보안서버 구축 가이드

(version 1.2)

한국무역정보통신

http://ssl.tradesign.net

한국무역정보통신은 전자서명법에 의거 정부가 지정한 공인인증기관이며 또한 보안서버전문가협의회 회원사로서 고객님들의 보안서버 인증서 신청 및 설치에 도움을 드리고자 이 문서를 제공해 드립니다.

목 차

제 1 장 보안서버 개요

1. 보안서버 개요 3

2. 보안서버 구축 절차 6

3. 보안서버 관련 법제도 현황 7

제 2 장 웹서버별 보안서버 인증서 발급 및 설치 방법

4. Apache Mod_SSL / OpenSSL 10

5 Microsoft IIS 4.x / 5.x / 6.x 18

6. BEA Weblogic 25

7. IBM WebSphere 29

8. Java Based Web Servers 33

9. iPlanet Web Server 36

10. WebtoB 40

11. Tomcat 44

제 3 장 보안서버 구축의 마무리 - 웹페이지 수정

12. 웹사이트 전체에 보안서버 적용하기 46

13. 웹사이트 일부에 보안서버 적용하기 49

첨부 : 보안서버 인증서 신청양식, 보안서버 구축공문(정통부, 정보보호진흥원) 53

제 1 장 보안서버 개요

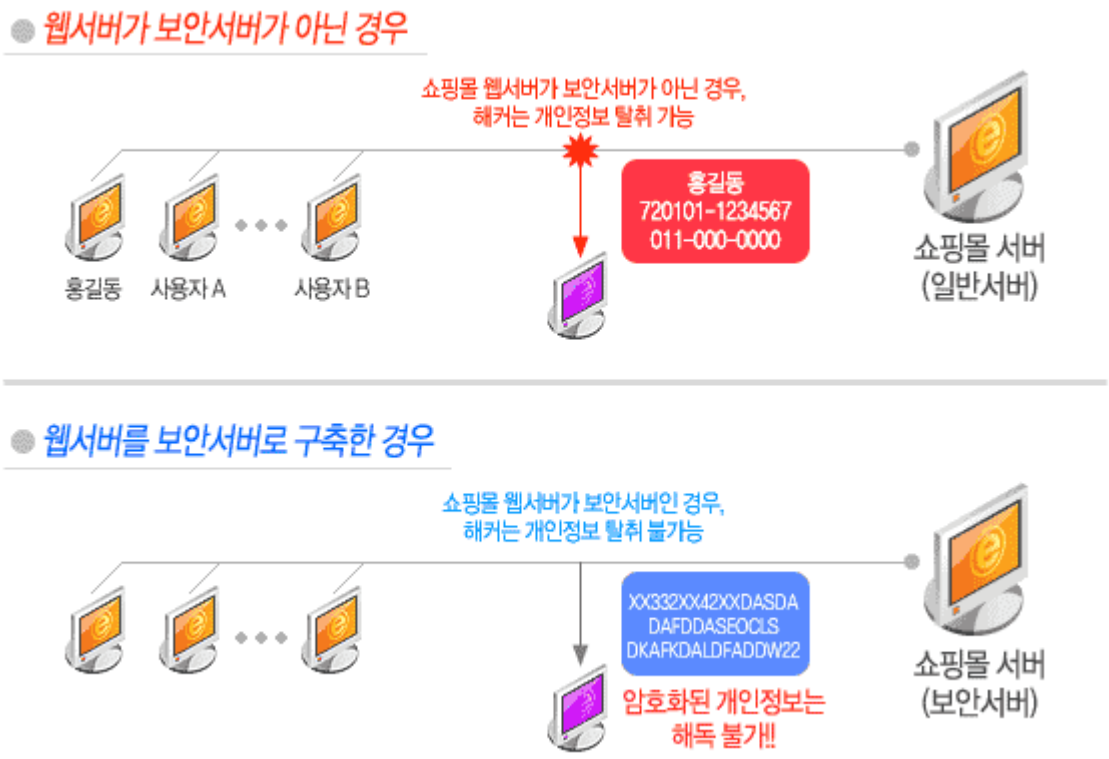
1. 보안서버 개요

1) 보안서버의 정의

보안서버란 인터넷상에서 사용자 PC와 웹서버 사이에 송수신되는 개인정보를 암호화하여 전송하는 서버를 의미합니다. 또한 보안서버는 해당 전자거래 업체의 실존을 증명하여 고객과 웹 서버간의 신뢰를 형성하고, 웹 브라우저와 웹 서버간에 전송되는 데이터의 암/복호화를 통하여 보안 채널을 형성하므로 안전한 전자거래를 보장합니다.

개인정보를 송/수신 하는 대표적인 예로는 회원 가입시 주민번호 입력, 로그인시 ID/패스워드 입력, 인터넷 뱅킹 이용시 계좌 번호/계좌 비밀번호 입력 등이 해당됩니다.

인터넷 상에서 암호화되지 않은 개인정보는 가로채기 등의 해킹을 통해 해커에게 쉽게 노출될 수 있으므로, 웹 서버에 보안서버 솔루션을 설치하면 해커가 중간에 데이터를 가로채도 암호화 되어 있어 개인정보가 노출되지 않습니다.

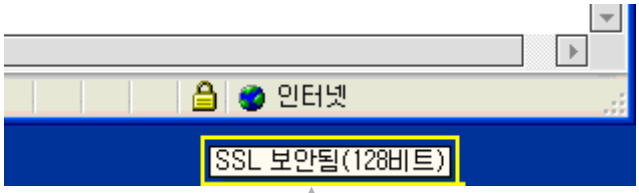


2) 보안서버가 구축된 웹사이트 확인

기본적으로 보안서버 웹사이트 주소는 http가 아닌 https 로 시작한다.
예) https://www.dcp.co.kr
아울러 보안서버 내용을 확인하려면 아래를 참고한다.

가. 웹브라우저 우측 하단에 자물쇠 모양 확인

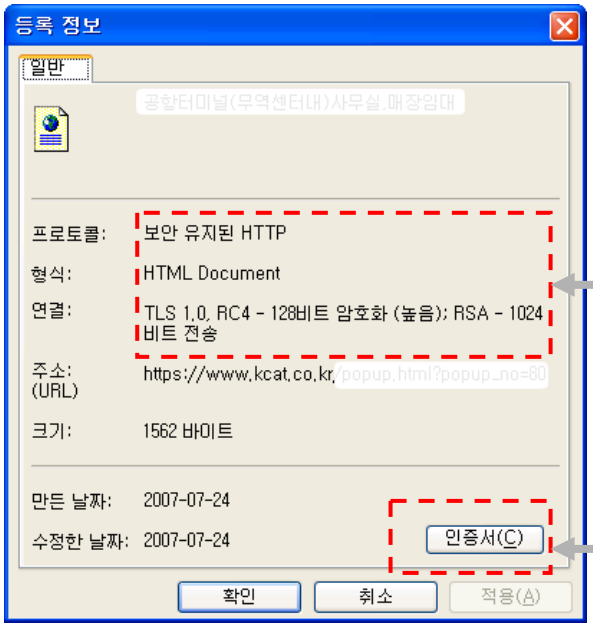
웹 브라우저 하단에 자물쇠 모양의 표시가 나타납니다. 단, 웹사이트 구성 방법에 따라서 자물쇠 이미지가 보이지 않을 수 있으며 구축방법에 따라서 모양도 다르게 나타날 수 있습니다.



브라우저 하단에 있는 자물쇠 아이콘을 마우스로 올리면 암호화 방식에 대한 확인이 가능

나. 웹페이지 속성 보기를 통한 확인

마우스의 오른쪽을 클릭하고 속성 탭을 선택한 후 웹페이지 등록정보를 통하여 확인



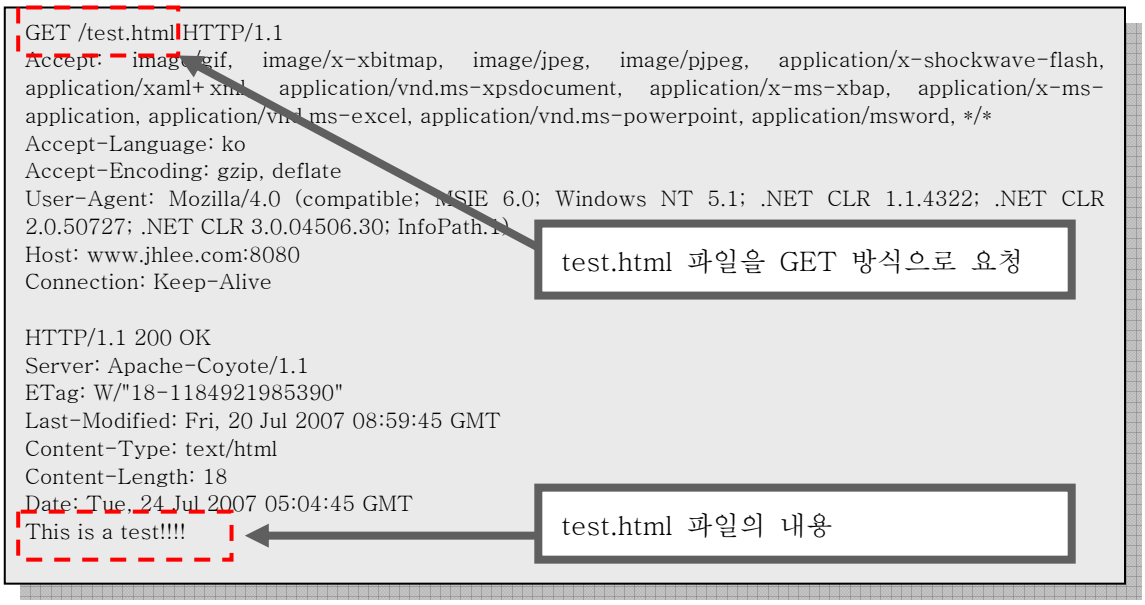
암호화 내용확인

보안서버 인증서 내용보기
☞ 웹사이트를 인증한 인증기관과 사이트의 내용을 확인할 수 있다.

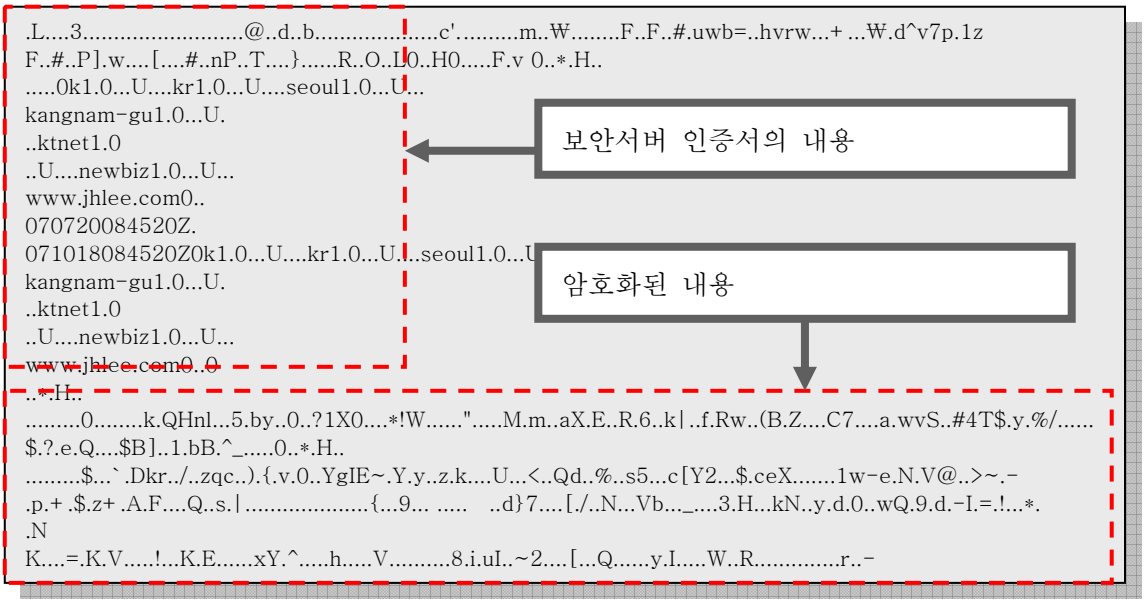
다. 패킷캡쳐 프로그램을 통한 확인

HTTP 패킷을 캡쳐하여 보안서버가 구축되기 이전과 비교를 해보면 암호화 여부를 구체적으로 확인할 수 있다.

< 암호화 하기 이전의 패킷 내용보기 (패킷캡쳐 프로그램 이더리얼 사용) >



< 암호화한 이후의 패킷 내용보기 (패킷캡쳐 프로그램 이더리얼 사용) >



2. 보안서버 구축 절차

단계 1) 서버의 종류확인

☞ 웹서버의 종류(IIS, 아파치, 아이플래닛, 웹로직, 탐캣, 제우스 등)와 버전을 확인합니다. 웹서버와 웹어플리케이션 서버가 연동되어 있는 경우, 웹서버의 종류를 확인합니다.

단계 2) 각 서버에 맞는 설치 진행

☞ 웹서버의 종류와 버전에 따라 개인키 및 CSR을 생성하기 위한 추가 모듈이 설치되어야 하는 경우가 있습니다. 자세한 내용은 본문을 참고하십시오.

단계 3) 개인키 및 CSR(인증서 요청정보) 생성

☞ "단계 2" 가 성공적으로 완료되면 개인키와 CSR(인증서요청정보)를 생성합니다. 이 두 개의 정보는 항상 쌍으로 존재하며 약 2K~3K Bytes 내외 크기의 파일입니다. CSR을 생성할 때에 웹서버의 신원 정보를 입력하는데 자세한 내용은 본문을 참고하십시오.

단계 4) 인증기관에 CSR 제출 및 인증서 발급신청 및 요금결제

☞ CSR(인증서요청정보) 를 인증기관에 제출(**http://ssl.tradesign.net** 에 신청) 및 신청정보를 입력합니다. 또한 요금을 결제합니다.

단계 5) 신청서 검토, 인증서 발급

☞ 인증기관은 신청서 내용의 무결성 및 신청인의 신원을 확인하고 인증서를 발급합니다. (인증서는 email 첨부 형태로 제공됩니다.)

단계 6) 인증서를 설치합니다.

☞ 인증서를 설치하고 새로운 웹사이트 인스턴스를 실행합니다.
(https://www.domain.com) 의 방법으로 접속. 자세한 내용은 본문을 참고하십시오

단계 7) 경우에 따라 웹페이지 링크 또는 소스를 수정합니다.

☞ “단계 6” 까지 완료하시면 보안서버를 운영하는데 무리가 없지만 플래쉬 등이 적용된 웹페이지에서 “보안되지 않은 링크가 포함되어 있습니다”의 경고창이 뜰 수 있습니다. 보다 완벽한 보안 웹사이트의 완성을 위해 최소한의 소스 수정은 불가피 합니다. 자세한 내용은 본문을 참고하십시오.

3. 보안서버 관련 법제도 현황

1. 정보통신망이용촉진및정보보호등에관한법률

▶ 제28조(개인정보의 보호조치) 정보통신서비스제공자등은 이용자의 개인정보를 취급함에 있어서 개인정보가 분실·도난·누출·변조 또는 훼손되지 아니하도록 정보통신부령이 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 조치를 하여야 한다. <개정 2004.1.29>

▶ 제55조 (자료제출 등) ④정보통신부장관은 이 법에 위반한 정보통신서비스제공자등에 대하여 필요한 시정조치를 명할 수 있다. <개정 2005.12.30>

▶ 제67조 (과태료) ②다음 각 호의 어느 하나에 해당하는 자는 1천만원 이하의 과태료에 처한다. <개정 2005.12.30>

8의2. 제28조의 규정을 위반하여 기술적·관리적 조치를 하지 아니한 자

2. 정보통신망이용촉진및정보보호등에관한법률 시행규칙

▶ 제3조의2(개인정보의 보호조치) ①법 제28조의 규정에 의한 개인정보의 안전성 확보에 필요한 기술적·관리적 조치는 다음 각호와 같다.

1. 개인정보의 안전한 취급을 위한 내부관리계획의 수립 및 시행
2. 개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단시스템 등 접근통제장치의 설치·운영
3. 접속기록의 위조·변조 방지를 위한 조치
4. 개인정보를 안전하게 저장·전송할 수 있는 암호화기술 등을 이용한 보안조치
5. 백신소프트웨어의 설치·운영 등 컴퓨터바이러스 방지 조치
6. 그 밖에 개인정보의 안전성 확보를 위하여 필요한 보호조치

②정보통신부장관은 제1항 각호의 규정에 의한 보호조치의 구체적인 기준을 정하여 고시하여야 한다. [본조신설 2004.7.30]

3. 개인정보의 기술적·관리적 보호조치 기준

▶ 제5조(개인정보의 암호화) ②정보통신서비스제공자등은 정보통신망을 통해 이용자의 개인정보 및 인증정보를 송수신할 때에는 보안서버 구축 등의 조치를 통해 이를 암호화해야 한다. 보안서버는 다음 각 호의 어느 하나의 기능을 갖추어야 한다.

1. 웹서버에 SSL(Secure Socket Layer) 인증서를 설치하여 개인정보를 암호화하여 송수신하는 기능
2. 웹서버에 암호화 응용프로그램을 설치하여 개인정보를 암호화하여 송수신하는 기능

제 2 장 웹서버별 인증서 발급 및 설치

웹서버용 SSL 인증서란?

SSL인증서란 웹서버용 인증서, 서버용 인증서라고도 하며, 일반 사용자가 웹 사이트에 접속해서 주고 받는 모든 정보를 암호화해 주는 SSL(Secure Socket Layer) 통신에 사용되는 인증서입니다.

웹서버용 SSL 인증서가 설치되어 있는 사이트는 "http://" 가 아닌 "https://"로 시작되며, 브라우저 하단에 노란 자물쇠 표시가 나타납니다. 이 노란 자물쇠를 더블클릭 해보면 어떤 인증서가 설치되어 있는지 암호화 수준은 어떻게 되어 있는지 확인하실 수 있습니다.

SSL 적용을 위해서는 http://의 기본 80 포트뿐만 아니라, https://의 기본 443 포트도 사용합니다. (설정에 따라 포트 번호는 달라질 수 있음.) 따라서, 해당 포트의 방화벽과 같은 네트워크 설정을 미리 변경하여 주시기 바랍니다.

웹서버용 SSL 인증서 발급 절차

1. 웹서버용 SSL 인증서 신청을 위한 담당자와 연락을 합니다. 이 때 사용하실 웹서버용 인증서의 용도, 웹서버의 종류 등의 정보를 알려 주셔야 합니다.

2. 웹서버용 인증서 신청서 양식에 따라 구비서류를 직접 제출합니다. 인증서 사용자의 신원확인을 위해 직접 방문하셔야 합니다. 이때 설치 일정 및 설치 설명서를 받으실 수 있습니다.

3. 설치 설명서를 참조하시어, 웹서버에서 CSR값을 생성하여 담당자에게 전달합니다. 이 CSR값은 공개 가능한 정보이기 때문에, 보통 이메일 또는 다른 수단을 통해 담당자에게 전달합니다.

4. 웹서버용 발급 담당자는 해당 CSR값을 이용하여 SSL 인증서를 발급하고, 이를 다시 인증서 사용자에게 전달하게 됩니다. 이후 설치 설명서를 참조하여 웹서버에 설치를 완료합니다.

5. SSL 인증서가 제대로 설치되었는지 테스트 한 후, SSL 서비스를 사용하시면 됩니다. 테스트 방법은 "https://"로 시작하는 해당 도메인 이름으로 접속하여(설정에 따라 다를 수 있음), 정상적으로 접속되면 브라우저 하단에 노란 자물쇠가 표시되는 것으로 확인할 수 있습니다. SSL이 제대로 동작하기 위해서는 해당 포트가 외부로 열려 있어야 합니다.

사용자 서명 요청서(CSR) 생성하기

사용자 서명 요청서(Certificate Signing Request; 이하 CSR이라 함)는 웹서버용 SSL 인증서를 발급 받기 위한 첫 번째 단계입니다. CSR은 사용하는 웹서버에서 생성하게 됩니다. 웹서버 소프트웨어 종류별로 CSR 생성 방법에 대해 설명하겠습니다.

TradeSign 웹서버용 SSL 인증서는 시중에 사용하는 거의 모든 웹서버 소프트웨어와 호환됩니다. 이 중 가장 많이 쓰이는 웹서버 소프트웨어에 대해 설치 설명서에서 다루겠습니다. 다음 목록에 나타나지 않는 웹서버 소프트웨어는 TradeSign 웹서버용 SSL 인증서 담당자에게 문의하십시오.

▶ 지원하는 웹서버 소프트웨어 목록

Apache	**Apache + mod_ssl with OpenSSL**
BEA	**BEA Weblogic**
IBM	**WebSphere**
Java	**Java Based Web Servers**
Microsoft	**Microsoft IIS 4.x / 5.x / 6.x**
Netscape	**iPlanet 4.1**

4. Apache Mod_SSL / OpenSSL에서 CSR 생성하기

CSR은 웹서버의 공개키를 포함한 인증서 신청정보가 들어있는 파일입니다. 이 CSR을 이용하여 SSL 인증서를 발급 받을 수 있습니다.

잠깐!!

Apache 웹서버에서 SSL 서비스를 이용하려면, mod_ssl이라는 Apache 모듈이 필요하며 또한, OpenSSL이라는 프로그램도 필요합니다.

mod_ssl은 Apache에 같이 설치가 되어 있어야 하는 모듈로서, Apache 1.x 버전은 기본적으로 이 모듈을 포함하고 있지 않기 때문에 별도로 설치해 주어야 하고, Apache 2.x 버전은 기본으로 포함되어 있습니다.

이 모듈이 설치되어 있는지는 다음의 명령어를 통해 확인할 수 있습니다.

♣ 다음의 명령어는 Unix 계열 운영체제를 기준으로 설명합니다.

▶ OpenSSL 설치 확인 방법

명령어	find / -name openssl
결 과	설치가 되어 있다면, 설치된 디렉토리 또는 파일이 출력됨. ex) /usr/bin/openssl

▶ mod_ssl 설치 확인 방법

명령어	/usr/local/apache/bin/httpd -l ("/usr/local/apache"는 Apache 웹서버의 설치 위치임)
결 과	설치가 되어 있다면, 다음의 모듈을 확인 할 수 있음. ex) Compiled in modules: mod_ssl.c (statically linking module로 설치 시) 또는 mod_so.c (DSO module로 설치 시)

만약, OpenSSL과 mod_ssl이 설치되어 있지 않다면, 다음 사이트를 참조하시어 설치하시기 바랍니다.

▶ OpenSSL 참조 사이트: http://www.openssl.org

▶ mod_ssl 참조 사이트: http://www.modssl.org

▶ Apache 참조 사이트: http://www.apache.org

잠깐!!

Windows용 Apache의 경우, 소스 파일을 컴파일 하는 것보다 바이너리 파일로 되어

있는 설치 파일을 다운 받아 설치하는 것이 편리합니다.

그리고, 다운 받으실 때에는 "no ssl" 버전을 받으시면 SSL 기능을 사용할 수 없으므로 openssl이 포함되어 있는 버전을 받으셔야 합니다. 이 버전에는 openssl을 미리 컴파일한 바이너리 파일이 같이 포함되어 있기 때문에, 번거롭게 컴파일을 하지 않아도 됩니다.

Apache 웹서버에 SSL 서비스를 이용하기 위한 기본 준비가 되어 있다는 가정하에, CSR을 생성하는 절차를 설명하겠습니다.

우선, 개인키 쌍과 CSR을 생성하기 위해 웹서버가 설치되어 있는 서버에서 다음의 명령어를 사용하여, 개인키를 생성합니다. 개인키는 SSL 통신 시 사용되는 기본적인 구성요소이며, 이 개인키와 TradeSign에서 발급한 웹서버용 SSL 인증서를 통해 보안서버를 구성할 수 있습니다.

개인키는 다음의 명령어를 통해 생성할 수 있습니다. 개인키 생성 시 오류가 발생한다면, 해당 OS가 random device를 사용할 수 없을 경우가 있으니, 개인키 생성 이전에 미리 random 입력값을 생성한 후 그 값을 이용하여 개인키를 생성하면 됩니다.

▶ 개인키 생성하는 방법

명령어	openssl genrsa -des3 -out private.key 1024 ("private.key" 개인키가 담길 파일입니다.)
결 과	Generating RSA private key, 1024 bit long modulus .....++++++ .....++++++ e is 65537 (0x10001) Enter pass phrase for private.key: Verifying - Enter pass phrase for private.key: 위의 명령어를 수행한 후, 현재 디렉토리에는 "private.key" 파일이 생성됩니다.
주 의	개인키 생성 시 "pass phrase" 즉, 비밀번호를 만들게 됩니다. 이 비밀번호는 개인키 확인 시, CSR 생성 시, SSL 적용 후 웹서버 기동 시 묻게 되는 중요한 비밀번호이기 때문에 반드시 기억하셔야 하는 비밀번호입니다. 비밀번호와 개인키는 꼭 백업해 놓으시기 바랍니다.

▶ random device가 없는 OS (Solaris 8 이하 버전)에서 개인키 생성하는 방법

명령어	openssl md5 * > rand.dat openssl genrsa -rand rand.dat -des3 -out private.key 1024
결 과	개인키를 생성할 때, random device에서 관한 오류가 발생한다면, 현재 사용하고 있는 OS에 random device가 없을 경우입니다. 이 때는 임의의 입력값을 생성한 후 그 입력값을 개인키 생성 시 지정하면 됩니다.

개인키를 생성하였다면, 이제 CSR을 생성하기 위해 다음의 세부사항을 입력하게 됩니다. 입력값은 되도록 정확하게 입력하여야 합니다. 하지만, 실제 인증서 발급 시 웹서버용 인증서 신청서를 통해 웹서버용 인증서 발급 담당자가 정확한 값으로 변경할 수 있기 때문에 틀린 값을 입력하였다고 염려하실 필요는 없습니다.

▶ CSR 생성 시 입력하는 세부항목

세부 입력 항목	설 명	예
Country Name (2 letter code)	국가 이름	KR
State or Province Name (full name)	도 또는 시 이름	Seoul
Locality Name (eg, city)	시 이름	Seoul
Organization Name (eg, company)	회사 이름	KTNET
Organizational Unit Name (eg, section)	부서 이름	IT
Common Name (eg, YOUR name)	*FQDN	www.tradesign.net
Email Address	담당자 이메일	tradesign@ktnet.co.kr
**A challenge password	비밀번호	그냥 엔터
**An optional company name	추가 회사 이름	그냥 엔터

* FQDN은 전체 주소 도메인 이름으로 호스트 이름과 도메인 이름을 합친 전체 도메인 이름입니다. Ex) www.tradesign.net

** 위의 두 항목은 입력하지 마시고, 그냥 엔터를 치시면 됩니다. 이 항목을 입력 시, 경우에 따라 인증서가 발급되지 않을 수 있습니다.

▶ CSR 항목 입력시 주의사항

입력 불가 문자	< > ~ ! @ # $ % ^ * / ₩ ( ) ? 등 특수문자 입력 불가
Common Name 입력 시	전체 주소 도메인 이름을 입력하여야 하며, http://, https:// 등은 입력하지 마십시오.
추가 입력 항목	A challenge password, An optional company name 항목은 입력하지 마시고, 바로 엔터를 입력합니다.

이제 다음 명령어를 통해 CSR을 생성합니다.

▶ CSR 생성하는 방법

명령어	openssl req -new -key private.key -out server.csr “private.key”는 이전 과정에서 생성한 개인키 파일이며, “server.csr”은 생성될 CSR 파일의 이름입니다.
결 과	Enter pass phrase for private.key: (개인키 비밀번호 입력) You are about to be asked to enter information that will be incorporated into your certificate request. What you are about to enter is what is called a Distinguished Name or a DN. There are quite a few fields but you can leave some blank For some fields there will be a default value, If you enter '.', the field will be left blank. ----- Country Name (2 letter code) [AU]:KR State or Province Name (full name) [Some-State]:Seoul Locality Name (eg, city) []:Seoul Organization Name (eg, company) [Internet Widgits Pty Ltd]:KTNET Organizational Unit Name (eg, section) []:IT Common Name (eg, YOUR name) []:www.tradesign.net Email Address []:tradesign@ktnet.co.kr Please enter the following 'extra' attributes to be sent with your certificate request A challenge password []: An optional company name []: CSR 생성 명령어 실행 후, 실행 디렉토리에는 “server.csr” CSR 파일이 생성됩니다.

▶ CSR 확인하는 방법

명령어 openssl req -noout -text -in server.csr

결 과 Certificate Request:

Data:

Version: 0 (0x0)

Subject: C=KR, ST=Seoul, L=Seoul, O=KTNET, OU=IT, CN=www.tradesign.net/emailAddress=tradesign@ktnet.co.kr

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

...

이제 CSR이 생성되었다면, server.csr 파일을 웹서버용 인증서 발급 담당자에게 이메일 또는 다른 수단으로 발송하면 됩니다. 이 CSR 파일은 해당 인증서 요청에 대한 정보가 들어있으며, 공개가 되어도 문제가 없는 정보이기 때문에, 온라인 상으로 전송하여도 문제가 되지 않습니다.

잠깐!!

서두에 언급하였듯이, SSL 통신을 이용하기 위해서는 해당 SSL 서비스가 이용하는 포트를 방화벽과 같은 네트워크 설정을 통해 외부로부터 열려 있어야 합니다.

기본적으로 http://는 80 포트, https://는 443 포트를 사용합니다. 이 포트의 네트워크 설정을 잊지 마시기 바랍니다.

Apache 웹서버에 인증서 설치하기

TradeSign 웹서버 인증서 담당자는 수신 받은 CSR을 이용하여, 웹서버용 SSL 인증서를 발급하게 됩니다. 해당 파일은 기본적으로 "[해당 도메인 이름].cer"의 이름으로 전달되게 됩니다.

이제 이 인증서 파일(www.tradesign.net.cer)과 전 과정에서 생성했던 개인키 파일(private.key)을 통해, Apache 웹서버에 SSL 서비스를 적용해 보겠습니다.

잠깐!!

Apache 웹서버는 버전에 따라 SSL을 설정하는 conf 파일이 상이할 수 있습니다. 보통 Apache 설치 디렉토리 하에 conf 디렉토리에 설정파일들이 위치하며, 웹서버의 전반을 설정하는 "httpd.conf" 파일에서 설정하게 됩니다. 하지만, 버전에 따라 "ssl.conf" 파일에서 설정을 대신할 수도 있습니다. 이 "ssl.conf" 파일은 보통 conf 디렉토리 밑 extra 디렉토리에 위치합니다.

다음에 설명하는 설정 내용이 "httpd.conf" 파일에 없다면, "ssl.conf" 파일을 찾아 해당 설정을 하면 됩니다. 단, 이때 "httpd.conf" 파일에 다음 항목의 주석처리를 해제해야 합니다.

```
# Secure (SSL/TLS) connections
#Include conf/extra/httpd-ssl.conf (앞의 "#"을 삭제)
```

기본적인 설정은 어느 설정 파일에서 수정하든지 동일한 내용입니다. 설치 환경에 따라, 설정 파일의 위치는 다를 수 있습니다.

Windows 버전의 경우, 다음의 주석도 삭제합니다.

```
#LoadModule ssl_module modules/mod_ssl.so (앞의 "#"을 삭제)
```

우선, 설정파일을 수정하기 전에 개인키 파일과 인증서 파일을 웹서버 시스템의 적당한 위치에 복사합니다. 다음은 설정파일에서 변경하여야 하는 부분입니다. 해당 부분을 찾아 내용에 맞게 설정을 변경하십시오.

▶ SSL 관련 설정 내용

```
<VirtualHost _default_:443>

#   General setup for the virtual host
DocumentRoot "/usr/local/apache2/htdocs"
ServerName www.tradesign.net:443
▲ 서버의 이름을 환경에 맞게 수정하세요.
ServerAdmin tradesign@ktent.co.kr
ErrorLog /usr/local/apache2/logs/error_log
TransferLog /usr/local/apache2/logs/access_log

#   SSL Engine Switch:
#   Enable/Disable SSL for this virtual host.
SSLEngine on
▲ SSL엔진을 "on" 하셔야 합니다. (기본값이 "on" 입니다.)

#   SSL Cipher Suite:
#   List the ciphers that the client is permitted to negotiate.
#   See the mod_ssl documentation for a complete list.
SSLCipherSuite
ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP:+eNULL

SSLCertificateFile /usr/local/apache2/conf/www.tradesign.net.cer
▲ 발급 받은 SSL 인증서의 경로에 맞게 수정해 주세요.
#SSLCertificateFile /usr/local/apache2/conf/server-dsa.crt

#   Server Private Key:
#   If the key is not combined with the certificate, use this
#   directive to point at the key file.  Keep in mind that if
#   you've both a RSA and a DSA private key you can configure
#   both in parallel (to also allow the use of DSA ciphers, etc.)
SSLCertificateKeyFile /usr/local/apache2/conf/private.key
▲ 개인키의 경로에 맞게 수정해 주세요.
#SSLCertificateKeyFile /usr/local/apache2/conf/server-dsa.key
```

이제 환경설정은 끝났습니다. Apache를 구동시켜서 SSL 통신으로 동작하는지 확인하여야 합니다.

▶ **Apache 웹서버를 SSL로 구동하는 방법**

명령어 **./apachectl startssl**

결 과 **Enter pass phrase:**

이 문구가 나올 때 개인키의 비밀번호를 입력하시기 바랍니다.

구동 후, 인터넷 주소창에 "https://설정도메인"으로 접속하여 정상적으로 구동되지는 확인하시기 바랍니다.

잠깐!!

설정파일 변경 후 구동이 되지 않거나, 정상적으로 SSL 서비스가 되지 않는다면, Apache, mod_ssl, OpenSSL 등의 사이트를 통해 정보를 확인하시기 바랍니다.

- ▶ **OpenSSL 참조 사이트: http://www.openssl.org**
- ▶ **mod_ssl 참조 사이트: http://www.modssl.org**
- ▶ **Apache 참조 사이트: http://www.apache.org**

5 Microsoft IIS 4.x / 5.x / 6.x CSR 생성하기

마이크로소프트 IIS (Internet Information Server)는 현재 4.x / 5.x / 6.x 버전이 사용되고 있습니다. 여러 버전이 존재하기는 하지만, 실제 SSL 인증서를 설치하는 명령어는 대동소이 하기 때문에 한가지로 설명하겠습니다. 순서는 CSR 생성하기, 개인키 백업하기 순으로 설명 하겠습니다.

CSR을 생성하기 위해서는 IIS 관리자를 실행해야 합니다. "인터넷 서비스 관리자" 또는 "인터넷 정보 서비스(IIS) 관리" 메뉴를 실행합니다.

▶ 인터넷 서비스 관리자 실행 방법

- ☑ **[시작] 메뉴 클릭**
- ☑ **[프로그램] 또는 [모든 프로그램] 메뉴 선택**
- ☑ **[관리도구] 메뉴 선택**
- ☑ **[인터넷 서비스 관리자] 또는 [인터넷 정보 서비스(IIS) 관리] 메뉴 실행**

이제 "인터넷 서비스 관리자"에서 서비스가 되고 있는 웹 사이트에 CSR을 생성하겠습니다. CSR을 생성하기 위해서는 "웹 서버 인증서 마법사"를 통해 생성하게 됩니다. 이 마법사 과정을 마치고 나면, CSR과 개인키가 생성됩니다.

▶ 웹 서버 인증서 마법사 실행 방법

- ☑ **"인터넷 서비스 관리자"의 왼쪽 트리 중 SSL을 적용할 웹 사이트 선택**
- ☑ **마우스 오른쪽 버튼을 클릭하여 [등록정보] 또는 [속성] 메뉴 선택**
- ☑ **해당 웹사이트 등록정보 창에서 [디렉토리 보안] 탭 선택**
- ☑ **[보안 통신] 부분에서 [서버 인증서] 클릭**

이제 화면에는 "웹 서버 인증서 마법사"가 실행되어 있습니다. 이 마법사는 약 10 단계의 과정으로 구성되어 있으며, CSR과 개인키 생성에 필요한 정보를 순서대로 입력 받게 됩니다. 이 과정에서 입력 시 주의 사항은 다음과 같습니다.

▶ CSR 항목 입력 시 주의사항

입력 불가 문자	**, < > ~ ! @ # $ % ^ * / ₩ ( ) ? 등 특수문자 입력 불가**
Common Name 입력 시	**전체 주소 도메인 이름을 입력하여야 하며, http://, https:// 등은 입력하지 마십시오.**

이제 "웹 서버 인증서 마법사"의 각 단계를 설명하겠습니다. IIS 버전에 따라, 각 단계의 용어가 다소 상이할 수는 있으나, 의미상 큰 차이는 없고 과정 또한 동일하게 진행됩니다.

입력값은 되도록 정확하게 입력하여야 합니다. 하지만, 실제 인증서 발급 시 웹서버용 인

증서 신청서를 통해 웹서버용 인증서 발급 담당자가 정확한 값으로 변경할 수 있기 때문에 틀린 값을 입력하였다고 염려하실 필요는 없습니다.

▶ 웹 서버 인증서 마법사 입력 방법

- ☑ **"웹 서버 인증서 마법사"가 처음 실행되면 마법사의 설명과 웹 서버 상태를 간략하게 나타냅니다. [다음]을 클릭하여 다음 단계로 넘어갑니다.**
- ☑ **[서버 인증서] 단계에는 인증서 할당 방법을 선택합니다. [새 인증서를 만듭니다.]를 선택하고 [다음]을 클릭하여 다음 단계로 넘어갑니다.**
- ☑ **[요청 연기 또는 즉시 요청] 단계에는 CSR 전송에 관련된 설정을 하게 됩니다. 보통 [요청을 지금 준비하지만 나중에 보냅니다.]만 선택 가능한 상태입니다. 이것을 선택한 후, [다음]을 클릭하여 다음 단계로 넘어갑니다.**
- ☑ **[이름 및 보안 설정] 단계에는 인증서의 이름과 암호화 키의 길이를 설정하게 됩니다. [이름]은 인증서 발급 정보에 포함되어 있지 않으며, 관리자가 식별하기 편리한 이름으로 적당하게 입력하면 됩니다. Ex) www.tradesign.net**
  암호화 키의 [비트 길이]는 [1024]를 선택한 후, [다음]을 클릭하여 다음 단계로 넘어갑니다. [비트 길이] 아래 사항은 체크하지 않습니다.
- ☑ **[조직 정보] 단계에는 [조직]란에 "영문 회사명"을 입력하시면 됩니다. [조직 구성 단위]란에는 "영문 부서명"을 입력하시면 됩니다. 입력 후, [다음]을 클릭하여 다음 단계로 넘어갑니다.**
- ☑ **[사이트 일반 이름] 단계에는 [일반 이름]을 입력하게 되는데, "도메인 주소"를 입력하시면 됩니다. 입력 후, [다음]을 클릭하여 다음 단계로 넘어갑니다.**
- ☑ **[지역 정보] 단계에는 [국가/지역]은 "KR (대한민국)"으로, [시/도]는 "영문 시/도 이름"을, [구/군/시]는 "영문 구/군/시 이름"을 입력합니다. 입력 후, [다음]을 클릭하여 다음 단계로 넘어갑니다.**
- ☑ **[인증서 요청 파일 이름] 단계에는 인증서 요청 파일이 저장된 위치와 파일 이름을 입력하게 됩니다. 기본적으로 "c:₩certreq.txt"로 지정되어 있으며, 임의로 변경 가능합니다. 입력 후, [다음]을 클릭하여 다음 단계로 넘어갑니다.**
- ☑ **[요청 파일 요약] 단계에는 지금까지 입력한 내용이 출력됩니다. 혹시 잘못 입력된 부분이 있다면, [뒤로]를 클릭하여 수정하면 됩니다. 확인 후, [다음]을 클릭하여 다음 단계로 넘어갑니다.**
- ☑ **이제 모든 단계가 끝났습니다. CSR 파일은 지정하신 디렉토리에 지정하신 이름의 파일로 생성되었습니다. [마침]을 클릭하여 과정을 끝냅니다.**

다음은 웹 서버 인증서 마법사의 단계별 입력 사항을 요약한 내용입니다.

▶ 웹 서버 인증서 마법사 단계별 입력 사항 요약

단 계	입 력 사 항	설명 및 입력
웹 서버 인증서 마법사		웹 서버 상태 표시
서버 인증서		[새 인증서를 만듭니다.]

요청 연기 또는 즉시 요청		[요청을 지금 준비하지만 나중에 보냅니다.]
이름 및 보안 설정	이름	[임의의 이름]
	비트 길이	[1024]
	비트 길이 아래 사항	체크 안 함
조직 정보	조직	[영문 회사명]
	조직 구성 단위	[영문 부서명]
사이트 일반 이름	일반 이름	[도메인 주소]
지역 정보	국가/지역	[KR (대한민국)]
	시/도	[영문 시/도 이름]
	시/군/구	[영문 시/군/구 이름]
인증서 요청 파일 이름		요청 파일 이름 및 위치 설정
요청 파일 요약		입력 내용 확인
마법사 완료		[마침]

마법사가 끝나고 나면, CSR 파일이 지정한 위치에 저장되어 있습니다. 비록 파일로 생성되지는 않았지만, 개인키 역시 생성되어 있습니다. 이 CSR 파일은 TradeSign 웹서버용 인증서 담당자에게 이메일 또는 다른 수단으로 보내주시기 바랍니다. 이 CSR 파일은 외부로 공개되어도 문제가 없는 공개적인 정보만을 담고 있기 때문에, 온라인으로 전송하셔도 괜찮습니다.

SSL 통신을 위해 필요한 두 가지 요소는 인증서와 개인키입니다. 인증서는 CSR을 통해 TradeSign의 해당 담당자가 인증서를 생성하여 다시 보내드릴 것입니다. 하지만, 개인키는 지금 웹서버가 있는 시스템에 저장되어 있으며, 이 파일은 반드시 백업 받아 보관하셔야 합니다.

이제부터 개인키를 백업하는 방법에 대하여 설명하겠습니다. 개인키를 백업하기 위해서는 "Microsoft Management Console (MMC)"를 이용하여 작업을 하게 됩니다. MMC를 실행하는 방법부터 시작하겠습니다.

▶ MMC 실행 방법

- ☑ [시작] 메뉴 클릭
- ☑ [실행] 메뉴 선택
- ☑ [열기] 항목에 "mmc" 입력 후 [확인] 클릭

이 MMC는 Windows하에서 하드웨어, 소프트웨어, 네트워크 구성요소를 관리하는 도구이며, 이러한 도구를 "스냅인"이라고 부릅니다. 여기서는 "인증서 스냅인"을 추가하고, 이 기능을 이용하여 개인키를 백업하겠습니다.

▶ 인증서 스냅인 추가 방법

- ☑ **MMC 메뉴 중 [콘솔] 또는 [파일] 메뉴에서 [스냅인 추가/제거] 메뉴 선택**
- ☑ **[스냅인 추가/제거] 창에서 [추가] 버튼 클릭**
- ☑ **[독립 실행형 스냅인 추가] 창에서 [인증서] 선택 후 [추가] 버튼 클릭**
- ☑ **[인증서 스냅인] 창에서 "관리할 인증서 대상"을 [컴퓨터 계정]으로 선택 후 [다음] 버튼 클릭**
- ☑ **[컴퓨터 선택] 창에서 [로컬 컴퓨터] 선택 후 [마침] 클릭**
- ☑ **[닫기] 버튼 클릭 후, [확인] 버튼으로 "스냅인 추가/제거" 창을 종료**

이제 MMC 왼쪽 "콘솔 루트" 트리에는 "인증서(로컬 컴퓨터)"가 추가되었습니다. "인증서(로컬 컴퓨터)" 트리를 확장하여 보면 "인증서 등록 요청" 트리 하위에 "인증서"를 선택하면 오른쪽 화면에 인증서가 보이게 됩니다. 이것을 선택하여 개인키를 백업하게 됩니다. 이 인증서를 선택 후 마우스 오른쪽 버튼을 누르면 [모든 작업] 하위에 [내보내기] 메뉴를 통해 "인증서 내보내기 마법사"를 시작할 수 있습니다.

▶ 인증서 내보내기 마법사 실행 방법

- ☑ **왼쪽 "콘솔 루트" 트리에서 "인증서(로컬 컴퓨터)" 트리 확장**
- ☑ **"인증서 등록 요청" 트리 확장**
- ☑ **"인증서" 선택**
- ☑ **오른쪽 "인증서" 선택 후 오른쪽 마우스 버튼 클릭**
- ☑ **[모든 작업] 하위에 [내보내기] 메뉴를 통해 "인증서 내보내기 마법사" 시작**

"인증서 내보내기 마법사"는 다음의 단계를 통해 개인키를 백업 받습니다.

▶ 인증서 내보내기 마법사 입력 방법

- ☑ **"인증서 내보내기 마법사 시작"에서 [다음] 버튼 클릭**
- ☑ **"개인키 내보내기" 단계에서 "예, 개인 키를 내보냅니다." 선택 후 [다음] 버튼 클릭**
- ☑ **"파일 내보내기 형식" 단계에서 "개인 정보 교환 - PKCS #12(.PFX)" 선택, "강력한 보호 사용(Internet Explorer 5.0, NT 4.0 SP4 이상 필요)"만 체크 선택 후 [다음] 버튼 클릭**
- ☑ **"암호" 단계에서 "암호", "암호 확인" 입력**
  (이 값은 개인키를 다시 사용하고자 할 때 입력해야 하는 값으로 반드시 기억하여야 합니다.)
- ☑ **"내보낼 파일" 단계에서 "파일 이름"에 디렉토리와 파일이름을 임의로 선택하여 입력 후 [다음] 버튼 클릭**
- ☑ **"인증서 내보내기 마법사 완료" 단계에서 정보 확인 후 [마침] 클릭**
- ☑ **내보내기가 정상적으로 성공하면 "내보내기를 완료했습니다."라는 확인 창이 나타납니다. [확인] 버튼으로 종료하시면 됩니다.**

이제 생성된 개인키와 개인키 암호는 안전한 저장 공간에 백업을 하시면 됩니다. MMC를 종료하려고 하면 저장을 할 수 있는데, 적당한 이름으로 저장하시면 됩니다. 이는 나중에 동일한 작업을 수행한다면, 인증서 스냅인 추가 작업을 다시 하지 않아도 됩니다.

Microsoft IIS 4.x / 5.x / 6.x에 인증서 설치하기

CSR을 생성하고 TradeSign 웹서버 인증서 담당자에게 전송하고 나면, 인증서 파일을 받을 수 있습니다. 이 인증서 파일을 이용하여 이제 SSL 통신이 가능하도록 설정하여야 합니다. 이 설정은 "인터넷 서비스 관리자" 또는 "인터넷 정보 서비스(IIS) 관리"를 통해 할 수 있습니다.

▶ 인터넷 서비스 관리자 실행 방법

- ☑ **[시작] 메뉴 클릭**
- ☑ **[프로그램] 또는 [모든 프로그램] 메뉴 선택**
- ☑ **[관리도구] 메뉴 선택**
- ☑ **[인터넷 서비스 관리자] 또는 [인터넷 정보 서비스(IIS) 관리] 메뉴 실행**

이제 다시 "웹 서버 인증서 마법사"를 통해 인증서를 설치하겠습니다.

▶ 웹 서버 인증서 마법사 실행 방법

- ☑ **"인터넷 서비스 관리자"의 왼쪽 트리 중 SSL을 적용할 웹 사이트 선택**
- ☑ **마우스 오른쪽 버튼을 클릭하여 [등록정보] 또는 [속성] 메뉴 선택**
- ☑ **해당 웹사이트 등록정보 창에서 [디렉토리 보안] 탭 선택**
- ☑ **[보안 통신] 부분에서 [서버 인증서] 클릭**

이제 "웹 서버 인증서 마법사"의 단계에 따라 인증서를 설치하겠습니다. 마법사는 이미 CSR을 생성한 다음이기 때문에 자동으로 인증서 설치를 위한 단계를 시작하게 됩니다.

▶ 웹 서버 인증서 마법사 단계별 입력 방법

- ☑ **"웹 서버 인증서 마법사 시작"에서 간략한 웹 서버의 정보를 볼 수 있습니다. [다음]을 클릭**
- ☑ **"인증서 요청 대기 중" 단계에서 [대기 중인 요청을 처리한 다음 인증서를 설치합니다.]를 선택 후 [다음]을 클릭**
- ☑ **"대기 중인 요청 처리" 단계에서 [경로 및 파일 이름]에서 해당 인증서를 선택 후 [다음]을 클릭**
- ☑ **"SSL 포트" 단계에서 [이 웹 사이트에서 사용해야 할 SSL]에서 "443"을 입력 후 [다음]을 클릭**
- ☑ **"인증서 요약" 단계에서 설치하려는 인증서 정보를 확인 후 [다음]을 클릭**
- ☑ **"웹 서버 인증서 마법사 완료"에서 [마침]을 클릭하여 종료**

이제 사용하고자 하는 웹 사이트에 SSL 인증서를 설치하였습니다. 이제 SSL 서비스를 이용할 수 있게 SSL 서비스를 활성화 합니다.

▶ SSL 서비스 활성화 방법

- ☑ **"인터넷 서비스 관리자"의 왼쪽 트리 중 SSL을 적용할 웹 사이트 선택**
- ☑ **마우스 오른쪽 버튼을 클릭하여 [등록정보] 또는 [속성] 메뉴 선택**
- ☑ **해당 웹사이트 등록정보 창에서 [웹 사이트] 탭 선택**
- ☑ **[웹 사이트 확인] 부분에서 [SSL 포트]에 "443"을 입력**
- ☑ **[확인]을 클릭하여 종료**

이제 SSL 서비스가 활성화 되었습니다. 확인 방법은 "https://도메인 주소"를 인터넷 주소창에 입력하여, 정상적으로 동작하는지 확인 하시면 됩니다.

6. BEA Weblogic CSR 생성하기

BEA Weblogic 서버는 CSR을 생성하기 위한 CSR 생성 Servlet을 제공합니다. 이 CSR 생성 Servlet은 CSR을 생성하기 위한 정보를 입력 받은 후, CSR 파일과 개인키 파일을 생성합니다. 이 CSR 생성 Servlet은 Weblogic이 설치될 당시, 자동적으로 설치됩니다. 이 CSR 생성 Servlet을 실행하여 CSR을 생성하겠습니다.

▶ CSR 생성 Servlet 실행 방법

명령어	https://hostname:port/Certificate
결 과	브라우저 인터넷 주소창에 위의 접속 주소를 입력합니다. "hostname"은 Weblogic이 구동되고 있는 서버의 DNS 이름이며, port는 Weblogic이 SSL 연결을 위해 사용하는 포트로서, 기본값은 7002 입니다.

CSR 생성 Servlet을 실행하면, 브라우저 화면에는 CSR 생성을 위한 정보를 입력하게 됩니다. 해당 정보를 입력한 후, [Generate Request] 버튼을 클릭하면, CSR이 생성됩니다. 다음은 CSR 생성을 위한 정보에 대한 설명입니다.

입력값은 되도록 정확하게 입력하여야 합니다. 하지만, 실제 인증서 발급 시 웹서버용 인증서 신청서를 통해 웹서버용 인증서 발급 담당자가 정확한 값으로 변경할 수 있기 때문에 틀린 값을 입력하였다고 염려하실 필요는 없습니다.

▶ CSR 생성을 위한 정보

입력 항목	설 명	예
Country code	국가 코드	KR
Organizational unit name	영문 부서 이름	IT
Organization name	영문 회사 이름	KTNET
E-mail address	관리자 이메일	tradesign@ktent.co.kr
Full host name	Full DNS 이름	www.tradesign.net
Locality name (city)	시/군/구 이름	Seoul
State name	시/도 이름	Seoul
Private Key Password	개인키 비밀번호	비밀번호 입력
Strength	키 길이	1024 bit key 입력

비밀번호는 개인키를 사용할 때마다 쓰게 되니, 개인키 파일과 함께 반드시 백업하셔야 합니다. CSR 생성 정보를 입력할 때에는 영문으로 입력하여야 하며, 특수문자는 입력하실 수 없습니다.

이제 [Generate Request] 버튼을 클릭한 후에는, CSR 생성 Servlet은 Weblogic의 시작 디렉토리에 다음의 3가지 파일을 생성합니다.

▶ **CSR 생성 Servlet이 생성한 파일**

파 일 명	설 명	비 고
hostname-key.der	개인키 파일	백업해 놓으세요.
hostname-request.dem	CSR 바이너리 파일	바이너리 형태의 CSR
hostname-request.pem	CSR ASCII 파일	이 CSR 파일을 TradeSign 웹서버 담당자에게 보냅니다.

이제 CSR이 생성되었다면, hostname-request.pem 파일을 웹서버용 인증서 발급 담당자에게 이메일 또는 다른 수단으로 발송하면 됩니다. 이 CSR 파일은 해당 인증서 요청에 대한 정보가 들어 있으며, 공개가 되어도 문제가 없는 정보이기 때문에, 온라인 상으로 전송하여도 문제가 되지 않습니다.

BEA Weblogic에 인증서 설치하기

TradeSign 웹서버 담당자에게 인증서 파일을 수신 받은 후, 이 인증서를 사용하여 SSL 통신이 가능하도록 Weblogic을 설정하겠습니다. SSL 통신은 Weblogic의 Administration Port에서 설정하게 됩니다. SSL 통신을 위한 설정은 다음과 같은 단계로 이루어집니다.

▶ SSL 서비스 활성화 방법

- ☑ **Server 노드를 확장합니다.**
- ☑ **"Connections"에서 "SSL Ports" 탭을 엽니다.**
- ☑ **"Enabled" 속성을 활성화 시킵니다.**
- ☑ **"SSL Listen Port" 속성에 SSL 통신을 위한 포트번호를 설정합니다 (Weblogic 기본은 7002 포트이며, 보통 443 포트를 사용합니다.)**
- ☑ **SSL 통신을 위한 상세 설정을 합니다. (설정법 아래에 설명)**
- ☑ **"Apply" 하여 변경사항을 저장합니다.**

다음은 상세 설정에 대한 설명입니다.

▶ SSL 속성 상세 설정 방법

속 성	설 명
Server Private Key Alias	keystore를 사용할 때 쓰이는 개인키의 Alias
Server Private Key Passphrase	Keystore를 사용할 때 쓰이는 개인키의 비밀번호
Server Certificate File Name	인증서의 경로
Server Key File Name	개인키의 경로
Trusted CA File Name	상위 인증서의 경로

keystore를 사용하지 않고, 파일 형태의 개인키를 사용하기 때문에, Server Private Key Alias와 Server Private Key Passphrase는 입력하지 않습니다. (해당 방식으로 사용하고자 할 경우, Weblogic 설명서 참조)

개인키를 사용할 때는 개인키의 비밀번호를 입력하여야 합니다. 비밀번호를 입력하는 방법은 command-line 인수를 사용하여 Weblogic 서버를 구동하게 됩니다.

▶ **command-line 인수 지정 방법**

명령어	**-Dweblogic.management.pkpassword=*pkpassword***
결 과	***pkpassword*는 개인키의 비밀번호**

이제 SSL 서비스가 활성화 되었습니다. 확인 방법은 "https://도메인 주소"를 인터넷 주소 창에 입력하여, 정상적으로 동작하는지 확인 하시면 됩니다.

7. IBM WebSphere CSR 생성하기

CSR을 생성하기 위해서는 우선, 개인키를 생성하여야 합니다. 이 개인키를 생성하는 툴로서 IBM은 WebSphere와 함께 "ikeyman"이라는 툴을 제공하고 있습니다. 이 툴을 이용하여 개인키를 생성하겠습니다.

▶ ikeyman 실행 방법

명령어	./ikeyman.sh
결 과	"IBM Key Management"가 실행됩니다.

"IBM Key Management"는 이미 존재하는 keystore를 사용하거나, 새로 keystore를 생성할 수 있습니다. 다음은 새로운 keystore를 생성하는 방법입니다.

▶ 새로운 keystore를 생성하는 방법

명령어	IBM Key Management 콘솔 메뉴 중 [Key Database File] 메뉴 중 [New] 메뉴 클릭
결 과	[New] 창이 실행되며, 입력 사항은 다음과 같습니다. ☑ Key database type: "JKS" 선택 ☑ File Name: keystore의 이름 입력 예) ".keystore" ☑ Location: keystore의 경로 입력 예) "/usr/bin/java/websphere/bin/" [OK] 버튼 클릭

다음으로 CSR을 생성합니다.

▶ CSR 생성하는 방법

명령어	IBM Key Management 콘솔 메뉴 중 [Create] 메뉴 중 [New Certificate Request] 메뉴 클릭
결 과	[Create New Key and Certificate Request] 창이 실행되며, 입력 사항을 입력한 후 [OK] 버튼 클릭

"Create New Key and Certificate Request" 창에서 입력하는 세부 사항은 다음과 같습니다.

입력값은 되도록 정확하게 입력하여야 합니다. 하지만, 실제 인증서 발급 시 웹서버용 인증서 신청서를 통해 웹서버용 인증서 발급 담당자가 정확한 값으로 변경할 수 있기 때문에 틀린 값을 입력하였다고 염려하실 필요는 없습니다.

▶ Create New Key and Certificate Request 상세 설정 방법

속 성	설 명
Key Label	리스트 화면에 표시되는 Request 이름
Key Size	1024로 입력
Common Name	Full DNS 이름 ex) www.tradesign.net
Organization	영문 회사 이름 ex) KTNET
Organization Unit	영문 부서 이름 ex) IT
Locality	시/군/구 ex) Seoul
State/Province	시/도 ex) Seoul
Country	KR 선택
Certificate Request file name	CSR 파일 이름과 경로 지정

[OK] 버튼을 클릭하면 CSR 파일이 생성됩니다. 개인키는 keystore에 안전하게 저장되게 됩니다. 이제 CSR이 생성되었다면, 해당 파일을 웹서버용 인증서 발급 담당자에게 이메일 또는 다른 수단으로 발송하면 됩니다. 이 CSR 파일은 해당 인증서 요청에 대한 정보가 들어 있으며, 공개가 되어도 문제가 없는 정보이기 때문에, 온라인 상으로 전송하여도 문제가 되지 않습니다.

IBM WebSphere에 인증서 설치하기

이제 TradeSign.net 웹서버 담당자는 해당 CSR을 통해 인증서를 발급하여 온라인 또는 기타 수단으로 인증서를 전달하게 됩니다. 이 인증서를 "ikeyman"을 통해 keystore에 등록하도록 하겠습니다.

▶ ikeyman 실행 방법

명령어	./ikeyman.sh
결 과	"IBM Key Management"가 실행됩니다.

우선, 인증서를 설치하기 전에 해당 인증서의 상위 기관 인증서를 등록하겠습니다.

발급 받은 인증서의 발급기관은 TradeSign 인증센터이며, 이 TradeSign 인증센터의 인증서를 발급한 상위 인증기관이 존재합니다. 최상위 인증기관을 root 인증기관, TradeSign 인증센터를 PrimServer 인증기관이라고 합니다. 이를 등록하겠습니다.

해당 root, primserver 인증서는 웹서버 SSL 인증서와 같이 제공됩니다. 만약 같이 제공받지 못했을 경우, TradeSign 웹서버 담당자에게 root 인증서와 TradeSign 인증서를 요청하시면 됩니다.

▶ 상위 인증기관 인증서 등록 방법

- ☑ "IBM Key Management" 콘솔에서 중간의 드롭다운 메뉴에서 "Signer Certificates"를 선택
- ☑ 하위 메뉴 중 "root"를 선택 후, [Add] 버튼을 클릭
- ☑ 해당 root 인증서 등록
- ☑ 하위 메뉴 중 "primserver"를 선택후, [Add] 버튼을 클릭
- ☑ 해당 primserver 인증서 등록

이제 웹서버의 인증서를 등록하겠습니다.

▶ SSL 인증서 등록 방법

- ☑ "IBM Key Management" 콘솔에서 중간의 드롭다운 메뉴에서 "Personal Certificates"를 선택
- ☑ [Rceive] 메뉴 클릭
- ☑ 다이얼로그 박스에서 인증서 파일 이름과 경로 입력
- ☑ [OK] 버튼을 클릭

이제 keystore에 개인키와 인증서가 정상적으로 등록되었습니다. IBM WebSphere의 administrative 콘솔에서 SSL을 활성화시키면 됩니다. 활성화 방법은 해당 매뉴얼을 참조하시기 바랍니다.

이제 SSL 서비스가 활성화 되었습니다. 확인 방법은 "https://도메인 주소"를 인터넷 주소 창에 입력하여, 정상적으로 동작하는지 확인 하시면 됩니다.

8. Java Based Web Servers CSR 생성하기

자바 기반의 웹서버들은 Java JDK에 포함되어 있는 "keytool"이라는 툴을 이용하여 CSR을 생성하게 됩니다. 이 툴은 보안에 사용되는 키와 인증서 등을 관리하는 프로그램입니다. 이 툴은 Java Home 디렉토리 하위 bin 디렉토리에 있습니다. CSR을 생성하기 위해서는 우선 개인키를 생성하여야 하며, 개인키 생성 후 CSR을 생성하게 됩니다.

▶ keytool을 이용하여 개인키 생성 방법

명령어	%JAVA_HOME%/bin에 keytool이 존재합니다. keytool -genkey -keyalg RSA -keystore private.key -validity 360
결 과	이 명령어를 실행하면 다음의 사항을 입력하게 됩니다. 그 후 명령어를 실행한 디렉토리에 private.key 파일이 생성됩니다.

입력값은 되도록 정확하게 입력하여야 합니다. 하지만, 실제 인증서 발급 시 웹서버용 인증서 신청서를 통해 웹서버용 인증서 발급 담당자가 정확한 값으로 변경할 수 있기 때문에 틀린 값을 입력하였다고 염려하실 필요는 없습니다.

▶ keytool에서 개인키 생성 시 입력 사항

속 성	설 명	예
key store password	keystore 암호	keystore의 비밀번호
Common Name	이름과 성 이름	www.tradesign.net
Organization Unit Name	조직 단위 이름	IT
Organization Name	조직 이름	KTNET
Locality Name	구/군/시 이름	Seoul
State or Province Name	시/도 이름	Seoul
Country Name	국가 코드	KR
입력 정보 출력	입력 정보 확인	yes
Key password for <mykey>	<mykey> 암호	keystore 비밀번호와 동일하게 입력

이제 해당 디렉토리에는 "private.key" 파일이 생성되었습니다. 이 파일은 개인키 파일이며, 입력한 비밀번호와 함께 백업해 놓으시기 바랍니다.

이제 개인키를 이용하여 CSR 파일을 생성하도록 하겠습니다.

▶ keytool을 이용하여 CSR 생성 방법

명령어	%JAVA_HOME%/bin에 keytool이 존재합니다. keytool -certreq -sigalg RSA -file server.csr -keystore private.key
결 과	이 명령어를 실행하면 개인키의 비밀번호를 입력하게 됩니다.

그 후 명령어를 실행한 디렉토리에 server.csr 파일이 생성됩니다.

이제 CSR이 생성되었다면, server.csr 파일을 웹서버용 인증서 발급 담당자에게 이메일 또는 다른 수단으로 발송하면 됩니다. 이 CSR 파일은 해당 인증서 요청에 대한 정보가 들어있으며, 공개가 되어도 문제가 없는 정보이기 때문에, 온라인 상으로 전송하여도 문제가 되지 않습니다.

Java Based Web Servers에 인증서 설치하기

CSR을 TradeSign 웹서버 담당자에게 제출하면, 웹서버 인증서를 전달 받게 됩니다. 보통 root 인증서, TradeSign 인증서, 신청한 서버 인증서 등 3가지 파일을 받게 됩니다. 이 인증서를 keytool을 이용하여 가져오기(import)를 하겠습니다.

개인키가 있는 디렉토리로 이동하여 실행하십시오.

▶ keytool을 이용하여 인증서 import하는 방법

명령어	**☑ root 인증서 import** **keytool -import -trustcacerts -alisa root -file (root 인증서 파일명) -keystore private.key** **☑ TradeSign 인증서 import** **keytool -import -trustcacerts -alias INTER -file (TrdesSign 인증서 파일명) -keystore private.key** **☑ SSL 서버 인증서 import** **keytool -import -trustcacerts -alias (임의의 별명 입력) -file (SSL 서버 인증서 파일명) -keystore private.key**
결 과	**이 명령어를 실행하면 개인키의 비밀번호를 입력하게 됩니다.**

이제, SSL 통신을 위한 keystore 설정을 성공적으로 끝냈습니다. 각 자바 기반의 웹서버는 이 keystore를 이용하여 SSL 통신을 사용할 수 있습니다. 웹서버 설정에서 SSL 관련 설정을 할 때 keystoreFile, keystorePass 등의 설정을 하시면 SSL 통신을 활성화 할 수 있습니다. SSL 통신에 관련된 사항은 각각의 설명서를 참조하시기 바랍니다.

이제 SSL 서비스가 활성화 되었습니다. 확인 방법은 "https://도메인 주소"를 인터넷 주소창에 입력하여, 정상적으로 동작하는지 확인 하시면 됩니다.

9. iPlanet Web Server에 CSR 생성하기

iPlanet Web Server는 Web Server Administration Server를 통해 CSR을 생성/설정할 수 있습니다. Administration Server에 접속한 후, SSL 인증서를 설치할 서버를 선택합니다. 이제, CSR을 먼저 생성하겠습니다.

▶ CSR을 위한 Database 생성 방법

- ☑ **Admin 화면에서 [Security] 탭을 선택**
- ☑ **[Create Database] 선택**
- ☑ **[Database Password] 입력**
  (이 비밀번호는 개인키 사용 및 서버 구동시 사용되는 비밀번호이므로, 꼭 기억하셔야 합니다.)
- ☑ **[OK] 클릭으로 생성**

다음은 CSR을 생성하는 절차입니다.

▶ CSR 생성 방법

- ☑ **Admin 화면에서 [Security] 탭을 선택**
- ☑ **[Request a Certificate] 선택**
- ☑ **세부 사항을 입력하여 [OK] 클릭으로 생성**

다음은 CSR 생성 시 입력하는 세부 사항입니다. 입력값은 되도록 정확하게 입력하여야 합니다. 하지만, 실제 인증서 발급 시 웹서버용 인증서 신청서를 통해 웹서버용 인증서 발급 담당자가 정확한 값으로 변경할 수 있기 때문에 틀린 값을 입력하였다고 염려하실 필요는 없습니다.

▶ CSR 생성 시 입력하는 세부 사항

속 성	설 명	예
New certificate	새로운 인증서 요청 생성	선택
Submit to Certificate Authority via:	TradeSign 담당자 이메일	[CA Email address:] 선택
Cryptographic Module:	암호 모듈	[internal (software)] 선택
Key Pair File Password:	비밀번호 입력	Database 비밀번호 입력
Requestor name:	담당자 이름	담당자 영문 이름
Telephone number:	담당자 전화번호	담당자 전화번호
Common name:	Full DNS 이름	ex) www.tradesign.net
Email address:	담당자 이메일	ex) tradesign@ktnet.co.kr
Organization:	회사 이름	ex) KTNET
Organization Unit:	부서명 이름	ex) IT
Locality:	시/군/구 이름	ex) Seoul
State or Province:	시/도 이름	ex) Seoul
Country:	국가 코드	ex) KR

정상적으로 CSR이 생성되었다면, 화면에는 인증서 요청 정보가 출력됩니다. 이 중에서 "-----BEGIN CERTIFICATE REQUEST-----"로 시작하여, "-----END CERTIFICATE REQUEST-----"로 끝나는 CSR 내용을 복사하여 문서편집기(메모장, vi 등)를 통해 text 파일로 저장합니다.

이제 해당 파일을 웹서버용 인증서 발급 담당자에게 이메일 또는 다른 수단으로 발송하면 됩니다. 이 CSR 파일은 해당 인증서 요청에 대한 정보가 들어 있으며, 공개가 되어도 문제가 없는 정보이기 때문에, 온라인 상으로 전송하여도 문제가 되지 않습니다.

iPlanet Web Server에 인증서 설치하기

CSR을 TradeSign 웹서버 담당자에게 제출하면, 해당 SSL 인증서를 전달 받게 됩니다. 이 파일을 이용하여 인증서를 설치하겠습니다. 인증서 설치 역시, Web Server Administration Server를 통해 설치할 수 있습니다.

Admin 서버에서 [Security] 탭에서 [Install Certificate] 메뉴를 통해 인증서를 설치합니다. 설치할 때 입력하는 사항은 다음과 같습니다.

▶ 인증서 설치 시 입력하는 세부 사항

속 성	설 명	예
Certificate for:	인증서 종류 선택	"This Server" 선택
Cryptographic Module:	암호 모듈 선택	"internal (software)" 선택
Key Pair File Password:	비밀번호 입력	개인키 비밀번호 입력
Certificate Name:	인증서 이름 입력	입력하지 않습니다.
Message text:	인증서 내용	인증서 파일의 내용 입력

인증서 내용은 받은 인증서를 문서편집기(메모장, vi 등)를 이용하여 복사/붙여넣기 하시면 됩니다. 단, 이때 "-----BEGIN CERTIFICATE-----"와 "-----END CERTIFICATE-----"도 포함하여야 합니다.

해당 내용을 입력한 후, [OK] 버튼을 클릭하면, 추가하려는 인증서의 내용이 출력됩니다. 확인하신 후, [Add Server Certificate] 버튼을 클릭하여 추가합니다.

이제 SSL 통신을 활성화하여 웹서버를 다시 실행하겠습니다.

Admin Server 화면에서 [Preferences] 탭에서 [Encryption On/Off]를 선택한 후 실행하면 됩니다.

▶ SSL 통신 활성화하는 방법

- ☑ **Admin Server 화면에서 [Preferences] 탭 선택**
- ☑ **[Encryption On/Off]를 선택**
- ☑ **[Encryption]을 "On"으로 설정**
- ☑ **[Port Number]를 설정 (보통 "443" 포트를 사용함)**
- ☑ **[OK] 버튼 클릭**
- ☑ **변경사항이 출력되며 [Save And Apply] 버튼 클릭**
- ☑ **개인키 비밀번호 입력**
- ☑ **[Preferences] 탭에서 [On/Off] 선택**
- ☑ **개인키 비밀번호 입력 후 서버 재시작**

이제 SSL 서비스가 활성화 되었습니다. 확인 방법은 "https://도메인 주소"를 인터넷 주소창에 입력하여, 정상적으로 동작하는지 확인 하시면 됩니다.

10. WebtoB에 CSR 생성하기

TMaxSoft 사의 Web서버인 WebtoB 제품은 커맨드 창에서 명령어를 실행시켜 CSR을 생성/설정할 수 있습니다. 개인키 및 CSR을 생성하는 명령어는 "CA" 라는 명령어로 옵션과 함께 실행합니다.

▶ CA 실행 방법

명령어	./CA -newreq
결 과	CSR 파일과 함께 개인키가 생성됩니다.

CA 명령어를 통해서 인증서 요청형식을 만들려면 아래와 같은 내용을 입력하여야 합니다.

▶ CSR생성시 입력정보 상세 설명

속 성	설 명
pass phrase	개인키를 암호화할 비밀번호
Country Name (2 letter code)	국가 이름
State or Province Name (full name)	도 또는 시 이름
Locality Name (eg, city)	시 이름
Organization Name (eg, company)	회사 이름
Organizational Unit Name (eg, section)	부서 이름
Common Name (eg, YOUR name)	설치할 서버의 URL 명
Email Address	담당자 이메일

완료후에는 newreq.pem 파일이 생성됩니다. 이 파일은 CSR 파일과 privatekey 파일이 함께 들어 있습니다. Vi 및 기타 텍스트 편집기로 newreq.pem 파일을 열면 아래와 같은 내용을 확인 할 수 있습니다. 여기서 BEGIN CERTIFICATE REQUEST 에서 END CERTIFICATE REQUEST 부분까지 복사하여 인증서 발행기관으로 전달한 후 인증서 발급을 요청합니다.

WebtoB에 인증서 설치하기

TradeSign 웹서버 담당자에게 인증서 파일을 수신 받은 후, 이 인증서를 사용하여 SSL 통신이 가능하도록 WebtoB를 설정하겠습니다. SSL 통신은 인증서를 복사하고 환경파일을 수정하는 순서대로 진행됩니다.

▶ 설정 변경 방법

- ☑ **인증서 파일을 수신받은 후 DER 포멧이면 PEM 형식으로 변경합니다.**
- ☑ **newreq.pem 파일을 열어서 CSR 부분을 삭제합니다.**
- ☑ **PEM 형식의 인증서를 삭제된 CSR 위치에 복사합니다.**
- ☑ **WebtoB의 http.m 파일을 열어 설정값을 변경합니다.**
- ☑ **IE의 주소창에 https 프로토콜을 이용한 url을 입력후 실행합니다.**

다음은 상세 설정에 대한 설명입니다.

▶ newreq.pem 설정에 대한 설명

아래는 인증서 요청포멧을 생성한 후의 newreq.pem 파일 입니다. 파일의 세부 내용을 확인하면 개인키값과 CSR 정보로 이루어져 있습니다.

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,AA015C077CE74A97

RIQzWFS2I8UNMMYhnApDuOIn3NcHzLS3CICYEjhftN/2prU6/nJwALiYve5MRXCm
V822gSj9k9an8eqyGs8jL/PHfbxxXJcmeZud3uBRP+wp0KuCSat+RbF++m+aUwsI
sJdrSNXYjLtYt7GT3S7MwlySZWlRUnW/7AucqFsHr3Yy5GT5/kGl7R0XEKlsSOt9
rpQ+mtCcNv8IF8qgIDjjlKBklVn3Frfuzxp0Z8cMk8521XsHfu/WQkCFEgnuQ9k8
.....
-----END RSA PRIVATE KEY-----


-----BEGIN CERTIFICATE REQUEST-----
MIIBujCCASMCAQAwejELMAkGA1UEBhMCS1IxDTALBgNVBAgTBEtJQ0ExDTALBg
NV
.....
-----END CERTIFICATE REQUEST-----
```

인증기관에서 인증서를 발급받은 후 인증서를 PEM 형식으로 변환합니다. PEM 형식의 파일을 메모장에서 확인하면 아래와 같이 "BEGIN CERTIFICATE"로 시작해서 "END CERTIFICATE"로 종료되는 형식을 취하고 있습니다. 이 부분을 복사하여 newreq.pem 파일의 CSR 부분(BEGIN CERTIFICATE REQUEST 에서 END CERTIFICATE REQUEST 부분)을 삭제하고 같은 자리에 인증서(BEGIN CERTIFICATE" 부터 "END CERTIFICATE" 까지)를 복사하고 저장합니다.
아래는 PEM 형태의 인증서의 예 입니다.

```
-----BEGIN CERTIFICATE -----
MIIEtzCCBCCgAwIBAgIQZd5GOtSfXHJBvoNkJkJooTANBgkqhkiG9w0BAQQFADCB
ujEfMB0GA1UEChMWVmVyaVNpZ24gVHJ1c3QgTmV0d29yazEXMBUGA1UECxMOVm
VyaVNpZ24sIEluYy4xMzAxBgNVBAsTKlZlcmlTaWduIEludGVybmF0aW9uYWwgU2Vy
dmVyIENBIC0gQ2xhc3MgMzFJMEcGA1UECxNAd3d3LnZlcmlzaWduLmNvbS9DUFMg
NjA0MjQwMDAwMDBaFw0wODA0MjMyMzU5NTlaMIH7MQswCQYDVQQGEwJLUjEO
MAwGA1UECBMFc2VvdWwxDzANBgNVBAcUBnNlb2NobzEXMBUGA1UEChQOREhDIE
tPUkVBIElOQy4xETAPBgNVBAsUCGluZm90ZWNoMTUwMwYDVQQLEyxUZXJtcyBvZiB
1c2UgYXQgd3d3LmNyb3NzY2VydC5jb20vcnBhIChjKSAwNDEkMCIGA1UECxMbQXV0a
-
-----END CERTIFICATE -----
```

▶ http.m 파일 수정 및 적용

SSLFLAG의 값을 "Y"로 설정하고 SSLNAME을 "ssl1" 으로 설정합니다. Ssl1 항목부분에서 CertificateFile, CertificateKeyFile 파일을 새로운 인증서를 복사한 파일의 path를 입력합니다. 만일 인증서를 발행한 상위기관의 인증서가 있을 경우에는 CACertificatePath, CACertificateFile 값도 설정합니다.

```
*DOMAIN
Webtob1
....

*VHOST
vhost1 DOCROOT="/data1/htdocs/webdocs",
        NODENAME ="www3",
        HOSTNAME ="www.dhckorea.com", (인증키 신청 시 요청한    domain)
        PORT ="443",
        IndexName = "index.html",
        SSLFLAG = Y,
```

```
        SSLNAME ="ssl1“

*SSL
Ssl1 CertificateFile="/data1/tmax/webtob/ssl/newreq.pem",
     CertificateKeyFile="/data1/tmax/webtob/ssl/newreq.pem",

     CACertificatePath="/data1/tmax/webtob/ssl/",
     CACertificateFile="/data1/tmax/webtob/ssl/intermediate.pem",

     RandomFile="/data1/tmax/webtob/bin/.rnd, 2048",
     RandomFilePerConnection="/data1/tmax/webtob/bin/.rnd, 512",
     VerifyClient= 0,
     VerifyDepth= 10,
     FakeBasicAuth= Y
     ..........
```

http.m 파일을 수정한 후 설정을 적용하기 위해서는 아래 명령어 및 방법을 통하여 확인할 수 있습니다.

▶ 적용 및 확인 방법 방법

확인 사항	방 법
http.m compile	- wscfl –i http.m
webtob service 기동	- wsboot / wsdown –i; wsboot
service 확인	IE를 실행시켜 주소창에서 “Https://” 및 해당 URL을 입력하여 접속함

11. Tomcat CSR 생성하기

Tomcat을 웹서버로 사용할 경우 RSA용 키쌍을 생성하고 생성된 키쌍을 이용하여 CSR 파일을 생성합니다.

Keytool 명령어는 java 명령어로 jdk 가 설치된 디렉토리에서 실행가능합니다. (JAVA_HOME₩BIN 디렉토리가 PATH에 잡혀있을 경우 어디에서도 실행 가능합니다)

▶ 키생성 방법

인증서에 필요한 RSA 키쌍을 생성하고 관련 정보를 키저장소에 저장합니다.

명령어	keytool -genkey -alias tomcat -keyalg RSA ₩ -keystore <your_keystore_filename>
결 과	<your_keystore_filename> 파일이 생성됩니다.

키를 생성시 개인키를 암호화할 암호, 조직단위, 조직명, 시/도 이름, 국가 등에 대한 정보를 입력받아 정보를 저장합니다.

▶ keytool에서 개인키 생성 시 입력 사항

속 성	설 명	예
Keystore 암호를 입력하십시요	keystore 암호	sslserver
이름과 성을 입력하십시요	이름과 성 이름	www.ktnet.co.kr
조직단위 이름을 입력하세요	조직 단위 이름	IT
구/군/시 이름을 입력하세요	구/군/시 이름	Samsung-dong
시/도 이름을 입력하세요	시/도 이름	Seoul
이 조직의 두자리 국가코드를 입력하세요.	국가 코드	KR
입력 정보 출력	입력 정보 확인	yes
키암호를 입력하세요.	<mykey> 암호	비밀번호 입력

▶ CSR 생성 방법

생성된 키를 이용하여 CSR 파일을 생성합니다.

명령어	keytool -certreq -keyalg RSA -alias tomcat -file certreq.csr ₩ -keystore <your_keystore_filename>
결 과	CSR 파일이 certreq.csr 파일에 생성됩니다.

생성된 CSR 파일을 인증기관으로 전송하여 인증서를 발급 받습니다.

Tomcat에 인증서 설치하기

발급받은 인증서를 서버에 설치하기 위해서는 keytool 이라는 명령어를 통하여 저장소에 import 시킵니다. 이와함께 server.xml 파일을 수정하여 SSL 설정을 완성합니다.

▶ 키 import 방법

인증서의 chain 이 있을 경우 아래의 keytool 명령어를 이용하여 순서대로 인증서를 import 하여야 합니다. (Root 인증서를 먼저 import 하고, 새로 발급 받은 인증서를 마지막에 import 하여야 함)

명령어	keytool -import -alias tomcat -keystore <your_keystore_filename> -trustcacerts -file <your_certificate_filename>
결 과	<your_keystore_filename> 안에 인증서가 keystore 형식에 맞춰 import 됩니다.

▶ server.xml 파일 변경

server.xml 파일을 열어서 아래와 같이 keystoreFile 변수의 값을 입력하고 키를 생성할 때 입력한 passphrase 값을 함께 입력합니다.

```
.....
<!-- Define an SSL HTTP/1.1 Connector on port 443 -->

<Connector className="org.apache.catalina.connector.http.HttpConnector"
        port="443" minProcessors="5" maxProcessors="75"
        enableLookups="true"
        acceptCount="10" debug="0" scheme="https" secure="true">
<Factory className="org.apache.catalina.net.SSLServerSocketFactory"
        keystoreFile="C:₩Program Files₩Apache Tomcat 4.0₩conf₩
                key₩www.ktnet.co.kr.keystore" keystorePass="sslserver"
        clientAuth="false" protocol="TLS"/>
</Connector>
.....
```

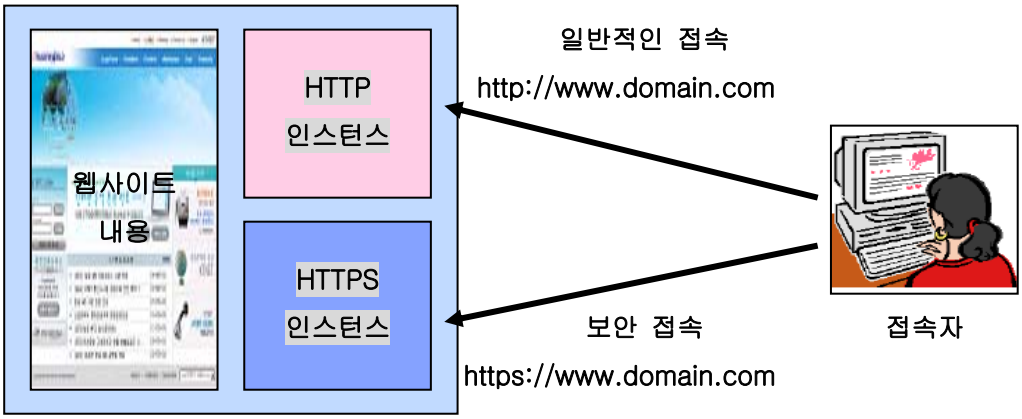
keystoreFile 항목은 CSR파일 생성시 작성한 keystore파일의 위치 및 path를 입력하고, keystorePass 항목은 개인키 생성시 입력한 패스워드를 입력합니다.

제 3 장 보안서버 설치의 마무리-웹페이지 수정

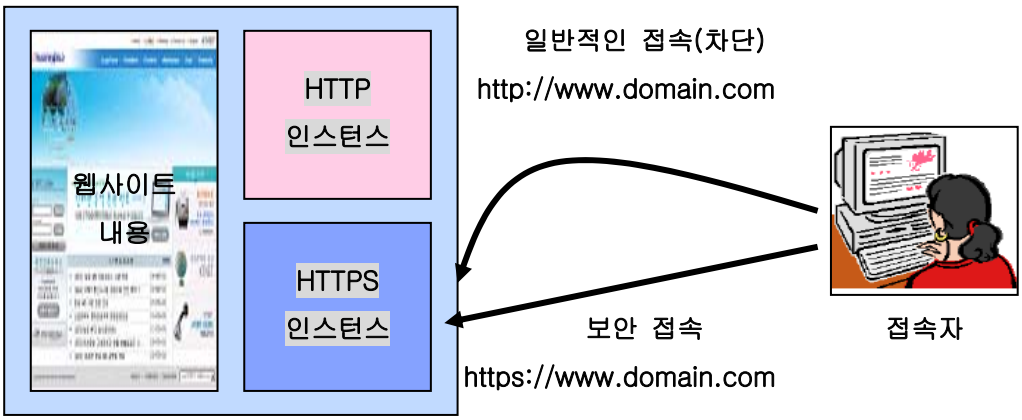
12. 웹사이트 전체에 보안서버 적용하기

본 문서는 웹서버에 보안서버 인증서의 설치가 완료되었으며 HTTPS 프로토콜로 접속이 가능하다는 전제하에 작성되었습니다. 아직 보안서버의 개념을 모르시거나 보안서버 인증서를 설치하지 않은 분들은 보안서버구축가이드(시작) 편을 참고 하십시오.

보안서버가 정상적으로 구축이 되었으면 다음과 같이 웹서버에 2개의 인스턴스가 동작하게 됩니다. 첫번째는 기존의 HTTP (80 포트로 서비스), 두번째는 새로운 HTTPS (443 포트로 서비스) 되는 인스턴스입니다.



접속자가 의도적으로 HTTPS 프로토콜로 접속하지 않는 이상 이 사이트는 안전하다고 할 수 없습니다. 따라서 기존의 HTTP 프로토콜 접속을 의도적으로 HTTPS 로 리다이렉트 (redirect) 할 필요가 있습니다. 리다이렉트 하는 방법은 다음과 같습니다.



1) 보안서버 웹페이지 리다이렉트 하기

< 웹서버 환경설정 변경하기 – 아파치 웹서버 httpd.conf 환경설정 수정 >

```
<VirtualHost   www.test.co.kr:80>
  ServerName www.test.co.kr
  ServerAdmin webmaster@ec21.com
  DocumentRoot /home2/kcat/html
  ErrorLog   "|/usr/local/apache/bin/rotatelogs.new   /var/log/http/www.kcat.co.kr-
  error_log 86400"
  Redirect / https://www.test.co.kr /
</VirtualHost>
```

HTTP 접속을 HTTPS 로 redirect

< HTML 태그를 이용한 보안서버 리다이렉트 >

초기 웹페이지에 아래 코드를 삽입함으로써 보안서버로 리다이렉트할 수 있다.

```
<meta http-equiv='refresh' content='0; url=https://www.test.co.kr/index.html">
```

이 때 중요한 것은 초기 웹페이지와 리다이렉트 되는 웹페이지가 서로 달라야 한다. 만일 동일한 웹페이지라면 무한정 리다이렉트가 발생할 것이다.

meta 태그와 동일한 효과를 나타내는 javascript 함수를 사용할 수도 있다.

```
<script>window.location.replace(https://www.test.co.kr/index.html);</script>
```

2) 플래쉬 소스코드 수정하기

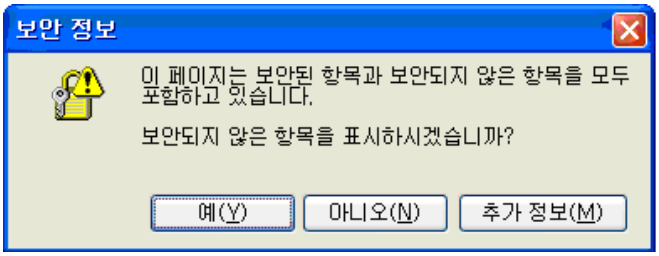
가. 객체를 HTTP 로 호출하는 부분 수정

플래쉬 기술이 적용된 웹페이지는 공통적으로 macromedia 웹사이트의 객체를 호출하는 소스를 포함하고 있다.

```
codebase="http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab#
version=6,0,29,0"
```

HTTP 방식으로 객체를 호출하고 있음

이 코드를 수정하지 않고 보안서버를 적용하면 "이 페이지는 보안된 **항목**과 **보안되지 않은 항목을** 모두 포함하고 있습니다. **보안되지 않은 항목을** 표시하시겠습니까" 라는 메시지가 뜨게 된다. 즉 보안되지 않은 항목이란 "플래쉬 객체"를 뜻하는 것이다.



이 메시지가 뜨지 않게 하려면 다음과 같이 수정하면 된다.

```
codebase="https://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab
#version=6,0,29,0"
```

HTTP 를 HTTPS 로 변경

나. 플래쉬 자체에서 링크되어 있는 절대경로 수정

HTML 소스코드가 아닌 플래쉬 자체에서 링크되어 있는 페이지가 있다. 이 링크가 상대경로라면 상관이 없으나 다음과 같이 절대경로인 경우, 보안되지 않는 페이지로 빠져나올 수 있으므로 수정하여야 한다.

2) 플래쉬에서 절대경로로 링크되어 있는 부분을 상대경로로 바꾸어 준다.

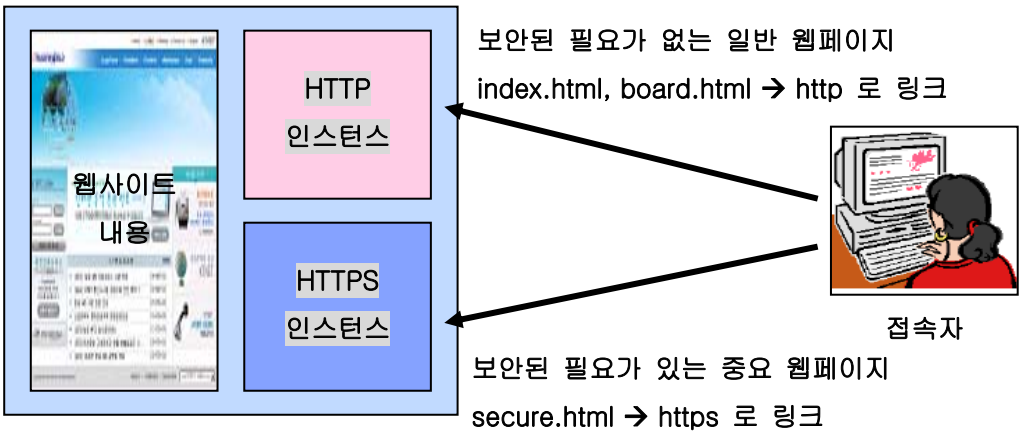
예) 어떤 플래쉬에서 http://www.domain.co.kr/guideline/index.html 등으로 링크가 되어 있으면 안되므로 /guideline/index.html 으로 링크를 바꾸어 준다.

13. 웹사이트 일부에 보안서버 적용하기

보안서버가 적용된 웹서버는 데이터의 암호화/복호화 처리를 위해 더 많은 CPU 점유율을 나타낸다. 이것은 웹서버 내의 모든 콘텐츠(글자, 그림, 동영상 등) 가 암호화 되기 때문이며 이를 해결하기 위해 일부 웹페이지 또는 일부 정보만 암호화할 수도 있다. 단 이렇게 하기 위해서는 웹페이지 소스코드의 수정이 불가피하며 경우에 따라 추가 개발이 필요하기도 한다.

가. 페이지별 암호화하기

페이지별 암호화의 원리는 HTTP 와 HTTPS 인스턴스가 동시에 서비스되고 있는 웹서버에서 암호화할 필요가 있는 페이지의 링크만 HTTPS 로 수정하는 것이다. 웹 사이트 내의 모든 링크를 찾아서 변경해야 하므로 다소 작업량이 많을 수 있다.



< 이미지 맵이 설정된 경우의 선택적 암호화 적용 >

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

첫번째 빨간색은 암호화 통신 페이지로 두번째 빨간색은 평문 페이지로 이동을 하게 됩니다.

나. 프레임별 암호화하기

프레임이 적용된 페이지를 이용하면 암호화된 페이지와 비 암호화된 페이지를 각각 적용시킬 수 있습니다. Index.html에 topmenu.htm 과 main.html의 두개의 프레임이 있다고 가정할 때 예를 듭니다.

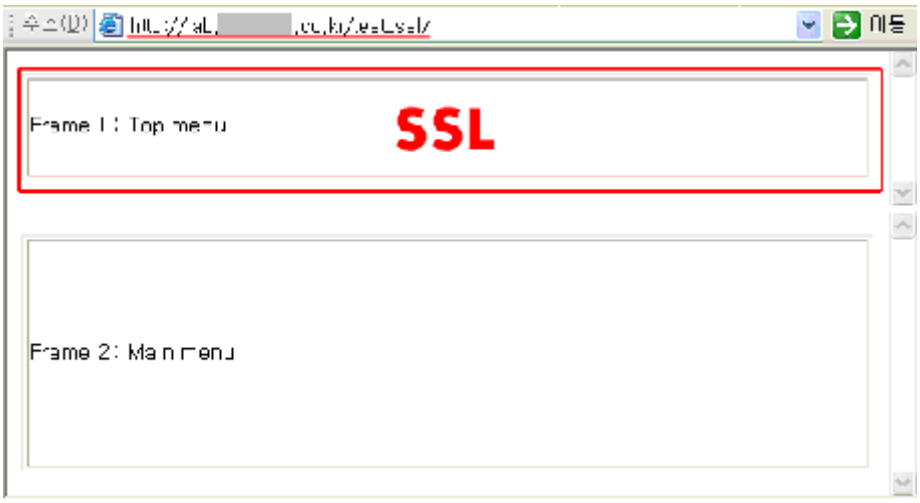
```
<html>

<head>
<meta http-equiv="content-type" content="text/html; charset=euc-kr">
<title>SSL Frame Test</title>
</head>
<frameset rows="100,*" border="1">
   <frame src="http://lab.[redacted].co.kr/test_ssl/topmenu.htm" scrol
ling="yes" name="top" namo_target_frame="main">
    <frame src="http://lab.[redacted].co.kr/test_ssl/main.htm" scrolli
ng="yes" name="main">
    <noframes>
    <body bgcolor="white" text="black" link="blue" vlink="purple" ali
nk="red">
    <p>SSL Frame Test의 페이지 입니다. <br> 이페이지를 보기 위해서는
       프레임을 볼수 있는 웹 브라우저가 필요합니다.</p>
    </body>
    </noframes>
</frameset>

</html>
```

두개의 프레임이 각각 다른 웹페이지를 참조하고 있으며 필요에 따라 https 링크를 걸어줌으로써 선택적인 암호화가 가능하다.

예) 한 개의 http:// 프레임과 한 개의 https:// 프레임을 포함한 html script 결과



다. 체크박스를 이용하여 선택적으로 ID/PW 만 암호화하기

웹 페이지 전체를 암호화하지 않고 선별적으로 암호화하는 경우, 정보 입력시 보안접속을 체크함으로써 프로토콜을 호출하는 방법이 있습니다. 다음은 로그인 박스에서 선별적으로 암호화된 통신을 하기 위한 HTML 소스예 입니다.


```
<script language="JavaScript">
< !--
function checkLoginForm1() {
var f = document.forms["LoginForm1"];
//아이디 입력 검사
if( f.memberID.value=="" ){
alert("아이디를 입력하세요");
f.memberID.focus();
return false;
}
//비밀번호 입력 검사
if( f.memberPW.value=="" ){
alert("비밀번호를 입력하세요");
f.memberPW.focus();
return false;
}
```

```
<script language="JavaScript">
<!--
function checkLoginForm2() {
var f = document.forms["LoginForm2"];
//아이디 입력 검사
if( f.memberID.value=="" ){
alert("아이디를 입력하세요");
f.memberID.focus();
return false;
}
//비밀번호 입력 검사
if( f.memberPW.value=="" ){
alert("비밀번호를 입력하세요");
f.memberPW.focus();
return false;
}
```

```
//액션
f.action = "h
http://login.your-domain.com/login1.html;
return true;
}
//-->
< /script>
< form name="Logi
onSubmit="return c
< table>
<tr>
<td>아이디</td>
<td><input type="text"
name="memberID"></td>
<td> </td>
</tr>
<tr>
<td>비밀번호</td>
<td><input type="password"
name="memberPW"></td>
<td><input type="submit" name="Submit"
value=" 로그인 "></td>
</tr>
< /table>

< /form>
```

```
//액션
if ( f.SSL_Login.checked ) { //보안접속 체크
판별
//보안접속을 체크했을 때의 액션
f.action =
"https://login.your-domain.com/login1.html";
} else {
}
return true;
}
//-->
</script>
<form name="LoginForm2" method="POST"
onSubmit="return checkLoginForm2();">
<table>
<tr>
<td>아이디</td>
<td><input type="text"
name="memberID"></td>
<td><input type="checkbox" value=1
checkedname="SSL_Login" >보안접속</td>
</tr>
<tr>
<td>비밀번호</td>
<td><input type="password"
name="memberPW"></td>
<td><input type="submit" name="Submit"
value=" 로그인 "></td>
</tr>
</table>
</form>
※ SSL 을 이용한 암호화된 폼 전송을 하려면,
action URL 에서 'http' 대신 'https'를

적어 주면 됩니다.
```

보안접속을 체크했을 때 action 을 https 로 변경한다.

공인인증서비스 신청서(보안서버 SSL 인증서)

신청정보

상 호	한글		사업자등록번호		
	영문		대표자 성명		
사업장 주소(한글)					우편번호)
사업장 주소(영문)					PostCode)
웹서버운영자 (인증서관리자) 정보	성 명		부 서		
	e-mail		팩 스		
	전 화		휴대전화		
인증서 종류	- 기본형 : 웹서버 1대의 1개 도메인에 인증서 설치 (예:www.ktnet.com) - 서브도메인형 : 웹서버 1대에 여러 개의 가상 호스트가 운영 중이며 각각에 2차(서브)도메인이 지정되어 있는 경우 (예:*.ktnet.com) - 멀티도메인형 : 웹서버 1대에 여러 개의 가상 호스트가 운영 중이며 각각에 서로 독립적인 도메인이 지정되어 있는 경우 (www.ktnet.com, www.ktnet2.co.kr …)				
	기본형	신청갯수: 개	이용기간 : □1년, □2년, □3년		
	서브도메인형	신청갯수: 개	이용기간 : □1년, □2년, □3년		
	멀티도메인형	신청갯수: 개	이용기간 : □1년		
신청내용	□신규발급 □재발급 □갱신				
재발급사유	□웹서버이전 □인증서분실 □도메인(DN) 변경 □기타사유 ( )				

전자서명법 제15조 및 ㈜한국무역정보통신의 공인인증서비스 이용 약관에 따라 상기와 같이 공인인증서비스를 신청하오며, 본 신청서의 신청내용을 공인인증 서비스 관련업무에 활용함을 동의합니다.

년 월 일

업체명 : _____ (인) (개인인감/법인인감)

인증기관 : **㈜한국무역정보통신**

◇ 준비서류

①공인인증서비스 신청서 ②사업자등록증 사본

◇ 발급절차

①신청서류 및 CSR 정보 전달 (☏02-6000-2093, FAX:02-6000-2093) ② 인증서파일 EMAIL 송부 ③ 웹서버에 인증서 설치 및 재기동

<table>
<tr><td>웹서버 정보</td><td colspan="2"></td></tr>
<tr><td>웹서버 종류</td><td colspan="2">☐ Apache-ModSSL
☐ Apache-SSL (Ben-SSL, not Stronghold)
☐ Java Web Server (Javasoft / Sun)
☐ Microsoft IIS 1.x to 4.x
☐ Microsoft IIS 5.x and later
☐ RedHat Linux
☐ Tomcat
☐ Zeus Web Server</td></tr>
<tr><td rowspan="4">웹서버 도메인</td><td>☐ 기본형</td><td>도메인 :
예) www.ktnet.com</td></tr>
<tr><td>☐ 서브(2차)도메인형</td><td>도메인 :
예) *.ktnet.com</td></tr>
<tr><td colspan="2">☐ 멀티도메인형 (가상 호스트에 할당된 개별적인 도메인을 모두 기재)
예) erp.ktnet.com www.ktnet.com www.ktnet.net</td></tr>
<tr><td colspan="2"></td></tr>
<tr><td rowspan="3">CSR
(인증서 요청정보)</td><td colspan="2">생성시각 : 년 월 일</td></tr>
<tr><td colspan="2">주 의
1) CSR은 1K~3K bytes 의 텍스트 정보이며 웹서버별로 생성하는 방법은 별도의 매뉴얼 참고하십시오. (http://ssl.tradesign.net)
2) CSR 생성시 입력하는 CN(Common Name)은 신청서 상의 도메인과 동일하여야 하고 특히 서브도메인인증서의 경우 *.도메인명 의 형태이어야 합니다.
3) CSR 정보는 나중에 생성해서 별도 전달해 주셔도 됩니다.
참고 → http://ssl.tradesign.net</td></tr>
<tr><td colspan="2"></td></tr>
</table>

※ 추가 CSR 은 본 페이지 양식을 활용하여 추가 제출하여 주십시오.

(작성예) 인증서비스 신청서(보안서버 SSL 인증서)

신청정보

상 호	한글	가나정보통신	사업자등록번호	120-81-11111	
	영문	gana systems	대표자 성명	홍길동	
사업장 주소(한글)		서울 강남구 삼성동 159-1 트레이드타워 11층			우편번호) 135-729
사업장 주소(영문)		www.etpost.co.kr/service/zipcode/zip_eng.php?mod=h 에서 주소 검색			PostCode) 135-729
웹서버운영자 (인증서관리자) 정보	성 명	연흥부	부 서	IT개발팀	
	e-mail	gaga@gaga.com	팩 스	02-6000-2086	
	전 화	02-6000-2093	휴대전화	011-1111-2222	
인증서 종류	- 기본형 : 웹서버 1대의 1개 도메인에 인증서 설치 (예:www.ktnet.com) - 서브도메인형 : 웹서버 1대에 여러 개의 가상 호스트가 운영 중이며 각각에 2차(서브)도메인이 지정되어 있는 경우 (예:*.ktnet.com) - 멀티도메인형 : 웹서버 1대에 여러 개의 가상 호스트가 운영 중이며 각각에 서로 독립적인 도메인이 지정되어 있는 경우 (www.ktnet.com, www.ktnet2.co.kr …)				
	기본형	신청갯수: 1 개		이용기간 : ■1년, □2년, □3년	
	서브도메인형	신청갯수: 1 개		이용기간 : ■1년, □2년, □3년	
	멀티도메인형	신청갯수: 개		이용기간 : □1년	
신청내용	■신규발급 □재발급 □갱신				
재발급사유	□웹서버이전 □인증서분실 □도메인(DN) 변경 □기타사유 ( )				

전자서명법 제15조 및 ㈜한국무역정보통신의 공인인증서비스 이용 약관에 따라 상기와 같이 공인인증서비스를 신청하오며, 본 신청서의 신청내용을 공인인증 서비스 관련업무에 활용함을 동의합니다.

년 월 일

업체명 : ㈜가나정보통신 (인) (개인인감/법인인감)

인증기관 : **㈜한국무역정보통신**

◇ 준비서류

①공인인증서비스 신청서 ②사업자등록증 사본

◇ 발급절차

①신청서류 및 CSR 정보 전달 (☏02-6000-2093, FAX:02-6000-2093) ② 인증서파일 EMAIL 송부 ③ 웹서버에 인증서 설치 및 재기동

웹서버 정보	
웹서버 종류	■ Apache-ModSSL ☐ Apache-SSL (Ben-SSL, not Stronghold) ☐ Java Web Server (Javasoft / Sun) ☐ Microsoft IIS 1.x to 4.x ☐ Microsoft IIS 5.x and later ☐ RedHat Linux ☐ Tomcat ☐ Zeus Web Server
웹서버 도메인	■ 기본형 / 도메인 : www.tradesign.net ■ 서브(2차)도메인형 / 도메인 : *.ktnet.com ☐ 멀티도메인형 (가상 호스트에 할당된 개별적인 도메인을 모두 기재) 예) erp.ktnet.com www.ktnet.com www.ktnet.net
CSR (인증서 요청정보)	생성시각 : 년 월 일 **주 의** 1) CSR은 1K~3K bytes 의 텍스트 정보이며 웹서버별로 생성하는 방법은 별도의 매뉴얼 참고하십시오. (http://ssl.tradesign.net) 2) CSR 생성시 입력하는 CN(Common Name)은 신청서 상의 도메인과 동일하여야 하고 **특히 서브도메인인증서의 경우 *.도메인명 의 형태이어야 합니다.** 3) CSR 정보는 나중에 생성해서 별도 전달해 주셔도 됩니다. 참고 → http://ssl.tradesign.net

-----BEGIN NEW CERTIFICATE REQUEST-----
MIIDQTCCAqoCAQAwZjELMAkGA1UEBhMCS1IxDjAMBgNVBAgTBVNlb3VsMQ4wDAYD
VQQHEwVTZW91bDEOMAwGA1UEChMFS1RORVQxCzAJBgNVBAsTAklUMRowGAYDVQQD
ExF3d3cudHJhZGVzaWduLm5ldDCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA
u6bgeC6/SclLkT5twPtTVLuUSTG6ynzJO/kLRhqHkwnvSNJ4T4QvFp4sXkpY3zmV
ftg/GU6TM5U321xfoB41ogtXhX5+C/P00RQ4w46yhJMiJ22hAR4Ue2alxzVIfHAg
KY06mYNga0h//hiRMoZ666KYFd9ugY4mrEvDLiVV+ukCAwEAAaCCAZkwGgYKKwYB
BAGCNw0CAzEMFgo1LjIuMzc5MC4yMHsGCisGAQQBgjcCAQ4xbTBrMA4GA1UdDwEB
/wQEAwIE8DBEBgkqhkiG9w0BCQ8ENzA1MA4GCCqGSIb3DQMCAgIAgDAOBggqhkiG
9w0DBAICAIAwBwYFKw4DAgcwCgYIKoZIhvcNAwcwEwYDVR0lBAwwCgYIKwYBBQUH
AwEwgf0GCisGAQQBgjcNAgIxge4wgesCAQEeWgBNAGkAYwByAG8AcwBvAGYAdAAg
AFIAUwBBACAAUwBDAGgAYQBuAG4AZQBsACAAQwByAHkAcAB0AG8AZwByAGEAcABo
AGkAYwAgAFAAcgBvAHYAaQBkAGUAcgOBiQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAMA0GCSqGSIb3DQEBBQUAA4GBAJTpwIN0PNyn2yVO
7FWFz7CP+LM8jopb7iZ3yZF/eR1pEZkai5emQiF7u6kTny9nH29cr0UFstGTxFqd
U9+Uk88xCDS69f2oHXh3ke8XLsVYGYtCbQkLNBoVAd3BqiPOFMyaOLvbJWU64p5J
ZS5Rp6mQekiug87ByP2j0v4kJRG4
-----END NEW CERTIFICATE REQUEST-----

※ 추가 CSR 은 본 페이지 양식을 활용하여 추가 제출하여 주십시오.

" IT강국 기반으로 선진한국 도약 "

정 보 통 신 부

수신자 한국정보보호진흥원장
(경유)
제목 보안서버 구축 안내 협조 요청

1. 귀 원의 무궁한 발전을 기원합니다.

2. 관련
가. 제43회 국무회의 보고(2006.9.27, 개인정보보호를 위한 보안서버 보급 확대)
나.「정보통신망 이용촉진 및 정보보호 등에 관한 법률」제28조(개인정보의 보호조치), 동법 시행규칙 제3조의2(개인정보의 보호조치), 동법 67조(과태료)

3. 최근 인터넷상 개인정보보호 강화를 위해 실시한 보안서버의 보급실태 조사 결과, 주민등록번호 등 개인정보를 취급하는 정보통신서비스제공자 웹사이트에서 보안서버 도입이 저조한 것으로 파악되었습니다.

4. 보안서버는 인터넷상에서 개인정보 전송시 암호화하는 기능을 제공하는 서버로서 개인정보를 취급하는 기관 및 사업자가 개인정보 보호를 위해 기초적으로 갖추어야 할 수단으로, 제43회 국무회의시 보안서버 도입 추진 결정에 따라 정보통신부는 민간부문 보급을 추진하고 관련 법률에 따라 미구축 사업자에 대한 과태료 부과 등 행정조치를 실시할 계획입니다.

5. 이에 귀 원에서는 웹사이트에서 개인정보를 취급하는 사업자가 조속히 보안서버를 구축할 수 있도록 붙임의 '보안서버 구축 안내문'을 활용하여 보안서버 도입 필요성, 관련 법령 등을 적극 홍보하여 주시기 바랍니다.

붙임 보안서버 구축 안내문 1부. 끝.

한국정보보호진흥원

수신자 보안서버 미구축 웹사이트 운영 사업자

고유 번호 : DXXXX 사이트 주소 : www.XXXXXX.co.kr

제 목 개인정보보호를 위한 보안서버 미구축 개선권고

---

1. 우리 원은 「정보통신망이용촉진및정보보호등에관한법률」 제55조 및 제56조제3항에 의거하여 정보통신서비스제공자 등의 개인정보보호에 대한 기술적·관리적 조치 실태조사를 담당하고 있습니다.

2. 인터넷상에서 아이디/패스워드, 연락처 등 개인정보를 수집 활용하는 정보통신서비스제공자는 고객의 개인정보를 보호하기 위해 의무적으로 보안서버를 구축해야 합니다.

3. 우리 원에서 2007.4.23(월)~30(월)까지 수행한 보안서버 구축 실태조사 결과, 귀사에서 운영하는 웹사이트에 보안서버가 구축되지 않은 것으로 나타났습니다. 이에 따라 향후 1천만원 이하의 과태료 부과 등 행정조치가 수반될 수 있으므로 조속한 개선 조치와 함께 아래와 같이 관련 문서를 제출하여 주시기 바랍니다.

4. 관련 근거

o 「정보통신망이용촉진및정보보호등에관한법률」 제28조(개인정보의 보호조치), 동법 시행규칙 제3조의2(개인정보의 보호조치), 동법 67조(과태료)

- 아 래 -

가. 제출 문서

o 보안서버 구축 예정 및 완료시 : 「보안서버 구축 계획(확인)서」 (붙임1)

o 보안서버 구축 대상자가 아닐 경우 : 「보안서버 구축 이의 신청서」 (붙임2)

나. 제출기한 : 2007.5.31(목) (답변서 제출기한)

다. 제출처 및 문의

o 보안서버 사무국 E-mail : secureserver@kisa.or.kr, 전화 : 02-405-4791

※ 접수는 E-mail을 통해서 받으며 수신 확인메일을 발송해 드립니다.

라. 주의 사항

o 보안서버 구축 완료 기한은 2007.7.31(화)입니다.

※ 기한 내에 필히 구축을 완료하여 주시기 바라며, 구축 후 결과를 통보하여 주시기 바랍니다.

o 실태조사에 사용되는 자동 점검 도구의 기능은 일반 사용자의 웹페이지 검색을 자동화한 것이나, 일부 보안장비에서 이를 악의적인 스캐닝으로 오인할 수 있습니다. 전화 및 이메일로 문의하시면 점검 일시를 확인해 드리도록 하겠습니다.

붙임 1. 보안서버 구축 계획(확인)서 1부 2. 보안서버 구축 이의 신청서 1부. 끝.

※ 보안서버 구축과 관련한 자세한 내용은 한국정보보호진흥원 홈페이지(www.kisa.or.kr)에 게재된 「보안서버 구축 가이드」와 「보안서버 자진등록」을 참조하시기 바랍니다.