A)
http		80	*		편집(E)
					제거(R)
(				F	찾아보기(B)

- 추가하는 정보를 확인 합니다.

사이트 바인딩 추가	S. X
종류(T): IP 주소(I): https · 지정하지 않은 모든 IP 호스트 이름(H):	포트(O): • 443
SSL 인증서(S): www.gpki.go.kr	▼ 보기(V)
	확인 취소

- ☞ 종류는 https, 포트는 443(또는 지정포트) SSL인증서는 해당 서버를 각각 선택 합니다.
- 443(또는 지정포트)포트가 추가 되었는지 확인 합니다.

종류	호스트 이름	포트	IP 주소	바인딩 정보	추가(A)
http		80	*	-	
https		443	*		편십(비)
					제거(R)
(				•	찾아보기(B)

- 🖉 IIS7 Windows Internet Explorer 🕒 🔍 👻 https://www.gpki.go.kr/ Q 🏫 🎲 🌈 IIS7 🐴 🔹 🗟 👻 🖶 🔹 페이지(P) 🕶 🍈 도구(O) 🕶 Welcome Bienvenido ようこそ Bem-vindo Willkommen Vítejte Bienvenue Tervetuloa 歡迎 ברוכים הבאים Velkommen VELKOMEN Benvenuto 欢迎 Welkom Witamy internet information services Välkommen مرحباً Hoş Geldiniz 환영합니다 Καλώς ορίσατε Üdvözöljük Добро пожаловать
- ⑤ "https://설치도메인"을 입력하여 접속 여부를 확인한다.

- ☞ IIS7.0의 경우 설치 후 IIS서비스를 재 구동할 필요가 없습니다.
- ⑥ 3개의 인증서중 RootCA 및 CA 인증서를 웹 서버에 설치합니다.
  - 시작 → 실행 → "mmc" 명령 입력 후 확인 버튼 클릭 → 파일 → 스냅인 추가/ 제거를 선택합니다.

응서비스 Mic 물안정성 모니터 Mic 용아정성 모니터 Mic	rosoft Cor	[ 利力(B)
아머서 미서는 미니다. 제네		
행한88 꽃 88 포니터 Mid 에 웹 주소에 연결 Mid	rosoft Cor	위로 이동(U)
이벤트뷰어 Mid	rosoft Cor	(이러로 이동(D)
	prosoft Cor	
Mic Mic	rosoft Cor	
될상지 한디사 Mic 경책 결과 집합 Mic	crosoft Cor	
컴퓨터 관리 Mic	rosoft Cor	
출출터 Mid	rosoft Cor 🕌	고급(V)

- 스냅인 추가/제거 창에서 인증서 항목을 추가합니다.

스냅인	공급업체	-				확장 기능	편집(X)
을 서비스 ■안정성 모니터	Microsoft Cor Microsoft Cor			이 연종/	(로컬 컴퓨터)	[]	4(B)
한 안정성 및 성능 모니터 - 1웹 주소에 연결	Microsoft Cor Microsoft Cor					위로 (	이동(U)
이벤트 뷰어	Microsoft Cor		0.71/A) >	1		아래로	이동(D)
응인쇄 관리 9 인증서	Microsoft Cor Microsoft Cor		주가(A) >	J		10	
이작업 스케줄러	Microsoft Cor						
옯장치 관리자 7 전해 편과 지하	Microsoft Cor Microsoft Cor	E					
김퓨터 관리	Microsoft Cor						
	Microsoft Cor	-				고급	(V)
명:							

- 인증서 대상을 "컴퓨터 계정"으로 선택합니다.

인증서 스냅인	×
미 스냅인이 항상 관리할 인증서 대상: ◎ 내 사용자 계정(M) ◎ 서비스 계정(S)	
◎ 컴퓨터 계정(C)	
	< 뒤로(B) 다음(N) > 취소

- "로컬 컴퓨터"를 선택 후 "마침"을 클릭 합니다.

컴퓨터 선택	
이 스냅인이 관리할 컴퓨터 - 이 스냅인이 항상 관리할	를 선택하십시오. 대상:
④ 로컬 컴퓨터: (이 콘플	on 실행되고 있는 컴퓨터)(L)
◎ 다른 컴퓨터(A):	찾아보기(R)
🔲 명령줄에서 시작할 🛙	ㅐ 선택된 컴퓨터를 변경할 수 있음. 사용자가 콘솔을 저장할 때만 해당(₩)
	< 뒤로(B) 마침 취소

- 추가 결과를 확인 한다.



- ⑦ 3개의 인증서중 RootCA 및 CA 인증서를 웹 서버 설치합니다.
  - "신뢰된 루트 인증기관 → 마우스 오른쪽 버튼 클릭 후 모든 작업 → 가져오기"를 선택합니다.
  - RootCA 인증서 파일을 선택합니다.

가져	을 파일 기계은 피아은 기계된시나요
~	까져볼 파일을 지정하십시오.
I	파일 미름(F):
	C:₩ssl₩rootca.cer 찾아보기(R)
100	참고: 다음 형식으로 한 파일에 두 개 미상의 인증서가 저장될 수 있습니다.
	개인 정보 교환- PKCS #12 (.PFX.,P12)
	암호화 메시지 구문 표준-PKCS #7 인증서(.P7B)
	Microsoft 일련 인증서 저장소(,SST)
인증/	d 파일 형석에 대해 자세히 알아봅니다.

- 저장 장소를 선택합니다.

이 가져오기 마랍자	1		
인증서 저장소는 인증서를 저장하는 시스템	! 영역입니다.		
Windows가 자동으로 인증서 저장소를 선택 습니다.	박하거나 사용자가 연	인증서 위치를 지	정할 수 있
◎ 인증서 종류 기준으로 인증서 저장소	를 자동으로 선택(U	))	
◉ 모든 인증서를 다음 저장소에 저장(P	9		
인증서 저장소:			
신뢰할 수 있는 루트 인증 기관		\$	한아보기(R)
<u>인증서 저장소</u> 에 대해 자세히 알아봅니다.			
	< 뒤로(B)	다음(N) >	취소

- 가져오기를 완료합니다.

인증서 가져오기 마법사	인증서 가져오기 마법사 완료
	[마침]을 클릭하면 인증서를 가져옵니다. 다음 설정을 지정했습니다. <mark>사용자가 선택한 인증서 제장소</mark> 신뢰할 수 있는 루트 인증 기 내용 인증서 파일 <b>이름</b> C:₩ssl\#rootca.cer
	< <u> </u>
	< 뒤로(B) 마침 취소

- 결과를 확인 합니다.



- ☞ 그러면, 인증서 설치가 완료됩니다. (와일드카드)SSL인증서 파일(\*.p7b)에서 내보낸 CA인증서를 설치하기 위해서는 ⑦번을 반복하면 됩니다.
- ⑧ 이제 SSL인증서의 설치가 완료되었으며, 웹 브라우저를 통해 SSL인증서 설치 정상 유무를 확인할 수 있습니다. (예. https://www.gpki.go.kr)

◆ ● 157 Wilk Model and the set of the se	e https://www.goki.go.kt/	* 🔒	→ X Uve Search	_
υάνοχοιμικ Κάλως ορίσατε	★ 第57 Wilk Bienvenue 数迎 Velkommen Benvenuto Welkom Valkommen Hoş Geld	MOGAHA Govt of Korea 에서 이사이트를 유입한 결과: www.gpkigo.kr         서비에 대한 연결이 알조좌되었습니다.         신뢰할 수 있는 사이트         민용서 보기         민용서 보기         Internet information services         internet information services	・ D ・ D ・ D 時の利の vindo Vitejte Tervetuloa Draa Draa VELKOMEN 欢迎 Witamy Mitamy ら習習니다	P) • () 도구(0
Добро пожаловать	1	Ичозоник Калыс оріаст Добро пожаловать	2	

- "인증서 보기"를 클릭하여 설치된 인증서 정보를 확인합니다.

인증서 📃 🛁 👘 👘
일반 자세히 인증 경로
[ 이중서 정보
인증서의 용도:
• 원격 컴퓨터의 신분을 확인합니다.
발급 대상: www.gpki.go.kr
발급자: CA131000001
유효 기간: 2010-05-13 부터 2012-05-13
인증서 설지(I) 말급자 설명(S)
민증지에 대한 자세한 정보
1048

## 다. 웹사이트 적용

웹사이트 이용시 암호화통신이 가능하도록 웹 프로그램을 수정합니다. ☞ 구축가이드 V장을 참조

#### 라. SSL 인증서 개인키 추출 방법

#### ※ 웹방화벽 및 개인정보 필터링에 적용시 필요

- 시작 → 실행 → "mmc" 명령 입력 후 확인 버튼 클릭 → 파일 → 스냅인
 추가/제거를 선택합니다.

·냅인	공급업체	^	E	확장 기능 편집(X)
서비스 안정성 모니터	Microsoft Cor Microsoft Cor			(R) (R)
안정성 및 성능 모니터 웹 주소에 연결	Microsoft Cor Microsoft Cor			위로 이동(U)
이벤트 뷰어	Microsoft Cor	r		이래로 이동(D)
9인쇄 관리  위쪽서	Microsoft Cor Microsoft Cor	_		-
작업 스케물러	Microsoft Cor			
장치 관리자	Microsoft Cor	Ξ		
성색 달과 집합   컨프터 파리	Microsoft Cor			
출더	Microsoft Cor	-		고급(V)
3.				

- 스냅인 추가/제거 창에서 인증서 항목을 추가합니다.

느냅인	공급업체	^		확장 기능 편집(X).
서비스 안정성 모니터	Microsoft Cor Microsoft Cor		<mark>办 인증서(로컬 컴퓨터)</mark>	제거(B)
) 안정성 및 성능 모니터 웹 주소에 연결	Microsoft Cor Microsoft Cor			위로 이동(U)
이벤트 뷰어	Microsoft Cor	0.71/		이래로 이동(D)
인증서	Microsoft Cor Microsoft Cor	<u>م</u>	<i>,,</i> ,	
	Microsoft Cor			
월양지 관리사 [정책 결과 집합	Microsoft Cor Microsoft Cor	E		
컴퓨터 관리	Microsoft Cor			
플더	Microsoft Cor	+		고급(V)

- 인증서 대상을 "컴퓨터 계정"으로 선택합니다.

인증서 스냅인	×
이 스냅인이 항상 관리할 인증서 대상: ◎ 내 사용자 계정(M) ◎ 서비스 계정(S) ◎ 컴퓨터 계정(C)	
	<뒤로(B) 다음(N)> 취소

- "로컬 컴퓨터"를 선택 후 "마침"을 클릭 합니다.

컴퓨터 선택	
이 스냅인이 관리할 컴퓨터 이 스냅인이 항상 관리할 ④ 로컬 컴퓨터: (이 콘솔	를 선택하십시오. 대상: ·미 실행되고 있는 컴퓨터)(L)
◎ 다른 컴퓨터(A):	찾아보기(R),,,
🔲 명령줄에서 시작할 때	선택된 컴퓨터를 변경할 수 있음. 사용자가 콘솔을 저장할 때만 해당(₩)
	(뒤로(B) 마침 취소

- 추가된 인증서 항목을 확인 합니다.

🚟 콘슐1 - [콘슐 루트]		
🚰 파일(F) 동작(A) 보기(V) 즐겨찾기(O)	장(W) 도움말(H)	_ <i>=</i> ×
📫 콘솔 루트	이름	작업
▲ 및 인증서(도접 컴퓨터) ▶ 월 개이용	🕼 인증서(르컬 컴퓨터)	돈을 두드 🔺
<ul> <li>○ 데 비율 수 있는 루트 인증 기관</li> <li>○ 행태프라이즈 신뢰</li> <li>○ 중개 인증 기관</li> <li>○ 정치 인증 기관</li> <li>○ 신뢰할 수 있는 게시자</li> <li>○ 해 타사 루트 인증 기관</li> <li>○ 전뢰된 사용자</li> <li>○ 환자 루트 인증 기관</li> <li>○ 전뢰된 사용자</li> <li>○ Remote Desktop</li> <li>○ 인증서 등록 요청</li> <li>▷ ○ 스마트 카드 신뢰할 수 있는 루트</li> </ul>		기타 작업 →

 - 인증서(로컬 컴퓨터)>개인용>인증서 항목을 클릭 하면 적용된 정보를 확인 할 수 있습니다.

해당 도메인에서 오른쪽 마우스 클릭 후 내보내기를 선택합니다.

존승 루트	발급 대상	~	발급지	ł	만료 날짜	용도	작업	
▲ 🖓 인증서(로컬 컴퓨터) ▲ 🧰 개인용	हिङ्ग www.gpk	열기(0)	P	1000001	2012-05-13	서비 인	인증서 기타 자유	-
인증서 > 이 신뢰할 수 있는 루트 안		모든 작업(K)	•	열기(O)			vww.apki.go.kr	
이 연터프라이즈 신뢰	잘	잘라내기(1)		개인 키 관리(M)			기타 작업	•
> · · · · · · · · · · · · · · · · · · ·	복사(C) 상제(D)			내보내기(E)				
<ul> <li>실뢰되지 않은 인증서</li> <li>한 타사 루트 인증 기관</li> </ul>		속성(R)						
▷ 🥶 신뢰된 사용자 ▷ 📑 Remote Desktop		도움말(H)						
이중서 등록 요정 이 스마트 카드 시리한 수 1	-		_					
> 🔤 그마드 카드 전되일 구								

- 인증서 내보내기 마법사가 실행되면 다음버튼을 클릭 합니다. 다음에서 "예 개인키를 내보냅니다.(Y)" 선택 후 다음을 클릭 합니다.

서 내보내기 마법사	
개인 키 내보내기	
인증서와 함께 개인 키를 내보낼 수 있습니	СЬ,
개인 키에는 암호가 설정되어 있습니다. 인 에서 암호를 입력해야 합니다.	증서와 함께 개인 키를 내보내려면 다음 페이지
인증서와 함께 개인 키를 내보내시겠습니까	117
◉ 예, 개인 키를 내보냅니다(Y).	
💿 아니요, 개인 키를 내보내지 않습니	EKO).
개인 키 내보내기에 대해 자세히 알아봅니다.	
게근 거 네포데거에 대해 지세히 올라봅니다.	
	< 뒤로(B) 다음(N) > 취소

## - 선택 내용 확인 후 다음을 클릭합니다.

인증서 내보내기 마법사
<b>파일 내보내기 형식</b> 인증서를 여러 형식으로 내보낼 수 있습니다.
사용할 형식을 선택하십시오.
<ul> <li>○ DER로 인코딩된 X,509 바이너리(.CER)(D)</li> <li>○ Base 64로 인코딩된 X,509(.CER)(S)</li> <li>○ 암호화 메시지 구문 표준 - PKCS #7 인증서 (.P7B)(C)</li> <li>□ 가능하면 인증 경로에 있는 인증서 모두 포함(I)</li> <li>◎ 개인 정보 교환 - PKCS #12(.PFX)(P)</li> <li>□ 가능하면 인증 경로에 있는 인증서 모두 포함(U)</li> <li>□ 대보내기가 완료되면 개인 키 삭제(K)</li> <li>□ 확장된 속성 모두 내보내기(A)</li> <li>○ Microsoft 일련 인증서 저장소(.SST)(T)</li> </ul>
<u>인증서 파일 형식</u> 에 대해 자세히 알아봅니다.
< 뒤로(B) 다음(N)> 취소

- 비밀번호를 입력합니다. (자릿수 제한 없음)

인증서 내보내기 마법사	×
암호	
보안을 유지하려면 암호를 사용하며 개인 키	l를 보호해야 합니다.
암호를 입력하고 확인하십시오.	
암호(P):	
******	
암호 입력 및 확인(필수)(C):	
••••••	
	< 뒤로(B) 다음(N) > 취소

- 내보낼 키 파일의 이름을 지정합니다.

찾마보기(R)
(및로(R)) 다음(N) > 최소

- 내보내기 결과를 확인한다.

인증서 내보내기 마법사	×
	인증서 내보 <mark>내</mark> 기 마법사 완료
	인증서 내보내기 마법사를 완료했습니다. 다음 설정을 지정했습니다. <mark>파일 이름 C:\#ssl\#gpkikey.pf</mark> 키 내보내기 예 인증 경로에 있는 인증서 모두 포함 아니요 파일 형식 Personal Informatio
	< <u> </u>
	< 뒤로(B) 마침 취소

- 저장한 위치에서 내보낸 파일을 확인 후 OpenSSL로 개인키를 분리 합니다.



- 생성된 key.pem파일의 내용을 확인 합니다.

Bag	Attributes
10000	1.3.6.1.4.1.311.17.2: <no values=""></no>
	localKeyID: 01 00 00 00
	Microsoft CSP Name: Microsoft RSA SChannel Cryptographic Provider
	friendlyName: 88472932a9b353da1ed6bc280d971d56 de2fbff6-0456-42a9-8d20-aa89ccb62a9
Key	Attributes
225	X509v3 Key Usage: 10
	BEGIN RSA PRIVATE KEY
MIIC	CXQIBAAKBqQC5rHkdo58M01048zltPSEN83miqy5T8SQ2WhKU4WdqlJjjdq77
tdNH	HXkIM15sarBvQt+cEu8tzSPFvWfI4GGarkpK+XU64KEUiNc2zResbmAo7YiUD
Flpc	gap5U2/osFwPOpCZXNw4NTX17SIGHrML9cCRM1p8kZ+iq6JAajdXTJQIDAQAB
AOGI	BALbIsM7Z1ejkYaFQZ/c/V3wJdXPj2kauvKx5DZPdNla5BK3f+i4XuG+ovjLx
SLM	APb3CXT3OtiG+7FdnX8mTU/XgvQcaDA/fqaaBDHw9/BjDHeeti6qWVkyh2L2h
+ei3	3jc8fNPy7GM4sMqsZUFtPWzDHitX4zrkqeIhBvSVi4uNhAkEA+HsH+8vymr3J
8853	3akQOWqTCdCwd2I6FQYP7aKELgX0U32BBDB+Bj8TRnW0sBH1v6xw1v18QMxii
LUni	r9a4wiQJBAL9K4TXrFt13AQ0yspuczbND+tGKYTQ43BOaZak8FEQHzubgukYR
BLAN	xxra2NEG932QvzCOOIew3VFKyg67Qjr0CQAIoR0x3W9beGPfDn3gLuTguQAX0
MBor	mOp/z/mXNKCVqqZi65DWvvFc8NTmxrfUn/MHEz8sUVjarWxUb1DHq3kkCQQC7
75I)	xieUt8dP7pnppffVuEPSj10NGrjIxpDgKu3bhm5Y/qDv5yJCFiawdKAdRK30F
Dhy	ONf7H91qF41KSdl41AkAdlZwuAjRbSdlAx+11WN1X7b02PDFm112Qzp8Y1X41
HORY	vLyOADfkNVV7h00/0DLPfaHZT3M6Qbky7VNSyIrmT
	END R3A PRIVATE KEY

## 2.3. Apache 서버에서 보안서버 구축하기

- Apache서버 1.3.x 버전에서는 기본적으로 SSL기능을 지원하지 않기 때문에 별도의 Mod\_SSL모듈과 OpenSSL모듈을 설치하셔야 SSL기능을 사용할 수 있습니다.
- Apache서버 2.x 버전부터는 SSL기능이 포함되어 나오므로 Mod\_ssl모듈을 추가 설치할 필요 없이 OpenSSL모듈만을 설치하면 되나, Apache설치시 Mod\_ssl모듈 을 옵션에서 제외시켰을 경우 Apache를 재설치해야 합니다.
  - ※ Mod\_ssl과 OpenSSL 모듈은 각각 <u>www.modssl.org</u>, <u>www.openssl.org</u>에서 무료 다운로드가 가능합니다.
- WIN O/S에 보안서버 구축시에도 적용방법은 비슷합니다. WIN O/S의 경우 아파치 2.x 버전을 사용하므로 OpenSSL 만 추가 설치해주시면 됩니다.
   <u>http://www.openssl.org/related/binaries.html</u> 페이지를 참고하세요.
- 아파치 SSL 설치관련 내용은 아파치 웹사이트에서 얻을 수 있습니다.
   <u>http://www.Apache-ssl.org</u>에서 자세한 설명을 찾을 수 있습니다.

**가.** Linux O/S에 OpenSSL과 Mod\_ssl의 설치 방법 Apache서버 1.3.x 버전에서 SSL 통신을 가능하게 하기 위해서는 OpenSSL과 Mod\_ssl이 필요합니다.

우선, 현재 서비스 중인 Apache서버에 Mod\_ssl이 설치되어 있는지를 httpd -1 옵션을 사용하여 mod\_ssl.c 또는 mod\_ssl.so가 있는지 확인하시기 바랍니다.

\$ /usr/local/apache/bin/httpd -l
Compiled-in modules:
 mod\_ssl.c

OpenSSL은 Apache 버전과 Mod\_ssl의 버전을 확인한 후에 알맞은 OpenSSL을 설치 해야 합니다. 예를들어 Apache 1.3.3 버전에는 Mod\_ssl 2.1.6 (또는 2.1.7)을 설치 해야 하고, Mod\_ssl 2.1.6은 OpenSSL 0.8.1b와 0.9.1c 버전 사이에서만 동작 합니다. 버전을 확인하지 않고 OpenSSL과 Mod\_ssl을 설치하면 Apache 컴파일 과정에서 오류가 발생합니다. Mod\_ssl은 반드시 Apache 서버 버전에 맞는 것을 설치하셔야 하며 <u>www.modssl.org에서</u> Apache 버전을 확인한 후 그에 맞는 Mod\_ssl을 다운받아 설치하시기 바랍니다.

Mod\_ssl에서 지원하는 Apache 버전 및 OpenSSL의 버전은 Mod\_ssl 소스의 README. Versions 에서 확인할 수 있으며, www.openssl.org에서도 확인할 수 있습니다.

Apache 서버 2.x 버전의 경우 Mod\_ssl, OpenSSL 최종버전을 설치해야 합니다.

① OpenSSL의 설치(www.openssl.org) 압축풀기

\$ gzip -cd openssl-0.9.6.tar.gz | tar xvf -

\$ ./config \$ make \$ make installconfig
 □ prefix를 주지 않았을 때에는 /usr/local/ssl 디렉토리에 설치가 됩니다.

다른 디렉토리에 설치를 하고자 한다면 다음과 같이 설치합니다.

\$ ./config --prefix=/usr/local --openssldir=/usr/local/openssl

☞ OpenSSL의 실행파일은 /usr/local/ssl/bin에 설치되고 인증서비스를 위한 파일들은/usr/local/openssl 아래의 디렉토리에 생성됩니다.

② Mod\_ssl의 설치 (www.modssl.org)

### <u>압축풀기</u>

\$ gzip -cd apache\_1.3.19.tar.gz | tar xvf \$ gzip -cd mod\_ssl-2.8.1-1.3.19.tar.gz | tar xvf

파일의 다운로드와 압축풀기가 끝나면 Mod\_ssl 설정을 합니다.

#### <u>Mod\_ssl</u> 설정

\$ cd mod\_ssl-2.8.1-1.3.19

\$ ./configure ₩

--with-apache=../apache\_1.3.19 ₩

--with-ssl=../openssl-0.9.6 ₩

--prefix=/usr/local/apache

③ Apache 서버 설치(www.apache.org)

\$ cd ../apache\_1.3.x
\$ SSL\_BASE=../openssl-0.9.6 ₩
./configure ₩
--prefix=/usr/local/apache ₩
--enable-module=ssl ₩
\$ make
\$ make
\$ make certificate
\$ make install

나. WIN O/S에 OpenSSL 설치 방법

☞Apache서버 2.x 버전부터는 SSL기능이 포함되어 나오므로 Mod\_ssl모듈을 추가 설치할 필요 없이 OpenSSL모듈만을 설치하면 되나, Apache설치 시 Mod\_ssl모듈 을 옵션에서 제외시켰을 경우 Apache를 재설치해야 합니다.

☞WIN O/S용 OpenSSL 설치방법은 다음과 같습니다.

①다운로드



②설치



③설치 확인

C·₩Ope	n S S n	>dir		
C 드라(	기브	의 돌큠 :		
볼륨 일	련 변	번호 : 54A5-8	EF0	
C:₩Op	enSS	SL 디렉토리		
2011/08	/31	오후 03:29	<dir></dir>	
2011/08	/31	오후 03:29	<dir></dir>	
2011/08	/31	오후 03:29	304,833	changes.txt
2011/08	/31	오후 03:29	36,610	faq.txt
2011/08	/31	오후 03:29	6,406	license.txt
2011/08	/31	오후 03:29	15,973	news.txt
2011/08	/31	오후 03:29	30,423	OpenSSLhelp.chm
2011/08	/31	오후 03:29	8,126	readme.txt
2011/08	/31	오후 03:29	77,824	regref.exe
2011/08	/31	오후 03:29	79,872	sslcopy.exe
2011/08	/31	오후 03:29	10,124	unins000.dat
2011/08	/31	오후 03:29	690,969	unins000.exe
		10 개 파일		1,261,160 바이트
		3 개 디렉	토리 6.75	258.416.384 바이트 남음

④ openssl.cnf 및 openssl.exe 파일은 bin 폴더에 있습니다.

```
C:₩OpenSSL₩bin>dir
c 드라이브의 볼륨 :
볼륨 일련 번호 : 54A5-7191
C:₩OpenSSL₩bin 디렉토리
2011/08/31 오후 03:29 <DIR>
                            .
2011/08/31 오후 03:29 <DIR>
                             ..
2011/08/31 오후 03:29 <DIR>
                            PEM
                    5,685 CA.pl
2011/08/31 오후 03:29
                    9,694 openssl.cnf
2011/08/31 오후 03:29
2011/08/31 오후 03:29 258,048
                           openssl.exet
2011/08/31 오후 03:29 15,973 news.txt
           3 개 파일
                           273,427 바이트
           3 개 디렉토리 6,758,416,384 바이트 남음
```

- 다. 개인키 생성 및 CSR생성 방법
  - ① openssl.cnf 설정값 수정
  - 행정전자서명 신청시에 메일로 수신 받은 dn을 참조합니다.
    - 예) CN=www.gpki.go.kr,OU=Group of Server,O=Government of Korea,C=KR
    - 설치된 Openssl 설치된 폴더의 openssl.cnf 내용을 확인하여 아래와 같이 수정 합니다. (미사용 항목을 주석(#) 처리 합니다)

[ req_distinguished_name ]	
countryName	= Country Name (2 letter code)
countryName_default	= KR
countryName_min	= 2
countryName_max	= 2
#stateOrProvinceName	= State or Province Name (full name)
#stateOrProvinceName_defaul	t = Some-State
#localityName	= Locality Name (eg, city)
0.organizationName	= Organization Name (eg, company)
0.organizationName_default	= Government of Korea
# we can do this but it is no	ot needed normally :-)
#1.organizationName	= Second Organization Name (eg, company)
#1.organizationName_default	= World Wide Web Pty Ltd
organizationalUnitName	= Organizational Unit Name (eg, section)
organizationalUnitName_defau	It = Group of Server
commonName	= Common Name (eg, YOUR name)
commonName_max	= 64
#emailAddress	= Email Address
#emailAddress_max	= 64

☞GPKI에서 사용하는 Country, Organization, Organization Unit, CommonName 을 제외한 항목은 주석처리 ② 개인키 생성

\$ openssl genrsa -des3 -out <key filename> 2048
Generating RSA private key, 2048 bit long modulus
....++++++
e is 65537 (0x10001)
Enter PEM pass phrase: > password>
Verifying password - Enter PEM pass phrase:

예) <리눅스&유닉스> openssl genrsa -des3 -out key.pem 2048 <윈도우> openssl genrsa -out key.pem 2048

문 윈도우의 경우 개인키에 패스워드를 지정해버리면 SSL 설정 적용 후 아파치가 기동되지 않기 때문에 -des3 옵션을 제거한 명령어를 통해 개인키에 패스워드 설정을 하지 않고 생성해서 작업을 하셔야 합니다.

☞ 개인키 비밀번호를 입력하며 **반드시 기억**해야 합니다. (암호를 분실할 경우 SSL사용을 위한 Apache를 구동할 수 없기 때문에 SSL인증서를 재발급 받아야합니다.)

③ 생성된 개인키를 이용하여 CSR생성

\$ openssl req -new -key <key filename> -out <csr filename> 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. ----ls Country Name (2 letter code) [KR]: Organization Name (eg, company) [Government of Korea]: -Organizational Unit Name (eg, section) [Group of Server]: -Common Name (eg, YOUR name) []:<cn name : domain>. Please enter the following 'extra' attributes to be sent with your certificate request A challenge password []:비밀번호교 An optional company name []:비밀번호ᆗ ☞ <key filename>은 단계 ②에서 생성한 개인키 파일이며 <csr filename>은 생성할

- Image: section and section
- ☞ [KR] 등 [] 안에 내용은 기본 설정 값입니다. 위 내용과 다르면 값을 직접 입력하여 주시면 됩니다. 위 내용 외 다른 값을 넣으시면 발급시 114에러가 발생합니다. (대소문자 구별)
- 예) \$ openssl -new -key key.pem -out csr.pem ~ ~ ~ Country Name (2 letter code) [KR]:교 Organization Name (eg, company) [Government of Korea]:교 Organizational Unit Name (eg, section) [Group of Server]:교 Common Name (eg, YOUR name) []:www.gpki.go.kr교 ~ ~ ~ A challenge password []:비밀번호교 An optional company name []:비밀번호교

④ CSR 제출

생성된 CSR(<csr filename>)의 내용은 다음과 같습니다.

-----BEGIN CERTIFICATE REQUEST-----

MIIBETCBvAIBADBXMQswCQYDVQQGEwJBVTETMBEGA1UECBMKU29tZS1TdGF0ZTEh MB8GA1UEChMYSW50ZXJuZXQgV2lkZ2l0cyBQdHkgTHRkMRAwDgYJKoZlhvcNAQkB ~ ~ ~ AaAAMA0GCSqGSlb3DQEBBAUAA0EAXcMsa8eXgbG2ZhVyFkRVrl4vT8haN39/QJc9 BrRh2nOTKgfMcT9h+1Xx0wNRQ9/SIGV1y3+3abNiJmJBWnJ8Bg== ------END\_CERTIFICATE\_REQUEST-----

☞ CSR 내용은 BEGIN CERTIFICATE REQUEST부터 END CERTIFICATE REQUEST 까 지입니다.

### ⑤ SSL인증서 발급

☞ 행정전자서명 인증관리센터 홈페이지에 (<u>www.gpki.go.kr</u>)에서 발급하면 됩니다. <붙임1 SSL인증서 발급 절차 참고>

#### 라. 인증서 설치 방법

- ① 발급받은 인증서를 확인합니다.
  - C:\GPKI\certificate\class1 디렉토리에 해당 <*cn name : domain*>.p7b 파일이 있는지 확인합니다. (예: www.gpki.go.kr.p7b)

-----BEGIN PKCS7-----MIILiQYJKoZIhvcNAQcCoIILejCCC3YCAQExADALBgkqhkiG9w0BBwGgggteMIID HTCCAgWgAwIBAgIQSAcIRgAuPO7tcwjaHEc8+jANBgkqhkiG9w0BAQUFADBQMQsw ... 8wQdPqvThnU/td3t6IrVG983r3rrP69GN/qspiJpBIryB019rK0cUeYFK95jaL3E 0lqDgGfm9I5cuWcJ8eaPfU/AlZYkXCss4jJrMQA= ------END PKCS7-----

② pkcs#7 ⇒ pem 변환

openssl pkcs7 -in <p7b filename> -out <pem filename> -print\_certs -text

- 여기서 <p7b filename>은 발급받은 인증서의 이름 및 전체 경로이며, <pem filename>은 변환되어 저장될 pem 파일 이름 및 전체 경로를 입력한다.
- 예) openssl pkcs7 -in www.gpki.go.kr.p7b -out cert.pem -print\_certs -text
- ③ CA 인증서 및 CAChain 인증서 생성
  - pem filename>파일을 편집기로 열어서 아래와 같은 내용들을 복사하여 각각의 파일을 생성합니다.
  - ☞ 파일 중에서 'CA131000001'이 들어있는 부분의 'Certificate:'에서 '----END CERTIFICATE-----'까지 부분을 복사하여 <*ca.pem*>파일을 생성합니다.
  - ☞ 파일 중에서 'RootCA'와 'CA131000001'이 들어있는 부분의 'Certificate:' 에서 '----END CERTIFICATE-----'까지 부분을 전부 복사하여 <*caChain.pem*>파 일을 생성합니다.

예) <ca.pem>, <caChain.pem> 생성 예제

Certificate:			
Data:			
Version: 3 (0x2)			
Serial Number:			
4a:65:5e:f5:03:d1:e7:b0:c6:e4:e5:db:e0:d0:52:e5			
Signature Algorithm: sha1WithRSAEncryption			
Issuer: C=KR, O=Government of Korea, OU=GPKI, CN=CA131000001			
Subject: C=KR, O=Government of Korea, OU=Group of Server, CN=www.gpkigo.kr			
BEGIN CERTIFICATE			
MIIDIzCCAgugAwIBAgIQSmVe9QPR57DG50Xb4NBS5TANBgkqhkiG9w0BAQUFADBQ			
END CERTIFICATE		Line	
		72	
Certificate:			
Data:			
Version: 3 (0x2)			
Serial Number:			
3c:c2:81:4b:00:e7:52:4d:9b:aa:47:b7:e1:61:f5:0e			
Signature Algorithm: sha1WithRSAEncryption			
Issuer: C=KR. O=Government of Korea. OU=GPKI. CN=Root CA			
~ ~ ~ ~			cert
Subject: C=KR, O=Government of Korea, OU=GPKI, CN=Root CA			.pem
BEGIN CERTIFICATE			
MIIDmTCCAoGgAwIBAgIQPMKBSwDnUk2bgke34WH1DjANBgkghkiG9w0BAQUFADBM			
~ ~ ~ ~ ~			
uSuQZ4ogBNo2kxt8Pg==	Line		
END CERTIFICATE	150	caChain	
	150	nom	
Certificate:		.pem	
Data:			
Version: 3 (0x2)			
Serial Number:			
48:15:99:5d:01:ea:17:36:01:73:5b:d1:16:f8:25:5c			
Signature Algorithm: sha1WithRSAEncryption			
Issuer: C=KR. O=Government of Korea. OU=GPKI. CN=Root CA			
	ca.pem		
Subject: C=KR, O=Government of Korea, OU=GPKI, CN=CA131000001			
~ ~ ~ ~ ~			
BEGIN CERTIFICATE			
MIIEnDCCA4SgAwIBAgIQSBWZXQHqFzYBc1vRFvgIXDANBgkqhkiG9w0BAQUFADBM			
~ ~ ~ ~ ~			
498KpPx9vfeB3R3h130seTSGa4JXgngrKoaCbTstU9U=			
END CERTIFICATE			

- ④ 환경설정 파일(httpd.conf 또는 ssl.conf)을 수정합니다.
  - 환경설정 파일중 mod\_ssl.so 부분이 있으면 mod\_ssl 사용을 위해 주석을 해제 합니다.

LoadModule ssl\_module modules/mod\_ssl.so

- 기존 http <VirtualHost www.gpki.go.kr:80> 항목을 복사하여 붙여넣고 SSL관련 4개 항목을 추가하고 각 항목에 맞는 파일의 경로를 입력합니다.

NameVirtualHost *	☜이름 기반 가상호스트 사용
<virtualhost *:<mark="">80&gt;</virtualhost>	
ServerAdmin admin@gpki.go.kr	
DocumentRoot "/home/gpki/www/"	☜홈디렉토리 설정
ServerName www.gpki.go.kr	☜도메인 설정
ServerAlias gpki.go.kr	
ErrorLog /home/gpki/error_log	
AccessLog /home/gpki/access_log	
<virtualhost *:<b="">443&gt;</virtualhost>	
ServerAdmin admin@gpki.go.kr	
DocumentRoot "/home/gpki/www/"	🖘 홈디렉토리 설정
ServerName www.gpki.go.kr	🖘 도메인 설정
ServerAlias gpki.go.kr	
ErrorLog /home/gpki/ssl_error_log	
AccessLog /home/gpki/ssl_access_log	
SSLCertificateKeyFile " <key filename="">"</key>	🖘 key.pem
SSLCertificateFile " <pem filename="">"</pem>	🖘 cert.pem
SSLCertificateChainFile " <cachain.pem>"</cachain.pem>	🖘 caChain.pem
SSLCACertificateFile " <ca.pem>"</ca.pem>	🖘 ca.pem

- ☞ <pem filename>은 발급받은 인증서 파일의 경로 및 파일명을 입력합니다.
- ☞ < key filename>은 CSR 파일 처음 생성시 생성한 key파일을 그대로 사용 해서 경로 및 파일명을 입력합니다.
- ☞ <caChain.pem>과 <ca.pem>은 <pem filename>에서 복사해서 생성한 파일의 경로 및 파일명을 입력합니다.

⑤ Apache 서버를 재구동합니다.

\$ ./apachectl stop ./apachectl stop: httpd stopped \$ ./apachectl startssl Apache/1.3.19 mod\_ssl/2.8.1 (Pass Phrase Dialog) Some of your private key files are encrypted for security reasons. In order to read them you have to provide us with the pass phrases. Server testssl.klid.or.kr:443 (RSA) Enter pass phrase: phrase Cok: Pass Phrase Dialog successful. ./apachectl startssl: httpd started

- Apache 서버에서 SSL을 사용하기 위한 시작 명령어인 startssl을 실행하면 개인키의 비밀번호를 묻는데, 이 비밀번호는 이전의 설치과정 '개인키 생성 및 CSR 생성 방법' 중 ② 개인키 생성시 입력한 개인키 비밀번호를 입력하시면 됩니다.
- ⑥ 웹 브라우저를 통해 SSL인증서 정상 적용 유무 확인
  - 웹 브라우저의 주소에 "https://도메인"(예: https://www.gpki.go.kr)이라 입 력 후 엔터를 치면 주소 입력란 옆에 자물쇠 모양이 나타나는 것을 볼 수가 있으며, 자물쇠를 클릭하면 "신뢰할 수 있는 사이트"라고 나타나는 것을 확인 할 수가 있다.



#### 마. 웹사이트 적용

웹사이트 이용시 암호화통신이 가능하도록 웹 프로그램을 수정합니다. ☞ 구축가이드 V장을 참조

#### 바. SSL 인증서 개인키 추출 방법

※ 웹방화벽 및 개인정보 필터링에 적용시 필요
☞ 아파치의 경우 개인키가 파일형태로 저장되므로 추출할 필요가 없습니다.

- 생성된 개인키 파일(key.pem)을 확인합니다.

----BEGIN RSA PRIVATE KEY----Proc-Type: 4, ENCRYPTED DEK-Infb: DES-EDE3-CBC,CB07B7A266E1867F yspxvlE8iJxANc703vz4Mvjtb+3c+uTVAcHCUNRxaSa54PDN0XHvPE6iNYiaEDf4 u1csATnOg1XLWLUSSpbQw3xLnZvbOYFYWuRsmmTSc4hJeNwkwmXCn45f0nZhiN2N jGdH2CqTPNDZaEHtiDQeNUqZOW/YnkJHNi3nwMjOOqnQp+HXEIIvjBpSDEhkOCFV PfuRRJz+7ksDmB5IVV3VL4z6cyYSthUw7qhGMINwGrd0Hsspya+mk8rN0+wfH9gi SRANmHWpqDoU/coscbQido4HtTWHwWb7SfVxicXXkNTnWSEusTDsSfokc+KJESce u08YWoCeDFF8Uy9tG7bKmfF8HfYyo7QV1QJPvlt0EuC7usQKHcjq+u4PNuCqstFn NMI8/iXnr2dkiLEY4c1QqvNsudY81U/BcDNE1kY18f6yhj9aSgVKd6E/re9HBcAF iSJGjHPBbjAVUXhuA7bNw/KM1dObbvz+jOoWNh8QQ4tiPFi/ZRRZCRnwYp/PsO1+ rE7Y14uRjgiV8c4oVhgg4KUMiUE67ki/Xrchx8CxGEpV2Ej6kK+W7sv+91wIIarN TMkYP16JejIGcEaJhC1x/y4iDHvFmOLCyLpNP13k4T08NfNY06HVpZkCw2b8nOuy 5mrdhkOshqivTMgoP3HgY+2cG7zbOTdjytvasuOFpW2+SzqBYHw2rBOwTdc21Dys nps8cap21XTsiLf8w25eM1RFcfMSaW/iMS01qUDP16ZPOUtSEixjwrLiGXvgLJ8i zfoyTHrbvPcRm1RRs85i5VIohSR1Zr80soqPxE7WFVNODObzgsXamQ== ----END RSA PRIVATE KEY-----

## 2.4. WebToB 서버에서 보안서버 구축하기

## 가. 개인키 생성 및 CSR 생성 방법

☞ WebtoB의 경우 개인키와 CSR을 동시에 생성되기 때문에 개인키 및 CSR을 분리해서 txt 파일로 저장해야 합니다.

① Default 설정 확인

서버에 접근하여 wbssl.cnf 파일을 확인합니다.

\$ cd \$WEBTOBDIR/ssl
\$ vi wbssl.cnf

② 해당 항목 확인

- 다른 부분은 수정하지 마시고 [req\_distinguished\_name] 만 확인합니다.
  - \* countryName\_default 가 KR 인지 확인합니다.
  - \* organizationName\_default 가 Government of Korea 인지 확인합니다.
  - \* organizationUnitName\_default 가 Group of Server 인지 확인합니다.
    - \* 그 외의 <u>stateOrProvinceName나 localityName은 default 항목이 설정되어 있으면</u> <u>주석처리(#) 하시기 바랍니다.</u>

- wbssl.cnf 파일 내용

[ req ] default_bits 그 외 내용 생략	= 2048 // 1024로 된걸 2048로 수정
[ req_distinguished_name ] countryName <i>countryName_default</i> countryName_min countryName_max	= Country Name (2 letter code) = KR = 2 = 2
stateOrProvinceName #stateOrProvinceName_default localityName	<ul> <li>State or Province Name (full name)</li> <li>Some-State</li> <li>Locality Name (eg, city)</li> </ul>
0.organizationName <i>0.organizationName_default</i>	= Organization Name (eg, company) <b>= Government of Korea</b>
organizationalUnitName organizationalUnitName_default	= Organizational Unit Name (eg, section) <b>= Group of Server</b>
#emailAddress #emailAddress_max	= Email Address = 40
#SET-ex3	= SET extension number3

◎ default 값이 위와 다른 경우에 수정하고 저장합니다.

③ CSR 정보 입력

WebtoB 웹 서버의 홈 폴더 아래에 ssl 폴더에 'CA' 명령어를 실행하여 CSR을 생성 합니다.

i. \$WEBTOBDIR/ssl 디렉토리에서 CSR을 생성합니다.

\$ CA -newreq
Using configuration from path/to/ssl/wbssl.cnf
Generating a 2048 bit RSA Private key
Enter PEM pass phase : <i><password></password></i>
verifying password - Enter PEM pass phase : <i><password></password></i>
Country Name <2 letter code> [KR] : KR
States or province Name <full name=""> [] :</full>
Locality Name <eg. city=""> [] :</eg.>
Organization Name <eg. company=""> [Government of Korea] : Government of Korea</eg.>
Organization Unit Name <eg. section=""> [Group of Server] : Group of Server</eg.>
Common Name <eg. hostname="" name="" or="" server's="" your=""> [] : <cn :="" domain="" name=""></cn></eg.>
Email Address [] :
A challenge password [] :
An optional company name [] :
Request <and key="" private=""> is in newreq.pem</and>
※ CA 이 이건

※ CA 의 옵션 : -newreq → CSR을 생성하는 옵션 -newcert → 데모 인증서를 만드는 옵션

입력 시 [ ]안의 내용이 default값입니다. 확인 후 입력합니다.

- ☞ **<password>** WebtoB 가동 시에 물어보는 암호입니다. 암호문을 잊어버리면 인증서를 사용할 수 없으므로 주의하세요.
- ☞ <cn name : domain> 기본적으로 서비스 하는 도메인명을 입력한다.
- default 값([] 안의 값)에 다른 값이 설정이 되어있는 경우는 입력하지 않고 Enter만 치더라도 의도하지 않은 값이 들어갑니다. 이것은 wbssl.cnf 파일에 default값이 설정이 되어있기 때문입니다. 확인하시고 wbssl.cnf를 변경하시기 바랍니다. (주석처리)

④ 개인키 및 CSR 추출

- ☞ 생성된 <newreq.pem>에는 (암호화된) 개인키와 CSR의 정보가 함께 포함 되어 있습니다. 위쪽이 개인키이고 아래쪽이 CSR입니다. 위 개인키(key 값) 및 아래 부분(CSR 값)을 복사하셔서 따로 txt 파일로 저장합니다. 개인키 파일은 꼭 보관하셔야 합니다.
- 개인키(PRIVATE KEY) 정보는 다음과 같습니다.

- ☞ 개인키(PRIVATE KEY) 내용을 파일(\*.txt)로 저장합니다.
- 예) key.txt 로 저장

- CSR 정보는 다음과 같습니다.

----BEGIN CERTIFICATE REQUEST-----

MIIByzCCATQCAQAwgYoxCzAJBgNVBAYTAktSMQ4wDAYDVQQIEwVTZW91bDEOMAwG A1UEBxMFU2VvdWwxDTALBgNVBAoTBEtJQ0ExDDAKBgNVBAsTA0IDQzEbMBkGA1UE AxMSamNsZWUuc2InbmdGUuY29tMSEwHwYJKoZIhvcNAQkBFhJqY2xIZUBzaWdu ... JSHC5uBNGVCOoUOEtSEkUfTi7a5Nt+2/4R/dy+z/SQ==

-----END CERTIFICATE REQUEST-----

☞ CSR 내용을 텍스트(Text) 파일(\*.txt)로 저장합니다.

- 예) csr.txt 로 저장
- ⑤ SSL인증서 발급
  - ☞ 행정전자서명 인증관리센터 홈페이지(<u>www.gpki.go.kr</u>)에서 발급하면 됩니다. <붙임1 SSL인증서 발급 절차 참고>

### 나. 인증서 설치 방법

- ① 발급받은 인증서를 확인합니다.
  - C:\GPKI\certificate\class1 디렉터리에 해당 <*cn name : domain*>.p7b 파일이 있는지 확인합니다. (예: www.gpki.go.kr.p7b)

----BEGIN PKCS7-----

MIILiQYJKoZIhvcNAQcCoIILejCCC3YCAQExADALBgkqhkiG9w0BBwGgggteMIID HTCCAgWgAwIBAgIQSAcIRgAuPO7tcwjaHEc8+jANBgkqhkiG9w0BAQUFADBQMQsw ... 8wQdPqvThnU/td3t6IrVG983r3rrP69GN/qspiJpBIryB019rK0cUeYFK95jaL3E 0lqDgGfm9I5cuWcJ8eaPfU/AIZYkXCss4jJrMQA= ------END\_PKCS7-----

- ② pkcs#7 ⇒ pem 변환 프로그램 설치
  - ☞ pkcs#7 => pem 변환해 주는 프로그램을 설치합니다. Openssl 프로그램으로 변환 할 수 있습니다.
- ③ pkcs#7 ⇒ pem 변환

openssl pkcs7 -in <p7b filename> -out <pem filename> -print\_certs -text

- 여기서 <p7b filename>은 발급받은 인증서의 이름 및 전체 경로이며, <pem filename>은 변환되어 저장될 pem 파일 이름 및 전체 경로를 입력한다.
- 예) openssl pkcs7 -in www.gpki.go.kr.p7b -out cert.pem -print\_cert -text
- ④ CA Chain 인증서 생성
  - <pem filename>파일을 편집기로 열어서 아래와 같은 내용들을 복사하여 각각의 파일을 생성합니다.
  - ☞ 파일 중에서 'RootCA'와 'CA131000001'이 들어있는 부분의 'Certificate:' 에서 '----END CERTIFICATE-----'까지 부분을 전부 복사하여 <*caChain.pem*> 파일을 생성합니다.

# 예) <caChain.pem> 생성 예제

Cartificata:	1	
Data.		
Serial Number:		
4a:65:5e:f5:03:d1:e7:b0:c6:e4:e5:db:e0:d0:52:e5		
Signature Algorithm: sha1WithRSAEncryption		
Issuer: C=KR, O=Government of Korea, OU=GPKI, CN=CA131000001		
~ ~ ~ ~ ~		
Subject: C=KR, O=Government of Korea, OU=Group of Server, CN=www.gpkigo.kr		
~ ~ ~ ~ ~		
BEGIN CERTIFICATE		
MIIDIzCCAgugAwIBAgIQSmVe9QPR57DG50Xb4NBS5TANBgkqhkiG9w0BAQUFADBQ		
~ ~ ~ ~ ~		
kKfuCm04KGUMn3q3OUyaL98ByM3jKeGQKRWviCN6rgfLN71GbnoP	Lino	
END CERTIFICATE		
	12	
Certificate:		
Data:		
Version: 3 (0x2)		
Serial Number:		
3c:c2:81:4b:00:e7:52:4d:9b:aa:47:b7:e1:61:f5:0e		
Signature Algorithm: sha1WithRSAEncryption		
Issuer: C=KR, O=Government of Korea, OU=GPKI, CN=Root CA		
~ ~ ~ ~ ~		cert
Subject: C=KR, O=Government of Korea, OU=GPKI, CN=Root CA		.pem
~ ~ ~ ~ ~		
BEGIN CERTIFICATE		
MIIDmTCCAoGgAwIBAgIQPMKBSwDnUk2bqke34WH1DjANBgkqhkiG9w0BAQUFADBM		
~ ~ ~ ~ ~		
uSuQZ4oqBNo2kxt8Pg==		
END CERTIFICATE	caChain	
	nem	
Certificate:	.pem	
Data:		
Version: 3 (0x2)		
Serial Number:		
48:15:99:5d:01:ea:17:36:01:73:5b:d1:16:f8:25:5c		
Signature Algorithm: sha1WithBSAEncryption		
Issuer: C=KR. O=Government of Korea. OU=GPKI. CN=Root CA		
~ ~ ~ ~ ~		
Subject: C=KR, O=Government of Korea, OU=GPKI, CN=CA131000001		
~ ~ ~ ~ ~		
BEGIN CERTIFICATE		
MIIEnDCCA4SaAwIBAaIQSBWZXQHaFzYBc1vRFvaIXDANBakahkiG9w0BAQUFADBM		
498KpPx9vfeB3R3h130seTSGa4JXanarKoaCbTstU9U=		
END CERTIFICATE		
#### ⑤ Config 설정

- .\$WEBTOBDIR/config 이동하여 httpd.m 파일을 수정합니다.
  - SSL은 443 포트를 사용하기 때문에 버추얼 호스트 노드를 하나 추가해야 합니다. 아래는 SSL을 적용시킨 config 파일 예입니다.

```
*DOMAIN
webtob1
*NODE
gpki
         WEBTOBDIR="/app/tmax/webtob",
                   SHMKEY = 54000,
                  DOCROOT="/app/tmax/webapps",
                  PORT = "80,443",
                  HTH = 1,
                  LOGGING = "log1",
                  ERRORLOG = "log2",
                  JsvPort = 9900
*VHOST
vgpki
         DOCROOT="/app/tmax/webtob/gpki",
                  PORT = "443",
                   NODENAME = "gpki",
                  HOSTNAME = "www.gpki.go.kr",
                  LOGGING = "log3".
                  ERRORLOG = "log4",
                   SSLFLAG = Y,
                   SSLNAME = "ssl1"
*SVRGROUP
htmlg
                  NODENAME = "gpki", SVRTYPE = HTML
                  NODENAME = "gpki", SVRTYPE = JSV
jsvg
*LOGGING
               Format = "DEFAULT", FileName = "/app/tmax/webtob/log/access.log"
log1
log2
               Format = "ERROR", FileName = "/app/tmax/webtob/log/error.log"
               Format = "DEFAULT", FileName = "/app/tmax/webtob/gpki/log/access_ssl.log"
log3
               Format = "ERROR", FileName = "/app/tmax/webtob/gpki/log/error_ssl.log"
log4
*SSL
              CertificateFile
ssl1
                               = "<pem filename>",
               CertificateKeyFile = "<key filename>",
               CertificateChainFile = "<caChain filename>"
```

☞ 빨간색으로 표시된 항목의 파란색 내용을 수정 또는, 추가하셔야 합니다.

*spem filename>*은 발급 받은 인증서 파일의 경로 및 파일명을 입력합니다.
 *key filename>*은 CSR 파일 처음 생성 시 생성한 key 파일을 그대로 사용 해야 합니다.
 *caChain.pem>*은 *spem filename>*에서 복사해서 생성한 파일의 경로 및 파일명을 입력합니다.

⑥ Config 컴파일

☞ 수정된 http.m 파일(실제 환경파일)을 웹 서버에서 사용할 수 있도록 wscfl 명령어를 사용하여 컴파일 하는 과정이 필요합니다.

예) wscfl - i http.m

⑦ 웹 서버 구동

wsboot 명령어를 사용하여 서버를 구동하고, 인증서 생성과정에서 입력했던
 개인키 비밀번호를 입력하시면 됩니다.

\$ wsboot
WSBOOT for node(IISTest) is starting:
Welcome to WebtoB demo system : is will expire 2011/08/10
Today : 2011/08/10]
WSBOOT : WSM is starting : 08/10/11 15:20:00
WSBOOT : HTL is starting : 08/10/11 15:20:00
WSBOOT : HTH is starting : 08/10/11 15:20:00
Current WeboB configuration :
Number of client handler(HTH) =1
Supported maximum user per node = 975
Supported maxinum user per handler = 975
Some of your private key files are encrypted for security reasons.
In order to read them you have to provide us with the pass phrases.
Server IISTest.gpki.go.kr:443 (RSA)
Enter pass phrase : <i><password></password></i>

⑧ 이제 SSL인증서의 설치가 완료되었습니다.

#### 다. 웹사이트 적용

웹사이트 이용시 암호화통신이 가능하도록 웹 프로그램을 수정합니다. ☞ 구축가이드 V장을 참조

#### 라. SSL 인증서 개인키 추출 방법

※ 웹방화벽 및 개인정보 필터링에 적용시 필요

☞ WebtoB의 경우 개인키가 파일형태로 저장되므로 추출할 필요가 없습니다.

- csr파일 생성 시 생성되는 newreq.pem 파일의 내용은 개인키와 csr 두 개의 블록으로 구성됩니다. 아래와 같이 첫 번째 블록의 내용을 확인 후 해당 내용을 파일(key.txt)로 저장합니다.

- KEY 정보는 다음과 같습니다.

# 2.5. iPlanet 서버에서 보안서버 구축하기

가. 개인키 생성 및 CSR 생성 방법

서버관리 화면에서 서버 선택
 서버관리 화면의 콤보박스에서 보안서버를 구축하고자 하는 웹 서버를 선택
 하고 'Manage' 버튼을 누릅니다.

<ul> <li>Web Server Administration Server - Microsoft Internet Explorer</li> </ul>					
· 파일(E) 편집(E) 보기(У) 즐겨찾기(A) 도구(I) 도움말(H)					
🌀 뒤로 • 🕥 - 💌 😰 🏠 🔎 검색 🌟 즐겨찾기 🤣 🔗 • 🌺 🔂 • 🦲 🗞 🦚 🦓					
: 주소(D) 🕘 http:// /https-admserv/bin/index	/ 🔁 이동				
iPlanet <sup>TM</sup> Web Server Administration Server Servers Preferences Global Settings Users and Groups Security Cluster Mgmt					
Manage Servers       Manage Servers         Add Server       Select a Server:         Remove Server       Select a Server:         Migrate Server       Settings         Settings       .or.kr         Hostname:       .or.kr         Error Log:       /usr/iplanet/servers/https-         User:       .or.kr         Brow of Log:       /usr/iplanet/servers/https-         User:       .or.kr         Help					
중 Users and Groups 🖉 인터넷					

② CSR 생성

Security Tab을 누르고 왼쪽 메뉴에서 'Create Database'를 선택하여 CSR을 생성시 이용되는 웹 인스턴스를 생성하기 위해 패스워드를 입력합니다.



iPlanet 웹서버가 설치된 디렉토리 밑의 certutil.exe 파일이 있는 경로로 이동합니다. (윈도우 OS에 iPlanet을 default로 설치했을 경우 certutil의 경로는 C:\Sun\WebServer6.1\bin\https\admin\bin입니다.)

아래의 명령을 서버에 맞게 조합해서 실행합니다.

```
certutil -R -s "CN=[도메인명],OU=Group of Server,O=Government of Korea,C=KR" -a -o [CSR이
저장될 위치] -k rsa -g 2048 -d [iPlanet 웹서버가 설치된 경로밑의 alias 디렉토리] -P [웹 인스턴
스명-]
```

\*OU, O, C 값은 고정값입니다. 수정하거나 하실 필요없이 가이드 그대로 하시면 됩니다.

예) certutil -R -s "CN=www.domain.com,OU=Group of Server, O=Government of Korea,C=KR" -a -o c:\csr.csr -k rsa -g 2048 -d c:\Sun\WebServer6.1\alias -P https-test1-498db9821efb4d4-

③ SSL인증서 발급

☞ 행정전자서명 인증관리센터 홈페이지(<u>www.gpki.go.kr</u>)에서 발급하면 됩니다. <붙임1 SSL인증서 발급 절차 참고>

### 나. 인증서 설치 방법

•••

- ① 발급받은 인증서를 확인합니다.
  - C:\GPKI\certificate\class1 디렉토리에 해당<*cn name : domain*>.p7b 파일이 있 는지 확인합니다.(예: <u>www.gpki.go.kr.p7b</u>)(와일드카드 SSL인증서일 경우는 wildcard.domain.p7b로 생성됨.)

----BEGIN PKCS7-----

MIILiQYJKoZIhvcNAQcCoIILejCCC3YCAQExADALBgkqhkiG9w0BBwGgggteMIID HTCCAgWgAwIBAgIQSAcIRgAuPO7tcwjaHEc8+jANBgkqhkiG9w0BAQUFADBQMQsw

8wQdPqvThnU/td3t6IrVG983r3rrP69GN/qspiJpBIryB019rK0cUeYFK95jaL3E

0lqDgGfm9I5cuWcJ8eaPfU/AlZYkXCss4jJrMQA=

----END PKCS7-----

### ② pkcs#7 ⇒ cer 변환

- 인증서 파일 <p7b filename>을 윈도우 환경에서 더블클릭 하여 파일을 open합 니다. 아래와 같은 창이 열립니다.

🌇 certmgr - [민증서 - 파일₩C:₩GPKI₩CI	🔓 certmgr - [인증서 - 파일₩C:₩GPKI₩CERTIFICATE₩CLASS1₩TEST2,GPKI,GO,KR,P7B₩인증서] 📃 🗖					
파일(E) 동작(A) 보기(V) 도움말(U)						
(월) 인증서 - IF일 ⊡	발급 대상 A E CA13100001 B Root CA E test2.gpki.go.kr	Ĭ발급자 Root CA Root CA CA131000001	만료 날짜 2010-07-21 2012-04-21 2010-04-08	응도 《모두》 《모두》 시버 인종		
	<b>   </b>			Þ		
C:₩GPKI₩CERTIFICATE₩CLASS1₩TEST2, GP	C:₩GPKI₩CERTIFICATE₩CLASS1₩TEST2,GPKI,GO,KR,P78 저장소에 3개의 인증서가 있습니다.					

- 인증서 파일(예: CA131000001)을 선택 후 마우스 우측버튼을 클릭하여 "모든작업(<u>K</u>) - 내보내기"를 클릭합니다.

<mark>@ certmgr - [인증서 - 파일₩C:₩GPKI₩CERTIFICATE₩CLASS1₩TEST2,GPKI,GO,KR,P7B₩인증서]</mark> 파일(F) 동작(A) 보기(V) 도움말(H)				
(월 연종세 - 파일 현· C:₩GPKI₩CERTIFICATE₩CLASS1₩TE └	발급 대상 A ECA13100001 Particles 2:9 모든 작업(K) * 복사(C) 도움말(H)	발급자 Root CA Root CA 열기 내보내기	만료 날짜 2010-07-21 2012-04-21 2010-04-08	용도 《모두》 《모두》 서비 인증
항목에서 실행할 수 있는 작업이 들어 있습니다.				

- 인증서를 "Base 64로 인코딩된 X.509(.CER)"을 선택하여 저장합니다.

민증서	4 내보내기 마법사	×
Щ	<b>)일 내보내기 형식</b> 인증서를 여러 형식으로 내보낼 수 있습니다.	
	사용할 형식을 선택하십시오. C DEB로 인코딩된 X 509 HHUH 1리(CEB)(D)	
	<ul> <li>☞ Base 64로 인코딩된 X,509(,CER)(<u>S</u>))</li> <li>☞ 암호화 메시지 구문 표준 - PKCS #7 인증서 (,P7B)(<u>C</u>)</li> </ul>	
	<ul> <li>□ 가능하면 인종 경로베 있는 인종서 모두 포함([)</li> <li>○ 개인 정보 교환 - PKCS #12(,PFX)(P)</li> <li>□ 가능하면 인종 경로에 있는 인증서 모두 포함([J))</li> </ul>	
	■ 강력한 보호 사용(Internet Explorer 5,0, NT 4,0 SP4 미상 필요)(E) ■ 내보내기가 완료되면 개인 키 삭제(K)	
	< 뒤로( <u>B</u> ) 다음( <u>N</u> ) > 취소	
5	2개 이즈서르 ㅁ드 "Page 64근 이크디딘 V 500( CED)"이근	H

☞ 3개 인증서를 모두 "Base 64로 인코딩된 X.509(.CER)"으로 변환하여 저장합 니다. (②번 과정 반복) ③ Server Certificate를 iPlanet 웹 서버에 설치

- 관리자 화면에서 Security → Install a Certificate를 선택한 후, 아래 화면에서 표시된 부분의 정보를 채워 넣습니다.

Install a Server Certificate	
Certificate For:	
C This Server	
Server Certificate Chain	
Trusted Certificate Authority (	CA)
Select the module to use with this	s certificate:
Cryptographic Module: Internal	
Key Pair File Password: ••••••	
Enter Certificate Name ONLY if co Certificate Name:	ertificate is not for 'This Server'.
C Message is in this file:	
Message text (with headers):	MJAUMJEWOTA3MIDL VEWXLZAJBGNYBAYTAKESMHWWGGYDYUUKEXNHD3216 552W5U IGGmIEtvor UndDovCwYDYDQLEWRHUEtJMRAwDgYDYQQDCwdSb2301ENBMIIBTNA BydahkidsWDBADEFAAOCAQA4MIIEQCKCAQBAIEFCFyxQUH+asoOPG009KSV121xm L41cxJUCUw9p8ScLvrwWba9tNKNKAirrxNBroBC90tcLV9+Q301ta8/3MQ9NkWS srh-ØbysxBrk2N5tzr0kjIB+SPStjtmGGTUDirccdS2CW0rspctxAvFEMYNKeez0 Zf8cTNmi19y2f7mrVrnTP1PGAWY2H4/2jdWBELsymbAtS3006Vy4yrqUDzzpc Ig492,VwcXb7RMBrACEmcDrhquvNSfs7VrhQW1a1BiySPrUAvIS/V0NCbo2i4052 raVDmP0v98Xo4PDVpr2gaW9ybo6ND8v2+0v2zftzndUBc4X2941f9yNAgMBAAGi eD82M8BGAIbVL9QMBBFAFIT7q4c1DgsqfBv61+fBzqT70d0MB0GA1Ud0g0WP6ac E+6uHCA4LKnwb-physcBc49HDA0BgNVH08BAf8EBAARCA0VwEWVDP0cxWWCjA1
OK	Reset

☞ "RootCA" 인증서를 변환한 파일(②번)을 편집기로 열어서 안의 내용을 복사 하여 위 내용을 채워 넣습니다.

Install a Server Certificate	
Certificate For:	
C This Server	
Server Certificate Chain	
C Trusted Certificate Authority (	CA)
Select the module to use with this Cryptographic Module: Internal -	s certificate:
Key Pair File Password: ••••••	
Enter Certificate Name ONLY if co Certificate Name:	ertificate is not for 'This Server'.
Message is in this file:	
Message text (with headers):	LzEwLJEUNU/Eusokotikz95L2NUPVJv50g000Es5U991BLSSkvP004004/Ebn11bn0g ▲ b2Yg502v2F084EsY21LUJ9104X805J04H1SZX2VP20849ub61240t i a¥bcnink5QVJ KoarniveNAQEFBQADggEBADRoA11QdaxbGu+j15keuFJiP0fexg6MU26kJhEqbs/ #20s51VakGhBod9hkyabj7Q1UGA3n1go1akwXrwxpPm11brJJSV/5UgZJ+4tWD07 hrSK0D+65248102/9X80LFW5n1W7RVEp+F4p/Kwa161ROSN8kw91w0mx0EiU+wR VVHqz82R4NEP06BonzdYML1+p9HzJcR3ChVcgjmQ2Q4SDFGo0d+PTs2tB8+Mc5p %C2XF272BD1-990GH713830itUb32eveus/r0V3+qvm1mkEiv1HTX2srRxR5gUr 3mNb sTSW00AZ+b0j1y5Zwnx5o99T8CV1iRcKyziMms= END SERTIF10ATE
ОК	Reset

☞ "CA131000001" 인증서를 변환한 파일(②번)을 편집기로 열어서 안의 내용을 복사하여 위 내용을 채워 넣습니다.

Install a Server Certificate	
Certificate For:	
This Server	
Server Certificate Chain	
C Trusted Certificate Authority	( (CA )
Select the module to use with the Cryptographic Module: internal sectors	his certificate:
Key Pair File Password: •••••	•••
Enter Certificate Name ONLY if Certificate Name: Message is in this file:	certificate is not for 'This Server'.
Message text (with headers	): FoAUAC8X rpl://woy3VUExbbit in 0axspUwHUVDVHU0EBVE+C01 vb Tmouv12gm ta AIX OCb4QLx3MA4GA1UdbwEB/wQEAw1FoDATB9NVHSUEDDAKB9grBgEFBQCDA1ANTB4g Hur3SWOBAQUFAA0CAQEAVsyQLaA/kD0s1txVSHcz1C1WFcu106aB6JTe5S7P+Rbit 42UNaNiiLUDt5T9iDc2s81rhCyp9Y9gy1247mLgV2s68V4qLDC85Gfb-ErwufYt EGuuz4vFm6nSVe/8c1F5CyAU2d9pxju07TFVr3owp9ArXofF61122b+7q9/xkHz uv7Va24VFRaLPBoa8QkHEv17s06b6nXVwoNd0UPKtR4/GJ/4dqBeV20v2VPwQV/0 PxiP+F0sHgt34gNubZmmVCEREp1RsT/WW1Ev10A4C+nbymjEbg48JtLLejHN1Mz 7f10st_4fp0VWviz2UITNVd8a1nuDISdra1TWo/xSA== END-SEPTLE1CATE
OK	Reset
🖙 <cn :="" domai<="" name="" th=""><th>↗&gt;인증서를 변화한 파일을 텍스트로 열어</th></cn>	↗>인증서를 변화한 파일을 텍스트로 열어

☞ <cn name : domain>인증서를 변환한 파일을 텍스트로 열어서 안의 내용을 복사하여 위 내용을 채워 넣습니다. (와일드카드 SSL인증서일 경우는 \*.domain으로 입력합니다.)

④ iPlanet 웹 서버를 재시작(Server Off → Server On)

iPlanet ** Web Server 6.0	v. or.kr	🐱 Server Manager	Class Manager Apply
Preferences Sec	rity Logs Monito	Virtual Server Class V 2ava V Legacy Serviets V Search	
On / Off	Server On / Off		
Performance Turing			
Magnus Editor		The server is currently On.	
Add Listen Socket		WARNING: You should only do this on your local machine.	
Edit Listen Sockets	The following pa	sswords are required to start the server:	
MIME Types	Module internal	:	
Restrict Access		Server On Server Of	
Restore Configuration		About this server	
File Cache Configuration			Help
Ihread Pools			

⑤ iPlanet 웹 서버 설정 변경

iPlanet 웹 서버에 인증서 설치가 완료됐다면, 서버에서 443 포트에 대하여 대기 (Listen)할 수 있도록 설정을 변경해야 합니다.

웹서버 관리자 화면에서 Preference → Add Listen Socket을 선택하여 아래와 같 이 정보를 입력한 후 'OK'를 선택합니다.

Planet Web Server 6.0	ar.kr s	Server Manager			Class Manager Apply
Preferences Secu	rity Loos Monitor	Virtual Server Class 🕖	ava Legacy Serviets	Search	
Qn / Off	Create a Listen Sor	ket			
Performance Tuning	ID:				
Magnus Editor	IP: 0.0				
Add Listen Socket	Port: 443 Servername: www	pe kr			
Edit Listen Sockets	Security: On v				
MIME Types	Default VS:	a and a			
Restrict Access	OK		Reset		leip
Restore Configuration					
File Cache Configuration					
Thread Pools					

입력해야 할 정보는 다음과 같습니다. (그림의 밑줄 참고)

ID : 이전 80포트에 대한 ID를 참고하여 SSL 포트를 위한 ID를 부여
IP : 0.0.0.0 / any 로 설정
Port : 443, SSL 포트는 443이 디폴트 포트이며, 서버 관리자와 상의하여 다른 포트를 사용하도록 설정 변경도 가능
Servername : 웹 서버명
Security : 'On' 선택
Default VS : 디폴트로 사용할 Virtual Server url을 입력

⑥ iPlanet 웹 서버 설정 추가변경

SSL에 대한 443Listen 기능을 입력한 후, 추가로 설정해야 할 부분이 있다 면 동일 화면에서 'Edit Listen Sockets'를 선택한 후 'Attributes' 링크를 클릭하여 수정합니다. 이 화면에서 SSL2, SSL3/TLS에 대한 설정을 변경하거나 iPlanet 기본 설정 값으로 리셋 할 수 있습니다.

iPlanet Web Server 6.0	.or.kr	🞽 Server Manager		Class Manager Apply
Preferences Secur	ity Logs Monito	ar 🗸 Virtual Server Class 🗸 Java	Legacy Serviets Search	
	-			
<u>Qn/Qff</u>	Listen Sockets	Table		
Performance	LISTER BOCKES	F dere		
Intering	Action ID	IP Port Security A	cceptors Advanced	
Magnus Editor	Edit 💌 1 0.0.	0.0 08 0.0	Groups	
Add Listen Socket	Edit 💌 🔤 2 0.0.	0 443 On Cttributes	Groups	
Sharkes		ОК	Reset	Help
Sockets				
MIME Types				
Restrict				
Configuration				
Eile Cache Configuration				
Thread Pools				

Planet Web Server 6.0	vor.kr	👿 Server Manager		Slass Manager Apply
Preferences 000	urity Logs Monitor	Virtual Server Class 7	1va V Legacy Servlets V Searc	ā\
On / Off	Security Settings	of Listen Sacket		<i><i>w</i></i>
Performance Tuning	IP Certificate	Name Client Auth	iphers Default	
Magnus Editor	default Server-Cert 🛩	Off SSL	SSL3/TLS Cipher Default	
Add Listen Socket	OK		Reset	Help
Edit Listen Sockets				
MIME Types				
Restrict Access				
Restore Configuration				
File Cache Configuration				
Thread Pools	5			

⑦ 이제 SSL인증서의 설치가 완료되었습니다.

#### 다. 웹사이트 적용

웹사이트 이용시 암호화통신이 가능하도록 웹 프로그램을 수정합니다. ☞ 구축가이드 V장을 참조

#### 라. SSL 인증서 개인키 추출 방법

※ 웹방화벽 및 개인정보 필터링에 적용시 필요

- iPlanet(Sonone)의 경우 인증서 정보가 server\_root/alias에 cert8.db, key3.db
   파일 안에 저장됩니다. 해당 파일에서 개인키를 분리하기 위해서는 pk12util.exe
   라는 프로그램을 실행하여, p12형식으로 인증서 분리 후 OpenSSL프로그램으로
   개인키를 분리할 수 있습니다.
- ① 관리자 페이지에 접속하여, 해당 서버 선택 후 Manage버튼을 클릭 합니다.

w Sun. Sun™ON	IE Web Server 6.1 Administration Server
Sur"Or Servers Manage Servers Add Server Remove Server Migrate Server	At web Server 6.1 Administration Server Ces Global Settings Users and Groups Security Cluster Mgmt Manage Servers Select a Server: Manage Settings Hostname:mhlee DNS: off Help

 ② Security -> Manage Certificates버튼 클릭 후 해당 서버의 Certificate Name을 확인합니다.

Adminis     Sun     Preferences     Security	stration Server > mhlee 🚽 Manage NE Web Server 6.1 Server Manager urity V Logs V Monitor V Yirtual Server Class V Java V	
<u>Create</u> <u>Database</u> <u>Request a</u> <u>Certificate</u>	Manage Server Certificates Server Certificates	
Install Certificate	Certificate Name	Тур
Change	<u>Server-Cert</u>	Own
Manage	<u>Builtin Object Token:ABAecom (sub., Am. Bankers</u> <u>Assn.) Root CA</u>	Trus
Certificates	Builtin Object Token:AddTrust External Root	Trus

- ③ 프로그램 실행 전 선행사항은 PATH 설정입니다. pk12util 프로그램 검색 후 해당 디렉토리를 PATH에 설정 해 주십시오.
- ex) PATH %server\_root%\bin\https\admin\bin;
- ④ server\_root/alias 밑의 database파일 명칭을 확인해 주십시오.

이름 🔺	371	종류	수정한 날짜
Shttps-mhlee-mhlee-cert8.db	64KB	데이터베이스 파일	2009-04-14 오후 2:47
🔊 https-mhlee-mhlee-key3.db	16KB	데이터베이스 파일	2009-04-14 오후 2:47
🔊 secmod.db	16KB	데이터베이스 파일	2009-04-13 오전 11:13

⑤ 시작 -> 실행에서 command를 입력하고 확인 버튼을 클릭 하십시오. pk12util 프로그램이 위치한 디렉토리로 이동 후 아래의 명령어를 실행합니다.

```
$ pk12util -o certpk12.p12 -n Server-Cert -d c:₩JOB₩WebServer6.1₩alias -P
https-mhlee-mhlee-
Enter Password or Pin for "NSS Certificate DB" :
Enter Password for PKCS12 file :
Re-enter password :
pk12util : PKCS12 EXPORT SUCCESSPUL
```

⑥ 패스워드 확인메시지가 나오면 아래의 창에서 입력했던 패스워드를 입력해 주십시오. 패스워드 3번 확인 후 해당 파일이 현재 위치에 생성됩니다.

♦ Sun nerregelern S	dministration Server > mhlee ▼ Manage un~ONE Web Server 6.1 Server Manager
Preferences	Security Logs Monitor Virtual Server Class Java
<u>Database</u> <u>Request a</u> <u>Certificate</u>	WARNING: You should only do this or Database Password:
Install Certificate Change Password	Password (again): OK Reset

- ※ 주의) -P옵션 뒤의 내용은 server\_root/alias에서 확인한 파일명에서 각각 key3.db를 제외한 부분을 입력해 주셔야 합니다.
- ⑦ 실행 디렉토리에서 certpk12.p12 파일의 생성여부를 확인합니다. 일단 여기까지의
   작업이 iplanet의 db 파일에서 p12형식으로 인증서를 내보내는 작업입니다.
- ⑧ key추출을 하기위해 openssl/bin/ 디렉토리로 이동 후 아래의 명령어를 실행 합니다. 패스워드는 pk12util실행시의 패스워드와 동일합니다.

\$ openssl pkcs12 -in certpk12.p12 -nocerts -nodes -out certpk12.key
Enter Import Password :
MAC verified OK

⑨ 생성된 파일의 생성여부와 내용을 확인합니다. 해당 파일을 열어보면 아래와 같은 내용으로 확인 됩니다.



### 2.6. Tomcat 서버에서 보안서버 구축하기

Tomcat에서는 java의 keytool 프로그램을 사용하여 KEY값 및 CSR값을 생성하여 처 리합니다. (http://developers.sun.com/downloads/)에서 java sdk를 다운받아 설치합니 다. Apache 서버 또는, 그 외 다른 웹 서버와 연동하여 사용하는 경우에는 해당하는 웹 서버에 SSL인증서를 적용해야 합니다. Tomcat 단독으로 서비스를 하는 경우에 아 래 내용을 참고합니다.

- keystore 는 Private Key와 Public Key로 사용되는 인증서(x.509)가 저장되는 데이터 베이스입니다.
- keytool 은 Private Key와 Public Key로 사용되는 인증서(x.509)가 저장된 keystore를 관리하는 툴입니다.
- keystore alias name

항목	내용
Caliac name	개인키
<anas name=""></anas>	서버 인증서 등록
<rootca alias="" name=""></rootca>	Root CA 인증서 등록
<cachain alias="" name=""></cachain>	CA Chain 인증서 등록

#### 가. 개인키 생성 및 CSR 생성 방법

- ① Keystore 생성
  - SSL을 구축하기 위해서는 Keystore를 만들어야 한다. Keystore를 만들기 위해 keytool 프로그램을 이용하여 아래와 같이 실행한다.

\$ keytool -genkey -alias *<alias name>* -keyalg RSA -dname "CN=*<CN name : domain>*, OU=Group of Server, O=Government of Korea, C=KR" -keystore *<keystore filename>* -keysize 2048 keystore 암호를 입력하십시오: *<password1>* (keystore 암호와 같은 경우 Enter을 누르십시오): *<password2>* 

- ☞ **<alias name>**은 Key값 및 인증서를 저장할 저장소 이름입니다.
  - ☞ <**CN** name : domain>은 인증관리센터에 등록된 CN값으로 입력합니다. 인증서 발급 안내 E-mail 및 인증관리센터에 확인 하십시오.
  - ☞ password1>는 담당자가 원하는 비밀번호로 설정하여 입력하면 Keystore가 생성됩니다.
  - **c c** <
  - ☞ <keystore filename>은 Keystore가 파일형태로 저장될 경로 및 파일 이름입니다.
  - 예) \$ keytool -genkey -alias CERT -keyalg RSA -dname "CN=www.gpki.go.kr, OU=Group of Server, O=Government of Korea, C=KR" -keystore gpkikeystore -keysize 2048 keystore 암호를 입력하십시오: cpassword1> (keystore 암호와 같은 경우 Enter을 누르십시오): cpassword2>

- ② CSR(Certificate Signing Request) 생성
  - SSL 인증서를 발급 받기 위해서는 CSR 데이터가 필요하다. 이를 위해서 keytool 프로그램을 이용하여 아래와 같이 실행한다.

- □ T ① Keystore 생성 시 입력한 <alias name>과 password1>, <keystore filename>를 입력 합니다.
- ☞ 위 화면에서 "-----BEGIN NEW CERTIFICATE REQUEST-----"부터 "-----END NEW CERTIFICATE REQUEST-----"까지를 복사하여 텍스트 파일로 저장합니다.
- 예) keytool -certreq -alias CERT -keystore gpkikeystore

③ SSL인증서 발급

☞ 행정전자서명 인증관리센터 홈페이지(<u>www.gpki.go.kr</u>)에서 발급하면 됩니다. <붙임1 SSL인증서 발급 절차 참고>

### 나. 인증서 설치 방법

- ① 발급받은 인증서를 확인합니다.
  - C:\GPKI\certificate\class1 디렉터리에 해당 <*cn name : domain*>.p7b 파일이 있는지 확인합니다. (예: <u>www.gpki.go.kr.p7b</u>)
  - ※ 와일드카드 SSL인증서일 경우는 wildcard.domain.p7b로 생성됨.

END PKCS7
0lqDgGfm9l5cuWcJ8eaPfU/AlZYkXCss4jJrMQA=
MIILiQYJKoZlhvcNAQcCoIILejCCC3YCAQExADALBgkqhkiG9w0BBwGgggteMIID
BEGIN PKCS7

- ② pkcs#7  $\Rightarrow$  cer 변환
  - 인증서 파일 <p7b filename>을 윈도우 환경에서 더블클릭 하여 파일을 open합 니다. 아래와 같은 창이 열립니다.

🌇 certmgr - [민증서 - 파일₩C:₩GPKI₩CE	ERTIFICATE#CLASS1#T	'EST2,GPKI,GO,KR,P7B₩인증	§∦]	_ 🗆 🗵
파일(E) 동작( <u>A</u> ) 보기(⊻) 도움말( <u>H</u> )				
E UEAL EN LE LA LE	발급 대상 / 코 CA13100001 교 Root CA 코 test2.gpki.go,kr	불급자 Root CA Root CA CA131000001	만료 날자 2010-07-21 2012-04-21 2010-04-08	용도 《모두》 《모두》 《민주》 시비 인종
				•

- 인증서를 선택(예: CA131000001) 후 마우스 우측버튼을 클릭하여 "모든작업(K) - 내보내기"를 클릭합니다.

隋 certmgr - [인증서 - 파일₩C:₩GPKI₩CI	ERTIFICATE#CLASS1#TES	ST2, GPKI, GO, KR, P7B\	/민증서]	_101 ×
파일(E) 동작( <u>A</u> ) 보기(⊻) 도움말( <u>H</u> )				
	발급대상 /	발급자	만료 날짜	85
III C:#GPNI#CENTIFICATE#CLASST#TE	Boot C 열기	Boot CA	2010-07-21	〈모두〉 〈모두〉
	test2.g 모든 작업(K) ▶	· · · · · · · · · · · · · · · · · · ·	2010-04-08	서버 인증
	早れ(())			
		ur±ur>1		
	도움일(년)			
항목에서 실행할 수 있는 작업이 들어 있습니다.	1.1			

- "DER로 인코딩된 X.509바이너리(.CER)"을 선택하여 저장합니다.

인증서 내보내기 마법사	×
파일 내보내기 형식 이즈서를 대려 형신으로 내보낼 수 아스티다	
사용할 형식을 선택하십시오.	
○ DER로 인코팅된 X,509 바이너리(,CER)(D)	
○ Base 64로 인코딩된 X,509(,CER)( <u>S</u> )	
C 암호화 메시지 구문 표준 - PKCS #7 인증서 (,P7B)(C)	
□ 가능하면 인종 경로에 있는 인증서 모두 포함(j)	
C 개인 정보 교환 - PKCS #12(,PFX)(P)	
가능하면 인종 경로에 있는 인증서 모두 포함(U)	
🗖 강력한 보호 사용(Internet Explorer 5,0, NT 4,0 SP4 미상 필요)(E)	
🗖 내보내기가 완료되면 개인 키 삭제(K)	
<u> </u>	소 .
· = BootCA 미 CAChaire 이즈시르 모드 "DED로 이	그디디

☞ RootCA 및 CAChain 인증서를 모두 "DER로 인코딩된 X.509바이너리 (.CER)"으로 변환하여 RootCA 인증서는 ca.cer 로 CAChain 인증서는 caChain.cer 로 저장합니다.

- ③ RootCA 인증서 Keystore에 등록하기
  - 파일로 저장한 RootCA 인증서를 Keystore에 저장해야 사용 할 수 있습니다. 이를 위해서 Keytool 프로그램을 이용하여 아래와 같이 실행한다.

☞ <RootCA alias name>은 RootCA 인증서를 저장할 저장소 이름입니다.

☞ <RootCA filename>은 RootCA 인증서 파일이 존재하는 경로 및 파일 이름입니다.

☞ "가. 개인키 생성 및 CSR 생성 방법"에서 입력한 password1>와 <keystore
filename>를 입력합니다.

- ☞ "이 인증서를 신뢰하십니까?[아니오]"라고 물어오면 y를 입력합니다.
   예)keytool-import-alias RootCA-trustcacerts -file ca.cer -keystore gpkistore
- ④ CAChain 인증서 Keystore에 등록하기
  - 파일로 저장한 CA 인증서를 Keystore에 저장해야 사용 할 수 있다. 이를 위해서 keytool 프로그램을 이용하여 아래와 같이 실행한다.

\$ keytool -import -alias <CAChain alias name> -trustcacerts -file <CAChain
fillename> -keystore <keystore filename>
keystore 암호를 입력하십시오: <password1>
인증이 keystore에 추가되었습니다.

☞ **<CAChain alias name>**은 CA 인증서를 저장할 저장소 이름입니다.

- ☞ **<CAChain filename>**은 CA 인증서 파일이 존재하는 경로 및 파일 이름입니다.
  - ☞ "가. 개인키 생성 및 CSR 생성 방법"에서 입력한 password1>와 <keystore
    filename>를 입력합니다.
  - 예) keytool-import-alias CAChain.-trustcacerts -file caChain.cer -keystore gpkistore

- ⑤ Server 인증서 Keystore에 등록하기
  - 파일로 저장한 서버용 인증서를 Keystore에 저장해야 사용 할 수 있다. 이를 위해서 Keytool 프로그램을 이용하여 아래와 같이 실행한다.

```
$ keytool -import -alias <alias name> -trustcacerts -file <도메인 인증서>
-keystore <keystore filename>
keystore 암호를 입력하십시오: <password1>
인증서 회신이 keystore에 설치되었습니다.
```

- ☞ <도메인 인증서>는 발급 받은 서버 인증서 파일이 존재하는 경로 및 파일 이름입니다. (와일드카드 SSL인증서일 경우는 \*.domain으로 입력합니다.)
- ☞ "가. 개인키 생성 및 CSR 생성 방법"에서 입력한 password1>와 <keystore</pre>
  filename>, <alias name>을 입력합니다.
- 예) keytool -import -alias **CERT** -trustcacerts -file **www.gpki.go.kr.cer** -keystore **gpkistore**
- ⑥ Config 설정
  - \$TOMCAT\_HOME/conf/server.xml파일에 Connector를 추가 또는, 수정하여 보안 웹 페이지를 사용 할 수 있도록 해야 합니다.
  - "<Connector port="443"" 으로 시작하는 Connector를 찾아 주석처리 되어 있으면 아래와 같이 수정하고, 없으면 아래 내용을 추가합니다.

```
<Connector port="443"
```

```
protocol="HTTP/1.1" SSLEnabled="true"
maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
enableLookups="false" disableUploadTimeout="true"
acceptCount="100" debug="0" scheme="https" secure="true"
keystorePass="<password1>" keystoreFile="<keystore filename>"
clientAuth="false" sslProtocol="TLS" />
```

- ☞ "가. 개인키 생성 및 CSR 생성 방법"에서 입력한 password1>를 입력 합니다.
  - ☞ **<keystore filename>**은 Keystore가 파일형태로 저장될 경로 및 파일 이름 입니다.
  - ☞ **port="443"**은 https 프로토콜을 이용하는 기본 포트입니다. Thread 수량은 환경에 따라서 적당히 설정하여 주시면 됩니다.
  - ☞ sslProtocol="TLS" 값을 sslProtocol="SSL"로 변경하여 사용해도 합니다.(익스플로러 6.X 버전을 위해)

- ⑦ Tomcat 서버 재부팅
  - Tomcat 서버를 재부팅 합니다.
- ⑧ 웹 브라우저를 통해 SSL인증서 정상 적용 유무 확인
  - 웹 브라우저의 주소에 "https://도메인" (예: https://www.gpki.go.kr)이라 입력 후 엔터를 치면 주소 입력란 옆에 자물쇠 모양이 나타나는 것을 볼 수 있으며, 자물쇠를 클릭하면 "신뢰할 수 있는 사이트"라고 나타나는 것을 확인할 수 있습니다.



다. 웹사이트 적용

웹사이트 이용시 암호화통신이 가능하도록 웹 프로그램을 수정합니다. ☞ 구축가이드 V장을 참조

라. SSL 인증서 개인키 추출 방법

※ 웹방화벽 및 개인정보 필터링에 적용시 필요

1 tomcat의 경우 java프로그램으로 개인키를 추출 할 수 있습니다.
 □ exportprivatekey.zip 을 다운로드 받습니다.

② 아래의 exportprivatekey.zip 을 실행합니다. 파라미터는 각각 아래와 같습니다.

<keystore filename> - keystore 파일명 <alias name> - Private key 가 들어 있는 저장소 <password> - keystore 비밀번호 <key filename> - 생성할 개인키 파일명

\$ java exportprivatekey.zip <keystore filename> JKS calias name> <key</pre> filename>

예) java exportprivatekey.zip gpkikeystore JKS 비밀번호 CERT gpki.key

③ 명령어 실행하면 아래와 같이 파일이 생성됩니다.

2006/04/08	오후 03:29	<dir></dir>	
2006/04/08	오후 03:29	<dir></dir>	
2006/04/08	오후 03:29	902	gpki.key

④ 파일의 내용은 아래와 같습니다.

#### ----BEGIN PRIVATE KEY-----

MIICdQIBADANBgkqhkiG9w0BAQEFAASCA18wggJbAgEAAoGBALX0vHazjBblihrdw11QhTPaeOoQ9wDG1MTW68yhb1P778UJUW Xk9WsPo6pTJJj/fEZv6X5Dzoc654FwpJejWECot4B0a7x80ftSc+aDf5MZluVR0+u00lPfG5gmleVnk9/Br1bkUa/c0WwjeUK+ CB7bQs6yc+WA7xeIQsWJZdyFAgMBAAECgYAx7YDVVXkoQz39F0KhFlonm1k4aQVN+i+SP6MeWGGMvAHT4DWsrwHEqdrv/rZ5IQ m5zjWUxwhhxQEHXKBdV538UYfVaO9oozlgltXMBt5I2lJRImLXLN1/5/4yRPg9x+i/Z14JI+kNC3XQcti8I7zr9AZRnJC/w+we HfMpF0vI1iVMKQDdSA39rsjyzgz8Pe/wPdf3rtBx+PgNX7VCvyxA8SoGhUdcbt174B4RHUIDzM4DRGqZAkB1+18Ph6Z/mFta5d 5ko150x38cOmqEqENHuoQZ6tvrwYSQKY8mIoEhP1+yUKxopam+SGXsuXOw7nOhbHYIO31xAkAjOzyXOZVIsitf4A4b8v9LtbgL RmwOeH7aOR6peQOPd5qucI54DHUOeVDvglt14yFVYE5yxFWips4bWJF01wP1

-----END PRIVATE KEY-----

### Ⅲ 이중화된 웹서버 SSL 적용방법

이중화 서버나 와일드카드 인증서를 사용하여 여러개의 서버에 적용하는 방법입니다.

### 3.1. IIS 서버의 경우

개인키 추출시 생성한 확장자 pfx파일을 적용할 서버로 업로드 합니다. mmc를 실행 하여 인증서항목을 추가합니다.

- 개인의 인증서 항목에서 오른쪽 마우스를 클릭하여 가져오기를 선택합니다.



- 다음을 선택합니다.

인증치 가져오기 마법사	
	인증서 가져오기 마법사 시작
	마법사를 사용하면 인증서, 인증서 신뢰 목록, 인증서 해지 목록을 디스크에서 인증서 저장소로 복사할 수 있습니다.
	인증서는 인증 기관미 발급하는 것으로 사용자 신분을 확인 합니다. 인증서에는 데이터를 보호하거나 보안된 네트워크 연결을 하는 데 필요한 정보가 들어 있습니다. 인증서 저장소 는 인증서를 저장하는 시스템 영역입니다.
	계속하려면 [다음]을 클릭하십시오.
	< 뒤로(B) 다음(N) > 취소

- 가져올 파일을 지정합니다.(붙임3에서 내보낸 확장자 pfx 파일)



- 개인키 암호를 입력합니다.



- 기본선택 후 다음을 선택합니다.



### - 마침을 선택합니다.

인증서 가져오기 마법사		×
	인증서 가져오기 마법사 완료	
	다음 설정을 지정했습니다. 사용자가 선택한 인증서 저장소 개인	
	내용 PFX 파일 이름 D:₩job₩일별업무내역₩보	
	< 뒤로( <u>B</u> ) 마침 취소	

- IIS 관리를 실행합니다. 웹사이트 등록 정보에서 디렉터리 보안>서버인증서를 선택합니다.



- "기존 인증서를 할당 합니다"를 선택합니다.



- 적용할 정보를 선택한 뒤 다음을 선택합니다.



- 정보가 정확한지 확인한 후 다음을 선택합니다.



- 가져오기를 완료합니다.



- 홈페이지에 접속하여 적용 결과를 확인합니다.



### **3.2. Apache** 서버의 경우

- (1) 설정파일의 내용을 확인 하고 해당 경로의 인증서 파일 3개와 개인키 파일 1개를 신 규서버에 업로드 합니다.
- ② 신규 서버에 mod\_ssl설정 여부와 SSL적용 포트 오픈 여부를 확인합니다.
- ③ 환경설정 파일(httpd.conf 또는 ssl.conf)을 수정합니다.
  - 환경설정 파일중 mod\_ssl.so 부분이 있으면 mod\_ssl 사용을 위해 주석을 해제 합니다.

LoadModule ssl\_module modules/mod\_ssl.so

- 기존 http <VirtualHost www.gpki.go.kr:80> 항목을 복사하여 붙여넣고 SSL 관련 4개항목을 추가한 다음 각항목에 맞는 파일의 경로를 입력합니다.

NameVirtualHost *	☜이름 기반 가상호스트 사용		
<virtualhost *:80=""></virtualhost>			
ServerAdmin admin@gpki.go.kr			
DocumentRoot "/home/gpki/www/"	☜홈디렉토리 설정		
ServerName www.gpki.go.kr	☜도메인 설정		
ServerAlias gpki.go.kr			
ErrorLog /home/gpki/error_log			
AccessLog /home/gpki/access_log			
<virtualhost *:443=""></virtualhost>			
ServerAdmin admin@gpki.go.kr			
DocumentRoot "/home/gpki/www/"	☜ 홈디렉토리 설정		
ServerName www.gpki.go.kr	☜ 도메인 설정		
ServerAlias gpki.go.kr			
ErrorLog /home/gpki/ssl_error_log			
AccessLog /home/gpki/ssl_access_log			
SSLCertificateKeyFile " <key filename="">"</key>	🖘 key.pem		
SSLCertificateFile " <pem filename="">"</pem>	🖘 cert.pem		
SSLCertificateChainFile " <cachain.pem>"</cachain.pem>	🕶 caChain.pem		
SSLCACertificateFile " <ca.pem>"</ca.pem>	🔊 ca.pem		

④ config파일의 SSL설정부분을 수정한 후 Aapache서비스를 재구동합니다

### 3.3. WebToB 서버의 경우

① 인증서파일 2개와 Key파일 1개를 추가설치 서버로 업로드 합니다.

② 파일은 .\$WEBTOBDIR/config 이동하여 httpd.m 파일에서 확인합니다.

```
*DOMAIN
webtob1
*NODE
gpki
         WEBTOBDIR="/app/tmax/webtob",
                  SHMKEY = 54000,
                   DOCROOT="/app/tmax/webapps",
                  PORT = "80,443".
                  HTH = 1,
                  LOGGING = "log1",
                   ERRORLOG = "log2",
                  JsvPort = 9900
*VHOST
vgpki
         DOCROOT="/app/tmax/webtob/gpki",
                   PORT = "443",
                   NODENAME = "gpki",
                   HOSTNAME = "www.gpki.go.kr",
                  LOGGING = "log3",
                   ERRORLOG = "log4",
                   SSLFLAG = Y,
                   SSLNAME = "ssl1"
*SVRGROUP
                  NODENAME = "gpki", SVRTYPE = HTML
htmlg
                  NODENAME = "gpki", SVRTYPE = JSV
jsvg
*LOGGING
               Format = "DEFAULT", FileName = "/app/tmax/webtob/log/access.log"
log1
               Format = "ERROR", FileName = "/app/tmax/webtob/log/error.log"
log2
               Format = "DEFAULT", FileName = "/app/tmax/webtob/gpki/log/access_ssl.log"
log3
               Format = "ERROR", FileName = "/app/tmax/webtob/gpki/log/error_ssl.log"
log4
*SSL
ssl1
               CertificateFile
                               = "<pem filename>",
               CertificateKeyFile = "<key filename>",
               CertificateChainFile = "<caChain filename>"
```

③ Config 컴파일

- 수정된 http.m 파일(실제 환경파일)을 컴파일 합니다.
- 예) wscfl i http.m

④ 웹 서버 구동

wsboot 명령어를 사용하여 서버를 구동하고, CSR 생성과정에서 입력했던 개인키 비밀번호 입력 합니다.

⑤ 적용결과를 확인합니다.

# **3.4. iPlanet** 서버의 경우

① server\_root/alias 밑의 database파일을 적용할 서버에 업로드 합니다.

이름 🔺	크기	종류	수정한 날짜
Main the second	64KB	데이터베이스 파일	2009-04-14 오후 2:47
Nttps-mhlee-mhlee-key3.db	16KB	데이터베이스 파일	2009-04-14 오후 2:47
🔊 secmod.db	16KB	데이터베이스 파일	2009-04-13 오전 11:13

- ② 적용할 서버2 에서 csr파일을 생성합니다.
- ③ ②에서 생성한 db파일 2개를 백업 한 뒤 ①에서 업로드 한 파일을 같은 경로에 덮 어쓰기 합니다.
- ④ 매뉴얼의 나. 인증서 설치방법의 ③번부터 진행합니다.
- ⑤ 적용결과를 확인합니다.



# 3.5. Tomcat 서버의 경우

가. 적용된 서버에서 keystore 파일을 적용할 서버로 업로드 합니다.

나. config파일을 수정합니다.(server.xml)

<Connector port="443"
protocol="HTTP/1.1" SSLEnabled="true"
maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
enableLookups="false" disableUploadTimeout="true"
acceptCount="100" debug="0" scheme="https" secure="true"
keystorePass="<password1>" keystoreFile="<keystore filename>"
clientAuth="false" sslProtocol="TLS" />

다. tomcat을 재 구동 합니다.

라. 적용결과를 확인합니다.

## Ⅳ SSL 적용여부 확인방법

### 4.1. 보안서버 구축여부 확인방법

☞ HTTPS로 접속후 브라우저 상단 및 하단을 눌러 "인증서보기"를 클릭합니다.





## 4.2. 보안서버 적용전후 보안통신 비교

☞ HTTP 연결과 비교하면 HTTPS 는 암호화 통신을 함을 알 수 있습니다.
 ☞ 웹사이트 접속후 "마우스 오른쪽 클릭 > 속성" 하면 다음과 같은 자세한 내용을 볼 수 있습니다.



### V 웹페이지 SSL 구현방법

가. 웹사이트 구성에 맞게 웹프로그램 소스를 수정하여 암호화 통신 기능이 정상 동작 되도록 구성합니다.

나. 암호화 통신을 하기 위해서 보안 프로토콜을 호출하는 방법은 OS나 Program 언어를 가리지 않고 모두 동일합니다. 그 이유는 암호화 통신을 하기 위해 적용하는 부분 이 특정 OS나 특정 Program 언어에 의존하지 않는, 모두가 공통으로 사용하는 HTML 언어이기 때문입니다.

다. 보안경고



암호화가 적용된 사이트를 방문해보면, <그림>과 같은 경고창을 만나게 되는 경우가 있습니다. 이 경고창이 뜨는 것은 암호화 통신을 유지하기 위해서는 웹 페이지내의 모든 URL의 호출이 https://로 이루어져야 하나, http:// 즉 평문 통신을 위한 웹페이지 URL이 포함되어 있다는 것을 의미합니다.

이런 경고창이 발생하는 웹페이지 속성을 보면 처럼 '암호화 안됨'이라고 해서 마치 암호화가 되지 않은 평문 상태로 데이터가 전송되어지는 것처럼 생각 되지만 웹페이지간 전송되는 데이터를 볼 수 있는 third-parth 툴을 이용해서 확인해보면, 암호화 통신이 이루어지고 있다는 것을 알 수 있습니다.

경고창이 발생하게 되면, 상세한 내용을 모르고 웹사이트에 접속하는 사용자들 에게 보안이 되고 있지 않다는 불신을 줄 수도 있고, 또한 계속적인 경고창 으로 인해서 불편해 할 수 있으므로 가급적 발생하지 않도록 웹 페이지 내의 모든 URL을 https://로 바꿔주는 것이 좋습니다.

만일 절대경로로 호출하는 것이 아니라, 상대경로로 호출하는 것이라면 소스를 변경하지 않아도 됩니다.

※ 참고 : 절대경로와 상대경로
```
절대경로 호출과 상대경로 호출이란 무엇인가
절대경로란 내가 열어보고자 혹은 내가 가고자 하는 웹페이지의 경로를 전체적으로 기술하
는 것이고, 상대경로란 내가 현재 있는 위치를 기준으로 내가 열어보고자 혹은 내가 가
고자 하는 웹페이지의 경로를 기술하는 것을 말합니다.
아래 그림에서 첫 번째 밑줄 그은 부분이 상대경로로 호출하는 경우이고. 두 번째
밑줄 그은 부분이 절대경로로 호출하는 경우입니다.
첫 번째의 경우에는 https 암호화 통신을 하더라도 소스코드 수정이 필요없는 부분이
고, 두 번째의 경우에는 https 암호화 통신을 할 경우 호출 URL을 http에서 https로 바꿔
줘야 합니다.
만일 바꿔주지 않을 경우에는 보안경고 창이 뜨게 됩니다.
      40911 bytes received by 10.30.100.50:3434 in 19 chunks
                                               🔍 Find 🔈 Export
      90" href=",,/onlinebook/onlinebook,htm" target="_top">
      89" href="http:// .co,kr/zboard/zboard,php?id=lecture" target="_top">
      89" href="http://
                     .co,kr/zboard/zboard,php?id=problem" target="_top">
      89" href="http://_____,co,kr/zboard/zboard,php?id=qna" target="_top">
      89" href="http:// _____,co,kr/zboard/zboard,php?id=down" target="_top">
      3" href="../index.html" target="_top">
       1
                                                          >
```

# 5.1. 전체페이지 암호화하기

가. 링크를 통해 HTTPS 호출하기

```
if ($time3 == $time4) {
echo "
<a href='https://_____.co.kr/zboard/view.php?id=noti
&desc=asc&no=$no' target='_top'><font size=1 color='silve
::new::-></a> ";
} else {
echo "<a href='https://_____.co.kr/zboard/view.php?i
eadnum&desc=asc&no=$no' target='_top'><font size=1 color='
}</pre>
```

https 프로토콜을 호출하여 웹페이지 전체에 적용하는 방법은 그림만으로도 곧바로 이해를 할 수 있을 정도로 아주 쉽습니다. 간단히 호출하는 프로토콜을 http://에서 https://로 수정해 주기만 하면 됩니다.

- 나. 리다이렉션(Redirection) 설정으로 HTTPS 호출하기
  - 1) 웹서버에서 리다이렉션 하기

<virtu< th=""><th>ualHost test.co.kr:80&gt;</th></virtu<>	ualHost test.co.kr:80>
	ServerAdmin zmnkh@test.co.kr
	ServerName test.co.kr
	ServerAlias www.test.co.kr
	DocumentRoot /home/manpage
	CustomLog logs/test.co.kr-access log common
	Redirect / https://www.test.co.kr/
<td>tualHost&gt;</td>	tualHost>

앞서 설명을 하였듯이, 암호화 통신을 위해서는 https 프로토콜을 직접 호출을 해줘야합니다. 하지만, 웹페이지에 접속하는 사용자들은 일일이 https 프로토 콜을 붙여서 입력을 하지 않습니다. 대부분의 경우가 www.test.co.kr 또는 test.co.kr 도메인을 웹 브라우저의 주소창에 입력하고 접속하는 경우가 대부 분일 것입니다. 이 때 웹 브라우저에 그냥 도메인 주소만 입력하면, 웹 브라우 저는 해당 도메인 앞에 http://가 붙은 것으로 판단하고 평문통신을 하도록 합 니다.

평문 통신을 하는 경우라면 문제가 없지만, 암호화 통신을 해야 할 경우에는 https://를 직접 붙여서 입력해야 하므로 여간 불편해 하지 않습니다. 리다이렉션 은 현재 접속한 도메인이나 혹은 웹페이지를 강제로 다른 주소나 다른 페이지로 변경해 줌으로써 사용자들의 불편함을 감소시켜주고 자연스럽게 암호화통신을 할 수 있도록 해주는 기능입니다.

2) meta tag로 리다이렉션하기

```
<meta http-equiv='refresh' content='0; url=<u>https://____.co.kr/index.html</u>' target='_top'>
```

또 다른 방법으로는 O/S나 Web Programming 언어의 종류에 상관없이 모두 공통적으로 사용하는 HTML tag를 이용한 방법으로써, 어떤 경우에서나 적용 이 가능하기 때문에 가장 많이 이용되고 있습니다.

3) java script로 리다이렉션하기

```
<script>
var url = "https://www.test.com";
window.location.replace(url);
</script>
```

위와 같이 Meta 태그를 이용하는 경우, 1초 정도 깜빡하는 현상이 나타나기 때 문에 종종Javascript를 이용하기도 합니다.

Meta tag를 이용한 html Redirection 방법과 동일하게, 사용자들이 익숙하게 접속 하는 http://www.test.com의 index 페이지에 삽입해 두면, 사용자들이 불편하 게 https://라는 프로토콜을 특별히 지정해 주지 않아도, 보안을 위해서 암호화 통신이 적용된 https://www.test.com 으로 리다이렉션해주게 됩니다.

# 5.2. 페이지별 암호화하기

페이지별 암호화는 현재 위치하고 있는 페이지에서 다른 페이지로 이동할 때, 보안을 위해서 암호화된 전송을 할 것인지 아니면 평문 전송할 것인지를 선택 하여 암호화하는 것을 말합니다.

부분적인 페이지 암호화를 사용하는 이유는 암호화 적용이 필요없는 부분까지 암호화를 하여 서버의 부하를 증가시키는 것을 최대한 줄일 수 있기 때문입니다.

나. 다음은 사이트의 메뉴 부분 예입니다. 이중 '서버관련 강좌 & TIP' 메뉴를 클릭 하여 이동을 하면 https가 호출되어 서버와 클라이언트간의 통신이 암호화되어 전송되고,'Q&A' 메뉴를 클릭하여 이동하면 http가 호출되어 서버와 클라이언트 간의 통신이 평문으로 이루어지게 할 수 있습니다.

온라인북 | 서버관련 강좌 & TIP | 문제 해결 | Q&A | 다운로드

<map name="ImageMap1"></map>
<pre><area coords="193, 74, 249, 90" href="onlinebook/online.ht&lt;/pre&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;m" shape="rect" target="main"/></pre>
<pre><area coords="267, 75, 401, 89" href="&lt;u&gt;https://co.k&lt;/u&gt;&lt;/pre&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;r/zboard/zboard.php?id=lecture" shape="rect" target="_top"/></pre>
<pre><area coords="423, 73, 479, 89" href="https://co.k&lt;/pre&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;r/zboard/zboard.php?id=problem" shape="rect" target="_top"/></pre>
Karea shape="rect" coords="497, 73, 537, 89" href="http://co.kr
/zboard/zboard.php?id=qna" target="_top">
<pre><area coords="555, 73, 609, 89" href="http://co.kr&lt;/pre&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;/zboard/zboard.php?id=down" shape="rect" target="_top"/></pre>
<pre>Karea shape="rect" coords="679, 5, 717, 23" href="index.html" target="_</pre>
top">

# 5.3. 프레임별 암호화하기

가. SSL을 이용한 보안포트(443)를 웹페이지에 적용하는 방법을 앞서 소개하였 습니다. 단순히 http를 https로만 바꾸어주면 보안포트(prot)를 이용해서 암호화 통신을 할 수 있습니다. 하지만, 프레임이 삽입된 웹페이지의 경우에는 약간 적용하는 방식이 다르기 때문에 소개하고자 합니다. 프레임이 적용된 페이지를 이용하면 '암호화된 페이지'와 '비 암호화된 페이지'를 각각 적용시킬 수 있습니다.

아래 그림과 같이 웹페이지에 프레임으로 세 개의 페이지top.htm과 left.htm과 main.htm을 불러오는 소스코드가 있을 때 소스코드의 URL을 아래처럼 변경 하고 웹 브라우저에서 http와 https로 각각 호출했을 때의 결과를 살펴보고자

### 합니다.

이와 같이 프레임을 이용하면, 필요에 따라서 한 페이지에서 암호화가 제공되는 부분과 암호화가 제공되지 않는 부분이 공존할 수 있도록 구성할 수 있지만, 앞서서도 이미 언급했듯이 아무리 웹 브라우저에서 https를 이용해서 호출을 했어도 프레임으로 불러오는 페이지가 http 주소를 가지고 있을 경우에는 암호화가 되지 않고 정보의 노출이 발생할 수 있으므로, 프레임이 사용되는 페이지를 암호화를 위해서 https로 호출하고자 할 때에는 꼭 확인을 해보시기 바랍니다.

[주소(D) <u> http://lab.</u>	.co.kr	🗸 🏹 이용
	Frame 1: top HTTP	
Frame 2 : left HTTP	Frame 3 : main HTTPS	

```
<HEAD>
```

```
<TITLE>프레임 예제</TITLE>
</HEAD>
<FRAMESET rows="100, *">
<FRAMESET rows="100, *">
<FRAMESET cols="120, *">
<FRAME name="topFrame" src="top.htm">
<FRAMESET cols="120, *">
<FRAMESET cols="120, *">
<FRAMESET cols="left.htm">
</FRAMESET cols="left.htm"</p>
```

# VI 보안서버 구축 시 유의사항

- 보안서버 접속포트에 대해 침입 차단시스템 등 보안장비에서 허용 정책이 필요합니다.
   말반적으로 웹서비스는 TCP 80포트를 사용하지만, 보안서버는 TCP 443 포트를 사용하므로 이 포트에 대해서 보안장비에서 허용할 수 있도록 해야 합니다.
   단, 하나의 시스템에서 여러 웹서버가 운영 시 TCP 443 포트 이외에 여러 포트가 사용되므로 사용포트에 대한 허용정책이 추가로 필요합니다.
- 2. 웹방화벽 및 웹컨텐츠 필터링시스템이 있는 경우에는 암호화된 컨텐츠가 평문으 로 복호화 되어 필터링 될 수 있도록 보안장비에서 설정 해주어야 합니다.
  - 보안서버는 사용자 웹 브라우저와 웹서버 간에 통신이 암호화됩니다. 이때 웹방화벽이나 개인정보필터링 시스템도 암호화된 컨텐츠에 대해서 필터링하지 못하는 문제가 발생하므로, 이를 위하여 인증서에서 개인키를 추출하여 웹방화벽 및 개인정보필터링 시스템에 탑재함으로써 컨텐츠를 복호화 하여 필터링 할 수 있도록 해주어야 합니다.
- 3. 사용자가 HTTP로 접속시 HTTPS로 리다이렉션 할 수 있도록 해야 합니다.
  - ☞ 보안서버는 HTTPS 프로토콜을 사용하므로 사용자들이 주소창에 "https://도 메인 주소"로 입력을 해야만 개인정보가 암호화된 통신이 이용됩니다. 하지만, 사용자들이 https://로 입력하기가 어려우므로 "http://도메인 주소" → "https://도메인주소"로 리다이렉션 할 수 있도록 설정해 주어야 합니다.

# VII 보안서버 FAQ

# 7.1. 제도 관련 FAQ

### 가. 행정전자서명센터(GPKI)은 어떤 기관인가요?

- · 행정안전부 산하기관 한국지역정보개발원(KLID)의 소속기관으로 「행정전자서명 인증서」발급업무를 맡고 있습니다.
  - 한국지역정보 개발원 : www.klid.or.kr
  - 행정전자서명센터 : www.gpki.go.kr

### 나. 보안서버는 무엇이고, 구축하지 않으면 어떻게 되나요?

 보안서버란, 인터넷상에서 개인정보를 암호화하여 송수신하는 기능이 구축된 웹사이트를 말하며, 하드웨어를 설치하는 것이 아니라 이미 사용하고 있는 웹서버 에 인증서나 암호화 소프트웨어를 설치하여 암호통신이 가능한 것입니다.
 「개인정보보호법」[제73조]벌칙 다음 각호의 어느 하나에 해당 하는 자는 2년 이하의 징역 또는 1천만원 이하의 벌금에 처한다.

### 다. 보안서버는 구축의 의무인가요? 관련 법조항이 뭔가요?

☞ 「개인정보보호법」제24조[고유식별 정보의 처리 제한]

③항 개인정보처리자가 제1항 각 호에 따라 고유식별정보를 처리하는 경우에는 그 고유식별 정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 대통령령으로 정하는 바에 따라 암호화 등 안전성 확보에 필요한 조치를 하여야 한다.

### ☞ 「개인정보보호법」제29조[안전조치의무]

개인정보처리자는 개인정보가 분실·도난·유출·변조 또는 훼손되지 아니 하도록 내부 관리계획 수립·접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다.

「개인정보보호법」제73조[벌칙]
 다음 각호의 어느 하나에 해당 하는 자는 2년 이하의 징역 또는 1천만원 이하
 의 벌금에 처한다.

제24조 제3항, 제25조 제6항 또는 제29조를 위반하여 안전성 확보에 필요한 조치를 하지 아니하여 개인정보를 분실·도난·유출·변조 또는 훼손당한 자.

# 붙임 1 SSL인증서 발급 절차

(1)인증관리센터 홈페이지(www.gpki.go.kr)에서 [인증서 발급]을 선택합니다.

기관 또는 개인을 구분하시고 인증서 발급을 위해 행정전자서명 신청서를 제출하신 기 입력해 주십시오.		
-		
구분	○ 개인용 ● 기관용 * 선택시 예시를 참고해 주세요.	
기관명	검색	
-0		

(2)기관명을 검색합니다.

행정안전부	▶ 찾
기관명을 입력해 주세요.	Nation 201
예) '행정만전부 정보보호정책로 '해저마저브' 인터 서태	F. 이면
예) '서울특별시 종로구 보건소'	이면
'서울특별시' 입력, 선택	
※ 해당부서를 클릭하시면 자	동으로 입력됩니다.
The state	1

(3)부서명, CN(도메인), 이름을 입력 후 [확인]을 누릅니다.

(5)서버에서 생성한 CSR파일(인증서요청파일)을 에디터로 오픈시킵니다. (확장자가 이상해도 에디터로 드래그 앤 드롭하면 오픈됩니다.)

2	기관용 인증서 발급을 수행합니다. 내용을 확인 하시고 인증서 발급 버튼을 눌러 주십시오.
_	
구분	기관용
기관명	행정안전부
휴대폰	49132901
이메일	ssl@klid.or.kr
임시비밀번호 수신방법	수신방법 선택 후 전송 버튼을 클릭하시면 임시비밀번호가 발송됩니다. ○ 휴대폰 ○ 이메일 ▶ 전송
민증서 발급 요청	양식(PEM타입 : PKCS#10)
임시비밀번호 입력:	
저조되 아지마만버	호 입력 후 인증서 발급 버튼을 클릭하세요.

# (시)이러저머르 하이하니다

8	인증서 발급(기관) 인증서 발급을 위해 아래항목을 입력해 주십시오.
신청서에 기재한	상세부서까지 입력하셔야 합니다.(예 : 행정안전부 정보화전략실 정보기반정책관 정보보호정책과)
구분	⊙ 전자관인용 ○ 특수목적용(대표메일) ○ 특수목적용(차량) ○ 서버용 ○ SSL용
기관명	행정안전부
부서명	행성안전부 검색 하위무서까지 입력
부서명 CN	행성만전부 검색 하위부서까지 입력 www.tmxmfnptm.com

🝺 certreq_2048,txt - 메모장	
파일(F) 편집(E) 서식(Q) 보기(Y) 도움말(H)	
In Bird Pearl Araco series and se	A
 (6)에디터로 오픈된 CSR파일의 내용물을 복사해서 아래 화면과 같이 붙여 넣고	1

# 임시 비밀번호를 입력한 다음, [인증서 발급]을 클릭합니다.

	내용을 확인 하시고 인증서 발급 버튼을 눌러 주십시오.	
구분	기관용	
기관명	행정안전부	
휴대폰	49132901	
이메일	ssl@klid.or.kr	
임시비밀번호       수신방법 선택 후 전송 버튼을 클릭하시면 임시비밀번호가 발송됩니다.         수신방법       ○ 휴대폰 ○ 이메일 > 전송		
인증서 발급 요청 JcWeQBzkkR4YtEd XakgwNsLOrJhLEd txvNUGGwbyKI+xy 36qloOdM18D1bV END NEW CE	양식(PEM타입 : PKCS#10) SGCTAYJRA+4jim7qivUW6GoAG3Xq1jBUBgn87awQq2XxizdtOO ▲ orDn/3u3cTYSy/HYasg3jccACq5zkwh9Gx8AjPr9fqmm5M₩l1s /laM+Kt8tsnD+k62CFuYG2asTeYqx+tkJ1tTX2eTyNnmPlQnPv 3VDuijiSA= ERTIFICATE REQUEST ▼	
임시비밀번호 입력: 저조되 인지비밀버?	abcdefg 회압력 후 인증서 발급 버튼을 클릭하세요.	

(7)정상적으로 처리되면 아래의 페이지로 이동이 되고, 파일명을 클릭하면 저장하실 수 있습니다.

※취소를 클릭하면 공문과 신청서를 다시보내셔야 합니다.

	파일 다운로드	×
	이 파일을 열거나 저장하시겠습니까?	
	이름: www.tmxmfnptm.com,p7b 유형: PKCS #7 인증서 시작: admin.gpki.go.kr	
	열기( <u>0</u> ) 저장( <u>S</u> ) 취소	
정상처리되었습니다	일부 파일은 사용자의 컴퓨터에 피해를 줄 수 있습니다. 파일 정보가 의심스럽게나 원본을 신뢰할 수 없으면 이 파일을 열거나 저장하지 마 십시오. 위험성	
💾 www.tmxmfnptm	.com.p7b	

# 붙임 2 보안서버 구축 후 오류발생 시 참고사항

(1) 인증서를 발급 받은 웹 사이트 주소와 실제로 접속한 웹 사이트 주소가 다른 경우



(2) 인증서(SSL인증서)가 유효하지 않은 경우



(3) 웹 브라우저가 웹 서버 인증서를 신뢰할 수 없는 경우



(4) 보안된 항목 https와 보안되지 않은 항목 http를 모두 포함하는 경우



(5) 한 웹 페이지에 http://와 https://의 두 프로토콜이 존재하는 경우



한 웹 페이지 안에 http://와 https://의 두 프로토콜이 존재하기 때문입니다. 예를 들어, http://www.gpki.go.kr에서 로그인을 위해 https://www.gpki.go.kr/login.jsp로 접속할 때 /login.jsp 안에 http://www.gpki.go.kr로 호출하는 직접적인 소스가 있기 때문입니다.

이러한 경우 HTML 파일 중에 HTML 헤더 부분에 다음의 스크립트를 넣어주시면 됩니다.

<META HITP-EQUIV="REFRESH" CONTENT="0; URL=http://(해당 URL)">

이 스크립트는 https 페이지에서 로그인한 후, https로 암호화되는 임의의 페이지를 하나 만들 어 이동을 하되 그 페이지에서 메타태그를 이용하여 원하는 http 페이지로 리프레쉬하게 만드 는 것입니다.

보통의 CGI 프로그래밍에서의 리다이렉션 함수(메소드)나 또는, HTTP Location 헤더를 직접 가지고 보안되지 않은 곳으로 리다이렉션하면 보안되지 않은 곳으로 간다고 경고가 나오지만, HTTPS 서버의 HTML을 읽게 한 후 그 HTML 내에서 META 태그를 이용해서 리다이렉션 하게 되면, 웹 브라우저는 일단 그 HTML이 HTTPS 서버에서 읽은 것으로 간주하고 보안 경고가 뜨지 않으며 HTML의 META 태그로 리다이렉션 하는 경우에는 웹 브라우저가 리다 이렉션한 것처럼 동작되게 되어 경고가 뜨지 않습니다. (6) https://로 접속했을 때 "페이지를 표시할 수 없다"는 메시지가 나타낼 경우

# << 발생 원인 >> 1 https 디렉토리 내에 파일이 존재하지 않을 경우 2 서버와 사용자간의 방화벽에서 443 포트가 차단되었을 경우 3 https 서버가 다운되었을 경우 4 SSL인증서 파일이 정상적이지 않을 경우 5 웹 브라우저에서 ssl 3.0으로 세팅이 되어 있지 않을 경우

위의 경우에는 인증서가 정상적으로 설치되었는지, 서버에서 https를 위한 포트가 활성화 되었는지 확인하시기 바랍니다.(방화벽과 L4 스위치 등 장비가 있다면 https를 위한 해당 포트가 모 두 허용되었는지 확인합니다.) 윈도우즈의 경우 'netstat -na | findstr 포트번호', 유닉스 의 경우 'netstat -na | grep 포트번호' 명령어를 이용하여 https를 위한 포트가 활성화되어 있는지 확인할 수 있습니다. 위의 모든 내용을 확인한 후에도 정상적으로 동작하지 않을 경우 해당 설치 업체에게 문의하시기 바랍니다.

⑥ Windows XP sp2 이하일 경우
2048 key size로 발급된 SSL 인증서의 경우 반영된 SHA-2 암호 알고리즘을 지원하지
않아 발생되는 문제로 사용자의 OS를 Windows XP sp3로 업데이트해야 해결됩니다.

### [Windows Update 사이트] http://update.microsoft.com

### [서비스 팩 다운로드센터]

http://windows.microsoft.com/ko-KR/windows/service-packs-download#sptabs=xp

※ 보안 취약성 문제로 행정안전부에서 SHA-2 암호 알고리즘을 SSL 인증서에 사용하도록 권고하고 있습니다. (7) Windows XP Sevice Pack 1 이하의 운영체제(OS)를 사용하는 경우

행정전자서명 인증서가 인터넷 익스플로러(IE) 브라우저의 신뢰된 루트 인증기관으로 등록되어 Windows XP SP2 버전 이상부터 IE브라우저에 적용되었습니다. Windows XP SP2 버전 이 상부터 신뢰된 기관에서 발급받은 인증서로 인식되기 때문에 보안경고창 등의 문제점이 없 이 사용 가능합니다. 그러므로 Windows XP Service Pack 1의 운영체제를 사용하는 경우 윈 도우 업데이트를 통한 루트 인증서를 꼭 업데이트하여야 합니다.

### << 루트 인증서 업데이트 방법 >>

① 윈도우 "시작" 버튼 클릭 → "Windows Update" 실행 → "사용자 지정 설치" 버튼 클
 릭 → "다른 업데이트 검토" 버튼 클릭 → "소프트웨어, 선택적" 링크 클릭 → "루트
 인증서 업데이트" 선택 후, "업데이트 검토 및 설치" 버튼을 클릭하여 선택적으로 루트
 인증서만 업데이트를 실시할 수 있습니다.

- 17 X

일(E) 편집( <u>E</u> ) 보기(⊻) [	즐겨찾기(A) 도구(I) 도움말(H)		
🔅 🍕 Microsoft Update		🟠 • 🗟 - 🖶 • 🔝 ዝባ지(P)	• 🌀 도구( <u>0</u> ) •
		빠른 연결   대한민국 홈페이지   전시	171
licrosoft		Microsoft.com에서 검색:	검색
icrosoft Update			
licrosoft Update	선택적 소프트웨어 업데이트 선택 이 업데이트는 컴퓨터의 보안 또는 성능에 중요한 업데이트는 아니지만 일부 기능, 프로그램 또는 장치의	1 성능을 향상시킬 수 있습니다. 컴퓨터 보호를 위해 중요 업데이트를 모두	설치하십시오.
업데이트 설치 (26)	👌 업데이트 검토 및 설치	총: 26 업데이트 , 11	80,7 MB , 5 분
<b>동류별 선택</b> 중요 업데이트 (25) ~프트웨어 서태제	선택적 소프트웨어 업데이트 모두 지우가 모두 선택		
11)	Microsoft Windows XP		
하드웨어, 선택적 (1)	□		
<b>1품별 선택</b> Windows XP (21) Office (14) Silverlight (1)	▶ 후든 인증사 업데이트 다운로드 코가: 295 KB , 필요 시간 1 분 이 업데이트는 Microsoft Root Certificate Program의 일환으로 컴퓨터에 있는 후트 인증시 시물 추가하면 Intermet Explorer 개에서 EV(작용 유호성 경시) 인증시물 사용하고 보인이 강 로 코드를 전탈할 수 있습니다. 이 업데이트를 설치한 후 컴퓨터를 다시 시작해야 할 수 있습니다 때 이 업데이트를 다시 표시 안 함	목록을 Microsoft에서 하용하는 최신 목록으로 업데이트합니다. 컴퓨터에 화된 웹 감색의 범위를 늘릴 수 있으며 친자 메일을 양호화하고 보안이 강경 L. 이 업데이트는 한번 설치하면 제거할 수 없습니다. <u>자세한 정보</u> .	루트 인증 화된 방식으
GQL Server (0)	□ 표 Microsoft .NET Framework 2.0 서비스 팩 1(KB110806) x86 안머 팩		
옵션	🗆 🗉 Windows Media Player 11		
업데이트 내역 검토	□      Microsoft .NET Framework 3.0: x86(KB928416)		
숨겨진 업데이트 복원 역정 배경	□		
일은 건요 일문과 대답			
도움말 및 지원 보기	- I Microsoft 기본 스마트 카드 암호화 서비스 공급자 패키지: x86(KB909520)		
NDITLEALIE amaat lladata 개인 정보 보기	A 14		
2008 Microsoft Corporation, A	는 요구 NI rights reserved, <u>사용약관</u>   <u>상표</u>   <u>개인정보보호</u>   <u>법적정보</u>		
			100% •
) 또는, W	'indows XP Service Pack 2의 운영	체제로 업데이트를 통힌	: 루트
,			

### << 발생 원인 >>

아파치의 경우 개인키 생성 뒤 csr 파일을 생성하나, 나머지 4종류의 웹서버 경우 csr생성 시 개 인키가 생성된다. 인증서의 경우 개인키와 공개키가 쌍으로 존재하므로, 아파치를 제외한 나 머지 서버의 경우 인증서 발급 후 csr파일을 재생성 했다면, 인증서를 재발급 해야 하므로, csr 파일 생성은 한번만 하도록 유의 한다.

# <제·개정 연 혁>

버전	제·개정일	재·개정내역
v1.00	2008년 6월	•"보안서버 구축 가이드"으로 제정
v2.00	2009년 1월	· WebtoB, iPlanet 구축절차 반영 · 보안서버 구축 후, 오류발생시 참조사항 반영
v2.50	2009년 8월	· 보안서버 구축 시 유의사항 정리 반영 · 개인키 추출절차 반영
v3.0	2010년 6월	·웹서버 프로그램 대상(5종 → 7종 : Apache 2.0, IIS 7.0 추가) 확대 · 이중화 구성된 웹서버에서 보안서버 적용절차 해설 · 보안서버 구축 시 발생하는 오류코드 및 장애에 대한 해결 방법
v4.0	2011년 8월	·보안서버 설치 파일 설명 · consol mode 사용시 입력 예문 추가
v5.0	2012년 3월	·키 길이 고도화(1024 →2048)에 따른 내용 수정 · iPlanet, Tomcat 구축절차 수정
v5.1	2012년 11월	· Windows sp2 이하 OS에서 2048 SSL 인증서 문제발생 및 해결책 추가