made by kangsinbeom

e-mail: kangsinbeom2448@gmail.com

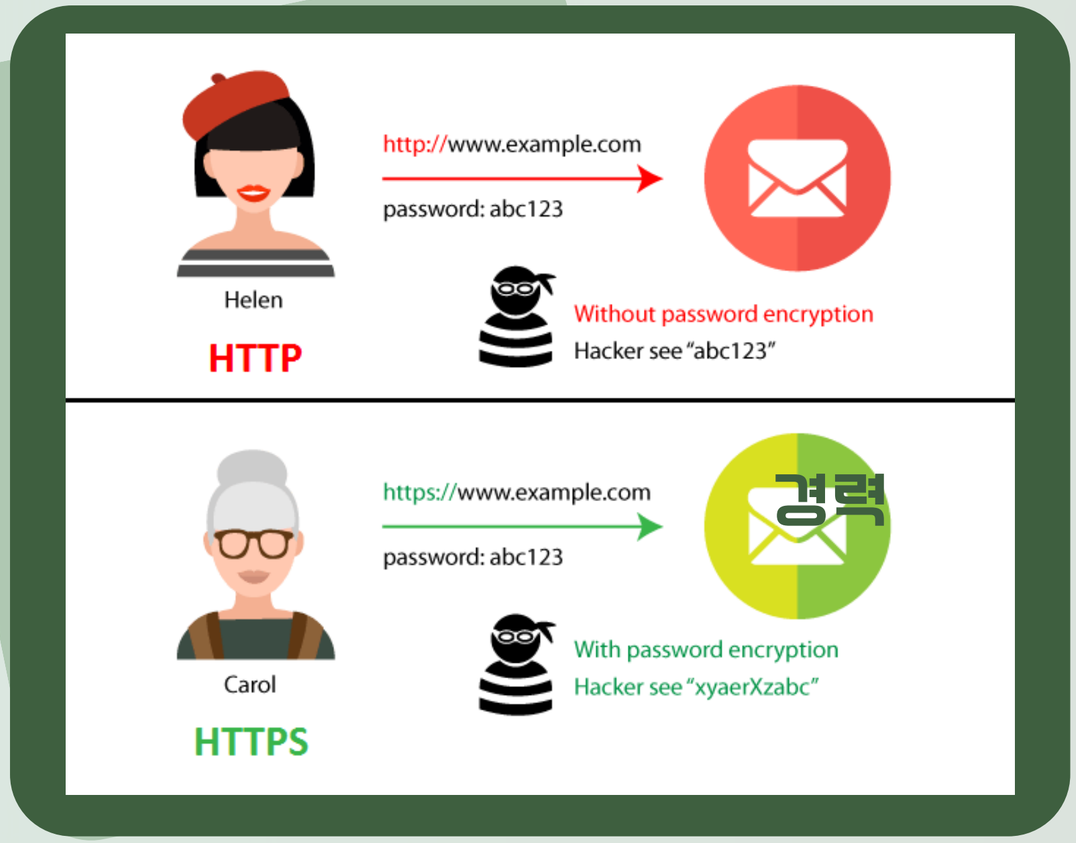
# HTTPS

INDEX

# 목차

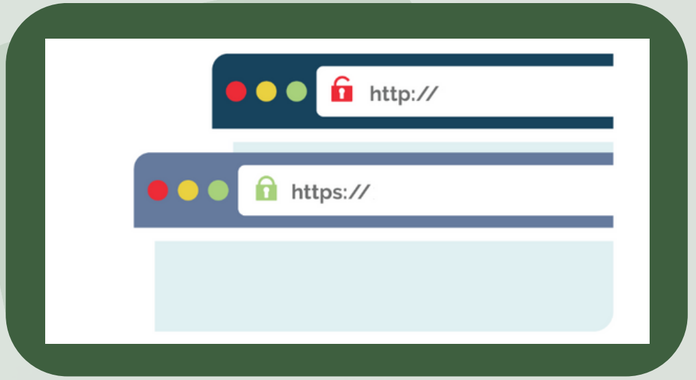
01

# ☒HTTPS란?




## HTTP vs HTTPS

HTTP + Security(보안)



# 01 장점 및 특징

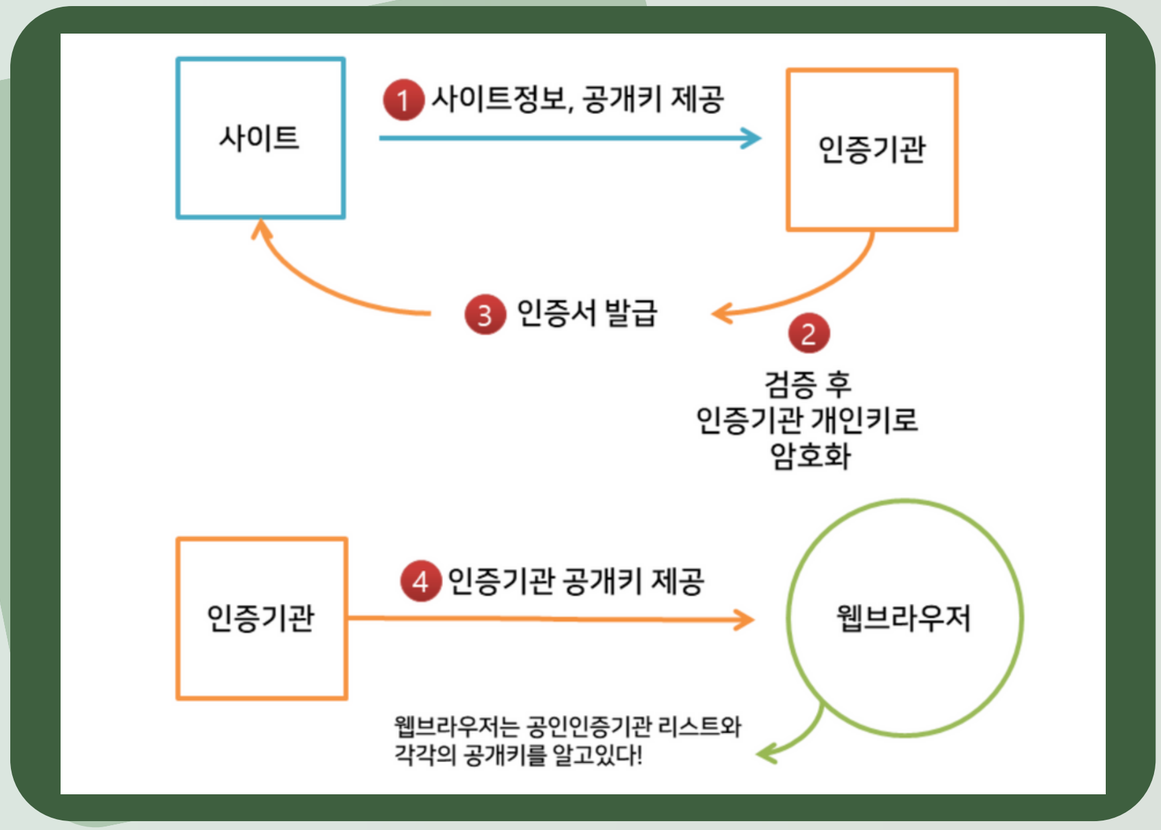
01
무결성 및 인증

02
개인 정보 보호

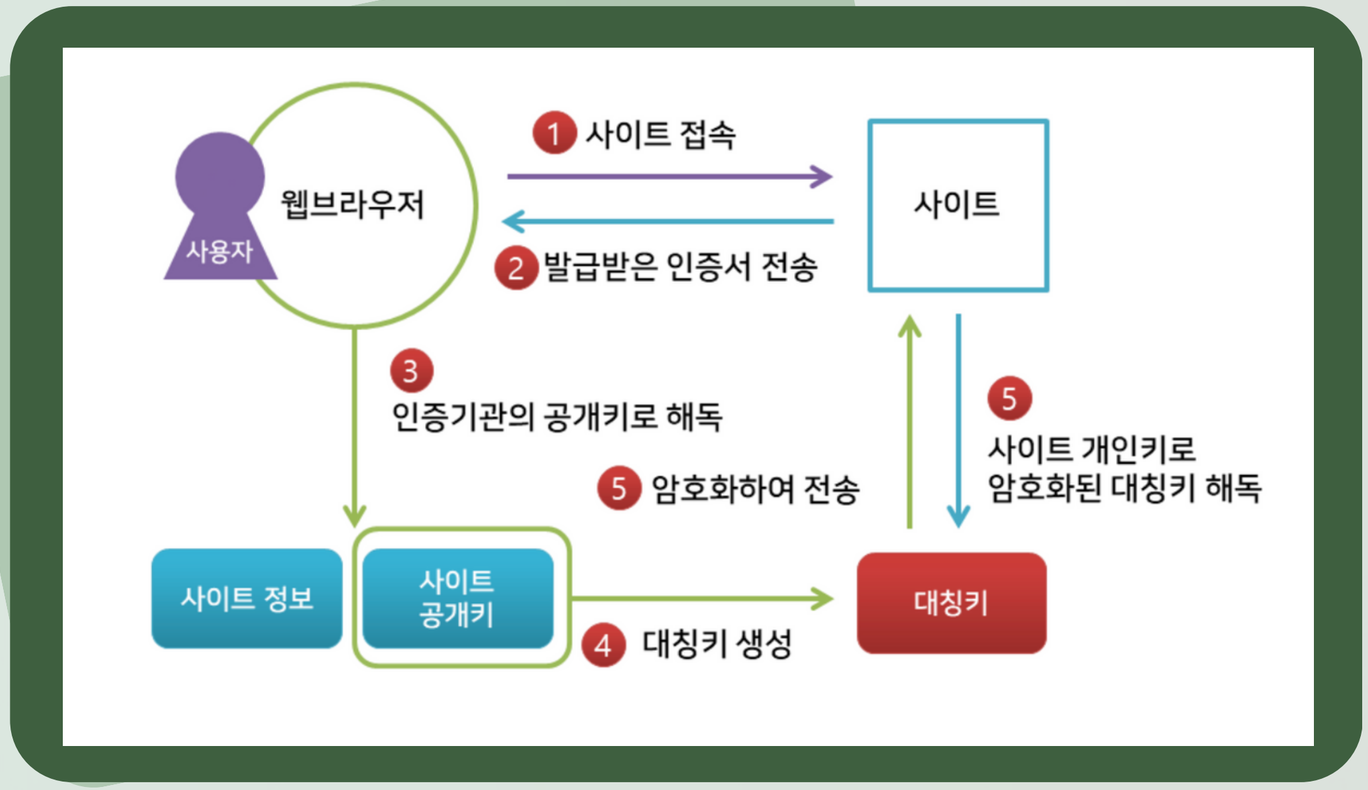
03
SEO 최적화

04
권한 부여

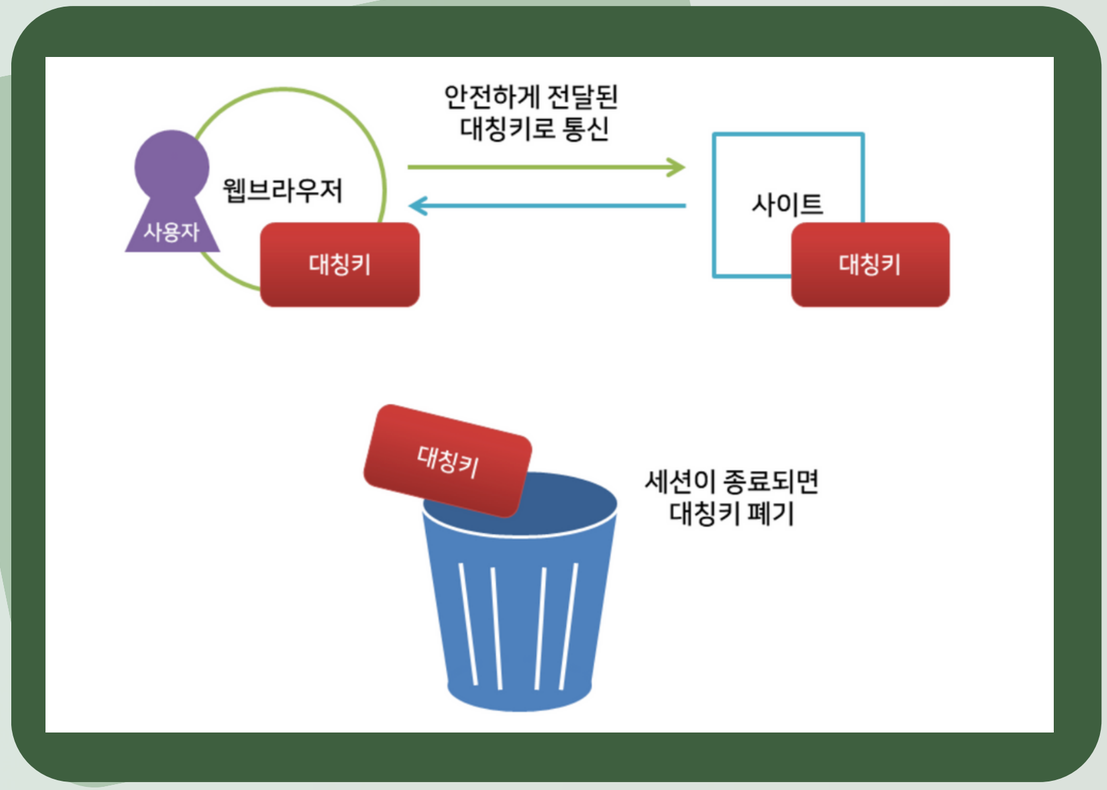
# 01 동작 방식


사이트
1 사이트정보, 공개키 제공
인증기관
3 인증서 발급
2
검증 후
인증기관 개인키로
암호화
인증기관
4 인증기관 공개키 제공
웹브라우저
웹브라우저는 공인인증기관 리스트와
각각의 공개키를 알고있다!

# 01 동작 방식


웹브라우저
사용자
1 사이트 접속
2 발급받은 인증서 전송
사이트
3
인증기관의 공개키로 해독
5 암호화하여 전송
5
사이트 개인키로
암호화된 대칭키 해독
사이트 정보
사이트
공개키
4 대칭키 생성
대칭키

# 01 동작 방식



# 02 SSL / TLS

암호화 프로토콜
SSL의 업그레이드 버전 TLS

01

## ☒DV 인증서

블로그 수준 (로우급 옵션)
(Domain Validated SSL 인증서)

02

## OV 인증서

기업 수준 (미들급 옵션)
(Organization Validated SSL 인증서)

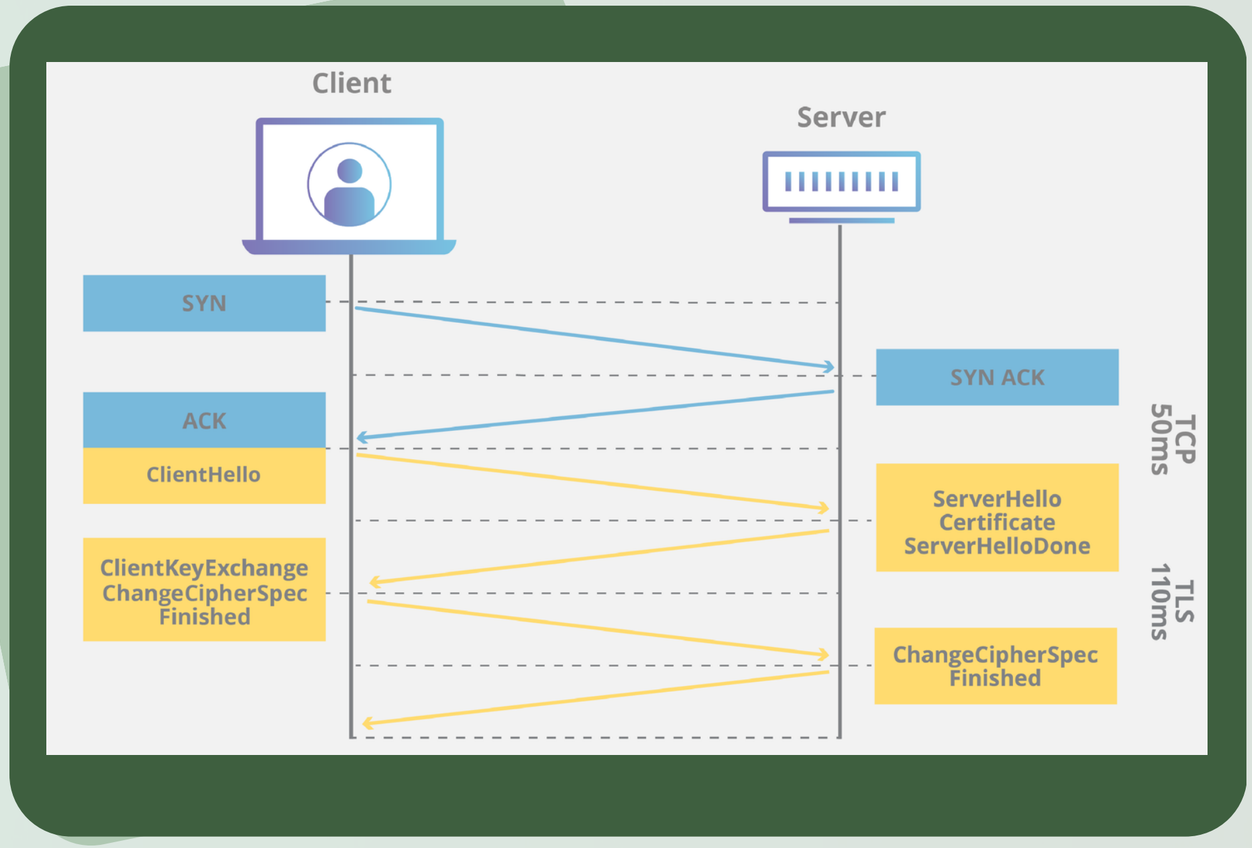
03

## ☒EV 인증서

은행, 소셜 커머스 (하이급 옵션)
(Extended Validated SSL 인증서)

02

# ☒TLS 핸드 셰이크




## 기능

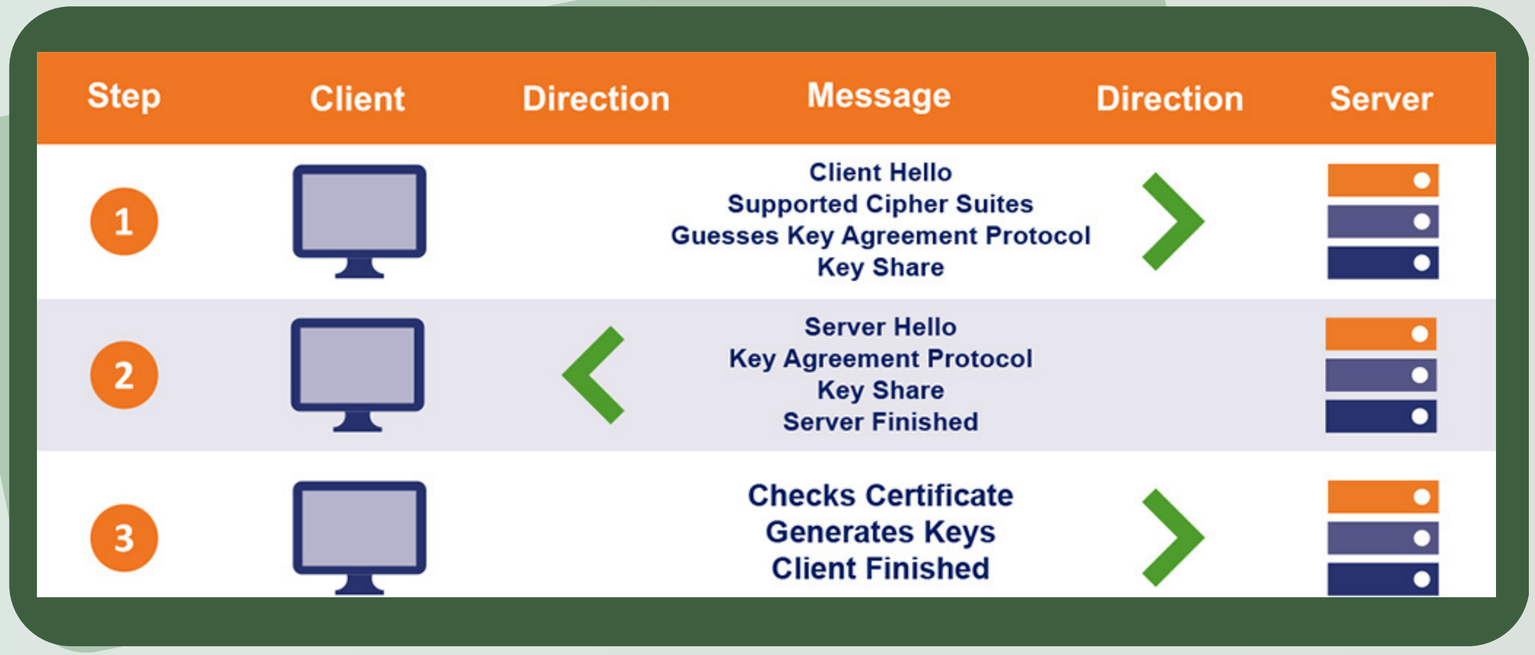
- 암호화
- 인증
- 무결성

## 작동 방식

- TLS 인증서를 소유한 원본 서버
- TLS 버전 지정
- 암호 제품군 결정
- TLS 인증서를 통한 신원 인증
- hand shake 완료 후 세션 키 생성

02

# ☒TLS 핸드 셰이크(1.3)




## 특징

- 빠르고 단축된 단계
- 향상된 안전성
- 취약 알고리즘 제거
- 0-RTT 모드

# 03 주의 사항

## 속도 저하

암호화로 인해 HTTP보다 낮은 속도

## 신뢰성 여부

자체적 발급이 가능한 인증서(사설 인증서)
신뢰성이 없는 사이트입니다.

# THANK YOU

감사합니다.