

대한민국 E-Business 대표 브랜드

# ITEASY

## Nginx

# 보안인증서 가이드

- ISMS(정보보호 관리체계) 인증 획득
- 일자리 창출 유공 정부포상 국무총리 표창
- 클라우드 산업발전 유공 과학기술통신부 장관 표창
- 9년 연속 랭키닷컴 IDC/클라우드 분야 1위
- 스마트시티 SOC-ICT 우수기업 과학기술정보통신부 장관 표창
- 최대 10억원 배상책임보험 가입
- 5년 연속 한국소비자만족지수 1위
- 한국인터넷진흥원 선정 고객만족도 우수기업



It is easy,  
IT is easy!

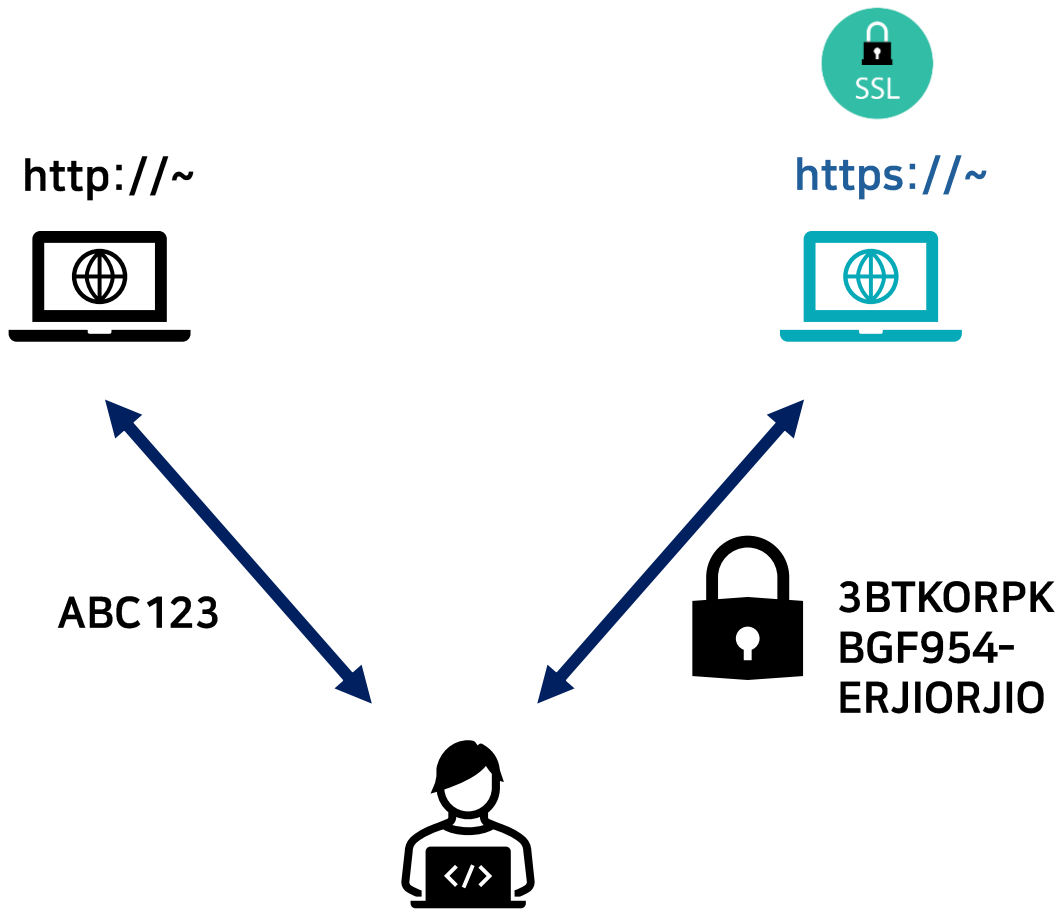
## CONTENTS

1. 보안인증서(SSL)
2. 신청 및 진행 절차
3. 설치방법

## 1. 보안인증서(SSL)

SSL 보안 인증서는 웹 서버와 클라이언트 간의 데이터 통신을 암호화하여, 데이터의 기밀성과 무결성을 보장하는 디지털 인증서입니다.

SSL 인증서를 사용하면 사용자와 서버 간의 정보가 암호화되어, 외부의 도청, 변조, 스니핑 등의 위협으로부터 소중한 데이터를 보호할 수 있습니다.



**http는 쉽게 볼 수 있지만,  
https는 암호화되어 볼 수 없어!**

## 2. 신청 및 진행절차

### (1) 고객 SSL 인증서 신청 접수

- 고객이 SSL 인증서를 신청합니다.
- 작성정보 : 도메인, 웹서버 종류, SSL 신청업체 정보
- SSL 신청 및 결제 후 작업의뢰 또는 서비스 문의 접수 시 발급이 진행됩니다.
- 아이티이지 SSL 페이지 : <https://www.iteasy.co.kr/sec/ssl>

### (2) 도메인 소유권 인증

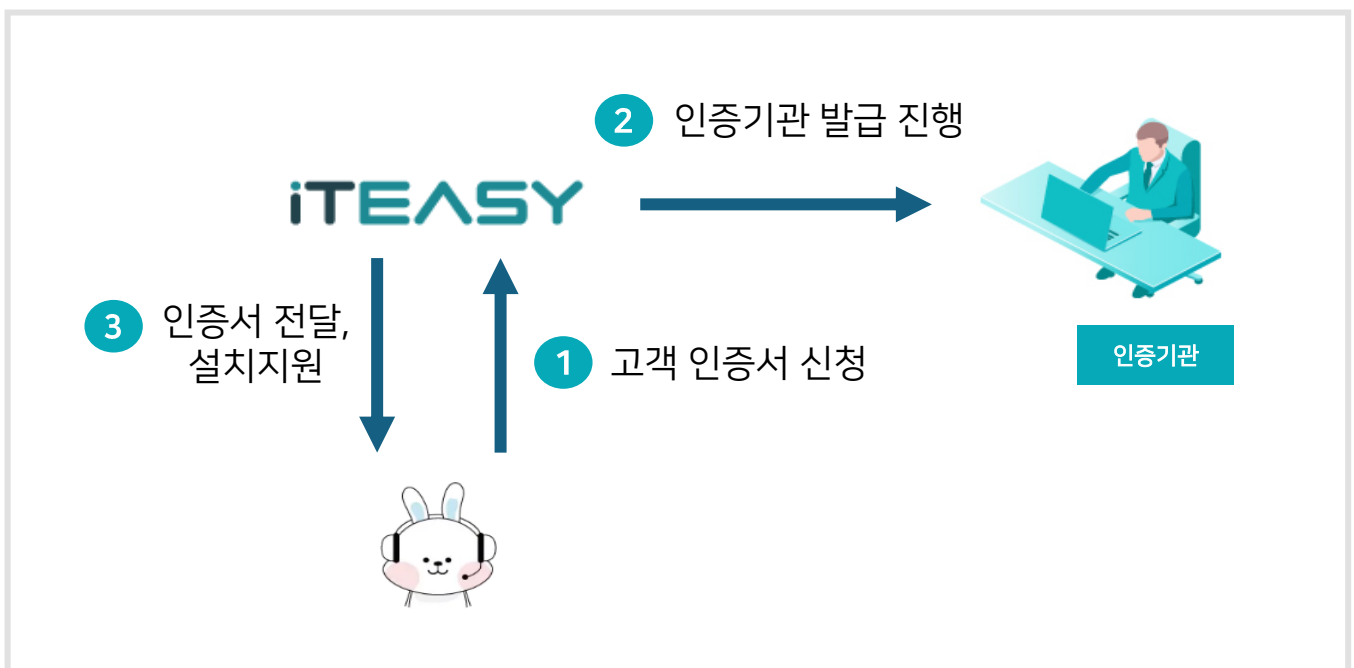
- 도메인에 대한 소유권을 확인하기 위해 인증을 진행 합니다.  
도메인 소유권 인증 방법 - 메타태그 [HTTP, HTTPS], DNS, 이메일

### (3) 인증서 발급 진행

- 신청하신 웹 서버에 맞는 형식으로 SSL 인증서를 발급 합니다.

### (4) 인증서 전달 및 설치 지원

- 발급된 인증서는 고객에게 전달 합니다.  
전달 파일 (예) Apache - CRT , CA , KEY / Nginx - CRT , KEY / Tomcat - JKS
- 직접 설치가 어려우신 경우 자사 전문 엔지니어를 통해 지원을 받을 수 있습니다.



### 3. 안내사항 및 설치 순서

#### ▷ 설치 전 안내사항

- 본 가이드는 기본적인 참고용 자료로, 사용자 환경에 따라 일부 내용이 다를 수 있습니다.
- 이 내용에 안내된 버전 외 다른 버전을 사용 중일 경우, 기재된 설정이 다를 수 있습니다. 사용 중인 버전에 맞는 적절한 설정 방법을 확인해주세요.
- 설정이나 작업 진행에 어려움이 있을 경우, 전문적인 기술 지원을 요청하는 것을 권장드립니다. 작업 의뢰를 통해 더 정확하고 안전한 설정이 가능합니다.

#### ▷ 설치 테스트 환경

- OS : Rocky 9.3
- Nginx : 1.20.1 (패키지 설치)
- Nginx는 OpenSSL을 사용하여 암호화를 처리합니다. OpenSSL이 미 설치된 경우 설치를 진행합니다.
- openssl 확인 : `nginx -V`

built with OpenSSL : Nginx가 빌드될 때 사용된 OpenSSL 버전

```
[root@root ~]# nginx -V
nginx version: nginx/1.20.1
built by gcc 11.5.0 20240719 (Red Hat 11.5.0-2) (GCC)
built with OpenSSL 3.2.2 4 Jun 2024 (running with OpenSSL 3.0.7 1 Nov 2022)
TLS SNI support enabled
```

- `ngx_httpd_ssl_module` 활성화 확인 : `nginx -V`
  - \* Nginx (패키지) - `ngx_httpd_ssl_module` 은 포함되어 있습니다.
  - \* Nginx (컴파일) - 컴파일 시 `--with-http_ssl_module` 옵션을 명시적으로 추가해야 합니다.

```
configure arguments: --prefix=/usr/share/nginx --sbin-path=/usr/sbin/nginx --modules-path=/usr/lib64/nginx/modules --conf-path=/etc/nginx/nginx.conf -
error-log-path=/var/log/nginx/error.log --http-log-path=/var/log/nginx/access.log --http-client-body-temp-path=/var/lib/nginx/tmp/client_body --http-
proxy-temp-path=/var/lib/nginx/tmp/proxy --http-fastcgi-temp-path=/var/lib/nginx/tmp/fastcgi --http-uwsgi-temp-path=/var/lib/nginx/tmp/uwsgi --http-sc
gi-temp-path=/var/lib/nginx/tmp/scgi --pid-path=/run/nginx.pid --lock-path=/run/lock/subsys/nginx --user=nginx --group=nginx --with-compat --with-debu
g --with-file-aio --with-http_addition_module --with-http_auth_request_module --with-http_dav_module --with-http_degradation_module --with-http_flv_mo
dule --with-http_gunzip_module --with-http_gzip_static_module --with-http_image_filter_module=dynamic --with-http_mp4_module --with-http_perl_module=dynamic --with-http_random_index_module --with-http_realip_module --with-http_secure_link_module --with-http_slice_module --with-http_ssl_module --with-http_stub_status_module --with-http_sub_module --with-http_v2_module --with-http_xslt_module=dynamic --with-mail=dynamic --with-mail_ssl_module --with-http_perl_module=dynamic --with-pcre-jit --with-stream=dynamic --with-stream_ssl_module --with-stream_ssl_preread_module --with-threads --with-cc-opt='-O2 -flto=auto -fat-lto-objects -fexceptions -g -grecord-gcc-switches -pipe -Wall -Werror=format-security -Wp,-D_FORTIFY_SOURCE=2 -Wp,-D_GLIBCXX_ASSERTIONS -specs=/usr/lib/rpm/redhat/redhat-hardened-cc1 -fstack-protector-strong -specs=/usr/lib/rpm/redhat/redhat-annobin-cc1 -m64 -march=x86-64-v2 -mtune=generic -fasynchronous-unwind-tables -fstack-clash-protection -fcf-protection' --with-ld-opt='-Wl,-z,relro -Wl,-z,now -Wl,-z,now -specs=/usr/lib/rpm/redhat/redhat-hardened-ld -specs=/usr/lib/rpm/redhat/redhat-annobin-cc1 -Wl,-E'
```

### 3. 안내사항 및 설치 순서

#### ▷ 설치 순서

##### (1) 인증서 파일을 서버에 저장

###### [인증서 파일]

- CRT(Certificate, 인증서)

인증서의 본문을 포함하며 사이트나 서버의 고유한 신원 정보를 암호화하여 담고 있습니다.

- KEY (Private Key, 개인 키)

서버 소유자가 보유한 비밀 키로 서버의 암호화된 데이터 복호화 및 서명 생성에 사용됩니다.

##### (2) nginx.conf수정

- 설정하기 전 기존 설정파일과 인증서 파일은 백업하시는 걸 권장 드립니다.
- Nginx에서 SSL 적용 시 사용하는 포트는 443입니다.
- Server\_name, root, access\_log 등의 항목은 서버의 환경에 맞게 설정해주세요.

```
server {
    listen 443 ssl;
    server_name example.com;
    ssl_certificate 인증서 경로 /도메인_cert.pem; # (인증서 파일)
    ssl_certificate_key 인증서 경로 /도메인_key.pem; # (개인키 파일)

    ssl_protocols TLSv1.2 TLSv1.3;
    ssl_ciphers HIGH:!aNULL:!MD5;
    ssl_prefer_server_ciphers on;

    root /var/www/html;
    index index.html;

    location / {
        try_files $uri $uri/ =404;
    }
}
```

##### (3) 구문 확인

- Nginx -t 명령어 입력 후 문법에 이상이 없다면 syntax is ok 문구가 표시됩니다.

```
[root@root nginx]# nginx -t
nginx: the configuration file /etc/nginx/nginx.conf syntax is ok
nginx: configuration file /etc/nginx/nginx.conf test is successful
```

##### (4) Nginx 재시작 및 적용 확인

- Systemctl restart nginx 명령어를 통해 nginx를 재실행 합니다.
- 웹브라우저에서 [https://도메인]으로 접속하여 https 통신 및 인증서 정보를 확인합니다.

“

# 감사합니다.

[ 365일 24시간 고객 만족센터 ]

마이페이지를 통한 관리 지원,

전문 엔지니어들이 365일 24시간 고객 만족센터 운영