대 한 민 국 E-Business 대 표 브 랜 드

ITEASY

Apache

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

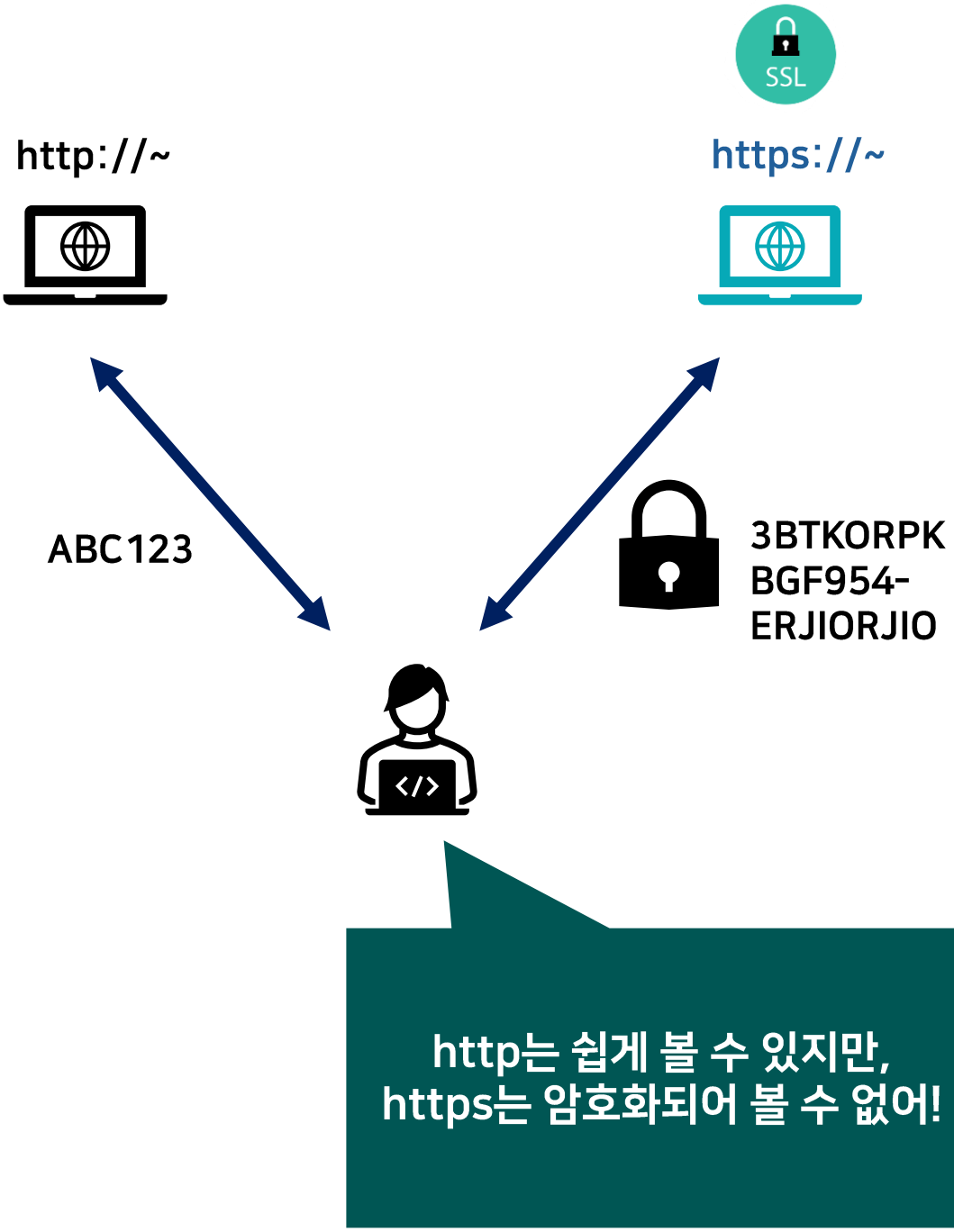
iTEASY It is easy, IT is easy

It is easy,
IT is easy!

CONTENTS

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 위협으로 부터 소중한 데이터를 보호할 수 있습니다.



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

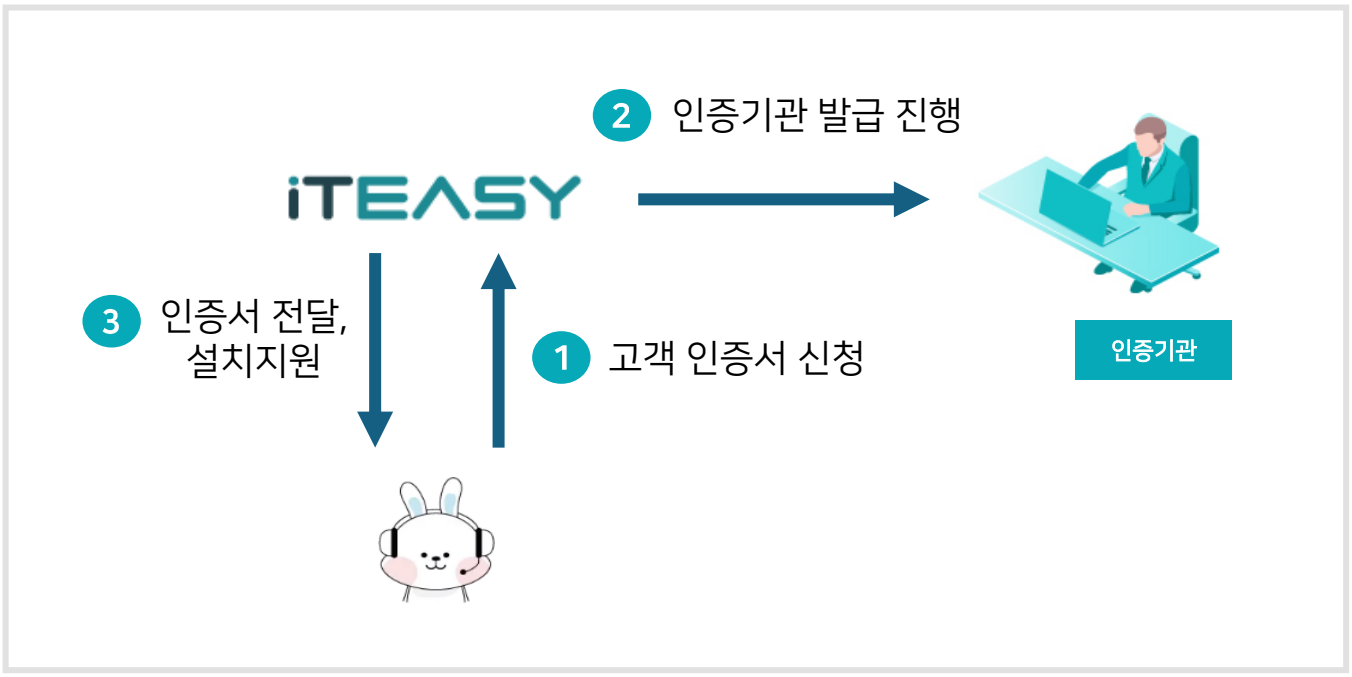
- 도메인에 대한 소유권을 확인하기 위해 인증을 진행 합니다.
  도메인 소유권 인증 방법 – 메타태그 [HTTP. HTTPS] , DNS , 이메일

(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 권장 드립니다. 작업 의뢰를 통해 더 정확하고 안전한 설정이 가능합니다.

▷ 설치 테스트 환경

- OS : Rocky 9.3
- Apache : 2.4.62 (패키지 설치)
- Apache 웹 서버가 HTTPS 기능을 지원하려면 openssl과 mod_ssl이 설치되어 있어야 합니다.
- 모듈 확인 : /usr/sbin/httpd – l , httpd – l

  mod_so.c 는 동적인 방식으로 모듈 설치를 지원하는 방식입니다.

  module 디렉터리 내에 mod_ssl.so가 있는지 확인하셔야 합니다.

```
[root@root ~]# /usr/sbin/httpd -l
Compiled in modules:
  core.c
  mod_so.c
  http_core.c
```

- openssl 확인 : rpm –qa | grep openssl

```
[root@root ~]# rpm -qa | grep openssl
openssl-libs-3.0.7-24.el9.x86_64
openssl-3.0.7-24.el9.x86_64
apr-util-openssl-1.6.1-23.el9.x86_64
```

- mod_ssl 활성화 확인 : httpd –M | grep ssl

  ssl-module (shared) 가 출력되면 mod_ssl이 활성화 된 상태입니다.

```
[root@root etc]# httpd -M | grep ssl
 ssl_module (shared)
```

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.

- CA (Certificate Authority, 인증기관)

- 서버의 인증서를 서명함으로써 신뢰성을 보장합니다.

- KEY (Private Key, 개인 키)

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

(2) ssl.conf 수정

- 설정하기 전 기존 설정파일과 인증서 파일은 백업하시는 걸 권장 드립니다.
- https의 기본 포트는 443입니다.
- ServerName, DocumentRoot, ErrorLog 등의 항목은 서버 환경에 맞게 설정해주세요.

```
Listen 443
<VirtualHost *:443>
SSLEngine On
SSLCertificateFile 인증서 경로/도메인_crt.pem(인증서 파일)
SSLCertificateKeyFile 인증서 경로/도메인_key.pem(개인키 파일)
SSLCertificateChainFile 인증서 경로/도메인_ca.pem(체인 인증서)
</VirtualHost>
```

(3) 구문 확인

- apachectl -t 명령어 입력 후 Syntax OK 가 출력되면 문법 상 오류가 없는 것을 의미 합니다.

```
[root@root ~]# apachectl -t
Syntax OK
```

(4) Apache 재시작 및 적용 확인

- 웹브라우저에서 [https://도메인]으로 접속하여 https 통신 및 인증서 정보를 확인합니다.

iTEASY It is easy, IT is easy

“

감사합니다.

[365일 24시간 고객 만족센터]

마이페이지를 통한 관리 지원,

전문 엔지니어들이 365일 24시간 고객 만족센터 운영

상호 : ㈜아이티이지 대표자 : 조명래 사업자등록번호 : 214-87-66295 통신판매업신고번호 : 제2005-05971호

주소 : 서울특별시 서초구 서초대로 250 3층 (스타갤러리브릿지) 개인정보관리자 : 임훈교 Tel) 1600-8324 Fax) 02-6264-8321