SSL/TLS 인증서는 웹사이트와 사용자의 브라우저 간의 안전한 통신을 보장하기 위해 사용되는 디지털 서명이다. SSL(Secure Sockets Layer)과 TLS(Transport Layer Security)은 웹 보안 프로토콜로 데이터 전송 과정에서 기밀성(정보를 오직 인가된 사람들에게 만 공개하는 것)을 유지하고 데이터가 변조되지 않도록 한다. 이 인증서는 웹사이트가 신뢰할 수 있는지 확인하고 클라이언트와 서버 간의 통신을 암호화한다.

SSL/TLS 인증서의 기능

1. 인증(Authentication) : 인증서는 웹사이트의 신원을 확인한다. 이를 통해 사용자는 자신이 접속한 사이트가 진짜 사이트인지 확인할 수 있다.
2. 암호화(Encryption) : 인증서는 웹사이트와 사용자가 주고받는 데이터를 암호화한다. 이를 통해 네트워크 상에서 데이터를 가로채더라도 내용을 읽을 수 없게 만들어 해킹이나 도청으로부터 안전하게 보호한다.

추가적인 인증서가 필요한 이유

1. 사용자 신뢰도 향상 : HTTPS로 시작되는 웹사이트는 사용자에게 안전하고 신뢰할 수 있다는 인상을 준다.
2. 검색 엔진 순위 상승 : 구글과 같은 검색 엔진은 HTTPS 웹사이트를 더욱 신뢰하고 검색 결과 상위에 노출시키는 경향이 있다.
3. 법적 요구 사항 : 일부 국가에서는 특정 산업 분야에서 SSL/TLS 인증서를 의무화하고 있다.

SSL/TLS 인증서의 종류

1. 도메인 검증 인증서(Domain Validation, DV) : 가장 기본적인 인증서로 도메인 소유권만 확인한다. 발급 절차가 간단하고 비용이 저렴하다.
2. 조직 검증 인증서(Organization Validation, OV) : 도메인 소유권 외에 기업의 법인등기부 등을 통해 조직의 신원을 확인한다. 회사나 기관의 법적 존재를 확인한 후 발급된다.
3. 확장 검증 인증서(Extended Validation, EV) : 가장 높은 수준의 인증서로 조직의 신원을 철저하게 검증하고 브라우저 주소창에 회사명이 녹색으로 표시된다. 금융기관 등 높은 수준의 보안을 요구하는 사이트에서 주로 사용된다.

SSL/TLS 인증서의 실행 과정

1. 핸드셰이크 과정 사용자가 웹사이트에 접속 :사용자가 웹사이트에 접속하면 브라우저가 웹 서버에 SSL/TLS 연결을 요청한다. (클라이언트와 서버는 서로의 인증서를 교환, 웹 서버는 사용할 암호화 방식 및 키 제공)
2. 데이터 암호화 : 브라우저는 핸드셰이크 과정 받은 공개 키를 사용하여 데이터를 암호화하고 웹 서버로 전송한다.
3. 데이터 복호화 : 웹 서버는 자신의 개인 키를 사용하여 받은 데이터를 복호화한다.

4. 세션 종료 : 통신이 끝나면 SSL/TLS 세션이 종료되고 사용된 키는 더 이상 유효하지 않게 된다. 새로운 통신이 시작될 때마다 새로운 핸드셰이크와 키 교환이 이루어진다.

마무리

SSL은 SSL 2.0과 SSL 3.0은 심각한 보안 취약점이 발견되어 현재는 더 이상 사용되지 않고 TLS가 표준으로 자리 잡았다. TLS 1.3은 현재 최신 버전으로 더욱 향상된 보안 기능과 빠른 성능을 제공한다.