

백서

SSL 인증서 초보자 가이드

온라인 보안을 위한 최선의 선택



SSL 인증서 초보자 가이드

온라인 보안을 위한 최선의 선택

목차

서론	3
SSL 인증서란 무엇입니까?	3
SSL 암호화는 어떻게 작동합니까?	3
사이트에 유효한 SSL 인증서가 있는지 확인하려면 어떻게 해야 합니까?	4
SSL 인증서는 어디에 사용할 수 있습니까?	5
다양한 SSL 인증서 유형	5
알기 쉬운 기술 용어 해설.	6
결론	7

서론

사람들이 집이나 회사 건물에 보안 장치를 설치하는 것과 마찬가지로, 온라인에서도 보안 수단이 필요합니다. 이러한 보안 조치는 본인의 안전뿐 아니라 귀하의 집이나 회사, 웹 사이트를 방문하는 다른 사람을 보호하기 위해서도 필요합니다. 그러려면 잠재적인 리스크가 무엇인지 파악하고 이러한 리스크를 확실하게 차단할 수 있는 방법을 강구해야 합니다. 하지만 모든 것이 빠르게 변화하는 IT 환경에 뒤떨어지지 않고 최신 기술을 습득하는 것은 쉬운 일이 아닙니다. 따라서 믿을 수 있는 인터넷 보안 업체와의 협력이 필요합니다.

본 가이드는 관련 기술을 자세히 설명하고 올바른 온라인 보안 결정을 내리기 위해 필요한 정보를 알려줍니다. 전문 용어는 본 문서의 “알기 쉬운 기술 용어 해설” 부분을 참조하십시오.

SSL 인증서란 무엇입니까?

SSL 인증서는 디지털 시스템 파일 또는 코드로서 다음 두 가지 기능을 담당합니다.

- 1. 인증 및 검증:** SSL 인증서에는 개인, 기업 또는 웹 사이트의 진위성을 확인할 수 있는 정보가 포함되어 있습니다. 이 정보는 방문자가 귀하의 웹 사이트를 방문하여 브라우저의 자물쇠 기호나 인증 마크(Norton™ Secured Seal)를 누르면 표시됩니다. 인증 기관(CA)이 SSL 인증서 발급 여부를 심사할 때 EV(Extended Validation) SSL 인증서가 가장 기준이 까다로우며 따라서 가장 많은 신뢰를 받습니다.
- 2. 데이터 암호화:** SSL 인증서는 암호화를 지원하므로 웹 사이트에서 교환되는 중요한 정보를 지정된 수신자가 아닌 타인이 가로채서 읽을 수 없습니다.

신분증이나 여권은 국가 기관에서만 발급할 수 있는 것처럼 SSL 인증서도 믿을 수 있는 인증 기관(CA)에서 발급받아야 신뢰할 수 있습니다. CA는 SSL 인증서를 발급할 때 매우 엄격한 규칙과 정책을 준수해야 합니다. 신뢰받는 CA에서 발급한 SSL 인증서가 있다면 고객이나 파트너가 더욱 안심하고 거래할 수 있을 것입니다.

SSL 암호화는 어떻게 작동합니까?

열쇠로 문을 열고 잠그는 것처럼 암호화에서도 키를 사용하여 정보를 잠그거나 해제합니다. 따라서 올바른 키가 없으면 정보를 “열 수” 없습니다.

각 SSL 세션은 다음 2개의 키로 구성됩니다.

- 공개 키는 정보를 암호화하는 데 사용합니다.
- 개인 키는 정보를 해독하여 판독 가능한 원래의 형태로 복원하는 데 사용합니다.

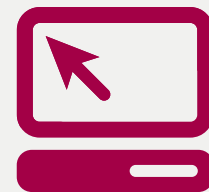
프로세스: CA에서 검증한 주체에게 발급되는 모든 SSL 인증서는 특정 서버 및 웹 사이트 도메인(웹 사이트 주소)을 대상으로 발급됩니다. 사용자가 브라우저를 통해 SSL 인증서가 있는 웹 사이트 주소로 이동하면 해당 브라우저와 서버 간에 SSL 핸드셰이크(greeting)가 수행됩니다. 그런 다음 서버가 정보를 요청하고 사용자의 브라우저 창에 해당 정보가 표시됩니다. 그러면 보안 세션이 시작되었음을 알립니다. 이를테면 인증 마크가 표시됩니다. 인증 마크를 누르면 SSL 인증서의 유효 기간, 보안 도메인, SSL 인증서 유형, 인증서를 발급한 CA와 같은 추가 정보가 표시됩니다. 이 일련의 과정은 고유한 세션 키를 사용하는 안전한 세션이 열렸으며 보안 통신을 시작할 수 있음을 의미합니다.

SSL은 “Secure Socket Layer”의 약자입니다. SSL은 방문자의 웹 브라우저와 귀사의 웹 사이트 간에 보안 세션 링크를 연결해주는 기술로, 이 링크를 통해 전송되는 모든 통신은 암호화되므로 안전합니다. 보안 이메일, 보안 파일 및 기타 여러 유형의 정보를 전송할 때도 SSL이 사용됩니다.

귀하라면 엽서 뒷면에 개인 정보나 은행 정보를 적어 보내시겠습니까?



SSL은 정보를 안전하게 보호하는 채널을 생성합니다.



사이트에 유효한 SSL 인증서가 있는지 확인하려면 어떻게 해야 할까요?

1. SSL 보안이 구현되지 않은 일반 웹 사이트는 브라우저 주소 표시줄을 보면 웹 사이트 주소 앞에 “http://”가 표시됩니다. HTTP는 “Hypertext Transfer Protocol”의 약자로 인터넷에서 정보를 전송하는 데 일반적으로 사용되는 방식입니다.



SSL 인증서로 보호받는 웹 사이트는 주소 앞에 “https://”가 표시됩니다. HTTPS는 “Secure HTTP”를 의미합니다.



2. 일부 인터넷 브라우저는 브라우저의 상단이나 하위에 자물쇠 기호를 표시하기도 합니다.
3. 웹 사이트 자체에 인증 마크가 표시되는 경우도 많습니다. 시만텍 고객사는 자사 웹 사이트에 Norton Secured Seal 인증 마크를 사용합니다. Norton Secured Seal 또는 자물쇠 기호를 누르면 CA가 검증하고 인증한 정보가 포함된 인증서가 표시됩니다.
4. 웹 사이트 방문자가 브라우저 창의 잠긴 자물쇠 또는 Norton Secured Seal과 같은 SSL 인증 마크를 누르면 인증된 조직 이름이 나타납니다. 보안 수준이 높은 브라우저인 경우 EV(Extended Validation) SSL 인증서가 탐지되면 인증된 조직 이름이 알아보기 쉽게 표시되고 주소 표시줄이 녹색으로 바뀝니다. 정보가 일치하지 않거나 인증서가 만료된 경우 브라우저에 오류 메시지 또는 경고가 표시됩니다.

SSL 인증서는 어디에 사용할 수 있습니까?

간단히 말하자면 정보를 안전하게 전송할 필요가 있는 모든 곳에서 SSL 인증서를 사용할 수 있습니다.

몇 가지 예를 들면 다음과 같습니다.

- 귀사의 웹 사이트와 고객의 인터넷 브라우저 간에 주고받는 통신을 보호합니다.
- 기업 인트라넷의 내부 통신을 보호합니다.
- 네트워크 또는 개인 이메일에서 주고받는 이메일 통신을 보호합니다.
- 내부, 외부 서버 간에 주고받는 정보를 보호합니다.
- 모바일 장치를 통해 주고받는 정보를 보호합니다.

다양한 SSL 인증서 유형

요즘은 다양한 유형의 SSL 인증서가 사용되고 있습니다.

- SSL 인증서의 첫 번째 유형은 자체 서명 인증서입니다. 이름으로 알 수 있듯이 이것은 CA에서 발급하지 않고 내부에서 사용할 용도로 생성된 인증서입니다. 웹 사이트 소유자가 자체적으로 인증서를 생성하므로 CA가 철저한 인증 및 검증을 거쳐 발급하는 SSL 인증서와 같은 신뢰도는 없습니다.
- 도메인 검증 인증서는 엔트리 레벨의 SSL 인증서로 신속한 발급이 가능합니다. 이 인증서는 인증서 신청자가 이 인증서를 사용할 도메인(웹 사이트 주소)을 실제로 소유하는지 여부만 검증합니다. 도메인 소유자가 합법적인 주체인지 여부는 확인하지 않습니다.
- 전체 검증 SSL 인증서가 진정한 온라인 보안을 실현하고 신뢰를 구축할 수 있는 인증서입니다. 이 인증서는 수 차례의 검증 및 검사 절차를 거쳐 사업체가 실재하는지 여부, 도메인의 소유권, 사용자의 인증서 신청 권한을 확인한 후 발급되며 따라서 시간이 조금 더 걸립니다.

모든 Symantec SSL Certificates는 전체 검증 SSL 인증서입니다.

- 128비트 또는 256비트 암호화를 지원하는 SSL 인증서를 사용하더라도 일부 오래된 브라우저 및 운영 체제는 이 레벨의 보안을 적용할 수 없는 경우가 있습니다. SGC(Server-Gated Cryptography) 기술이 구현된 SSL 인증서는 웹 사이트 방문자의 99.9% 이상이 128비트 또는 256비트 암호화를 사용할 수 있도록 지원합니다. 웹 서버에 SGC 인증서가 없으면 128비트의 강력한 암호화를 지원하지 않는 브라우저 및 운영 체제에서는 40비트 또는 56비트 암호화만 가능합니다. 하지만 SGC 기반 SSL 인증서를 구현한 웹 사이트에서는 오래된 브라우저 및 운영 체제 사용자도 임시로 128비트 SSL 암호화를 사용할 수 있습니다. SGC에 대한 자세한 내용은 www.symantec.co.kr/ssl-certificates에서 확인하십시오.
- 도메인 이름은 다양한 호스트 접미어와 함께 사용됩니다. 따라서 와일드카드 인증서를 사용하면 어떠한 도메인 호스트에도 완전한 SSL 보안을 적용할 수 있습니다(예: `host.your_domain.com`에서 “host”는 달라지지만 도메인 이름은 그대로 유지됨).
- SAN(Subject Alternative Name) SSL 인증서는 와일드카드 인증서와 유사하지만 더 다양하게 활용할 수 있습니다. 이 유형은 하나의 SSL 인증서에 둘 이상의 도메인을 추가할 수 있습니다.

- 코드 서명 인증서는 다운로드하는 소프트웨어가 전송 중에 무단으로 변경되지 않았는지 검증합니다. 많은 사이버 범죄자들이 인터넷에서 제공되는 소프트웨어를 무단으로 변경합니다. 이들은 안전한 패키지가 다운로드되는 동안 바이러스나 기타 악성 소프트웨어를 추가합니다. 코드 서명 인증서를 사용하면 위와 같은 문제가 발생하지 않습니다.
- EV(Extended Validation) SSL 인증서는 가장 엄격한 업계 표준을 적용하므로 고객이 가장 높이 신뢰합니다. EV SSL 인증서로 보호받는 웹 사이트를 방문하면 주소 표시줄이 녹색으로 보이고 해당 사이트의 합법적인 소유자 이름과 EV SSL 인증서를 발급한 보안 기관의 이름이 표시되므로 보안이 우수한 브라우저임을 나타낼 수 있습니다. 또한 인증서 보유자의 이름과 발급 CA의 이름도 주소 표시줄에 표시됩니다. 이처럼 눈으로 직접 보안 조치를 확인할 수 있기 때문에 고객이 안심하고 전자 상거래를 수행할 수 있습니다.

알기 쉬운 기술 용어 해설

Encryption(암호화): 정보가 “뒤섞이므로(scramble)” 지정된 사용자 이외 타인이 해당 정보를 사용할 수 없습니다.

Decryption(해독): 정보를 “올바른 순서로 재배치하고(un-scramble)” 원래의 형태로 복원합니다.

Key(키): 수학적 공식이나 알고리즘으로 정보를 암호화, 해독하는 데 사용됩니다. 자물쇠가 여러 개 있으면 열기가 더욱 어려운 것처럼 암호화 키의 길이(비트 수)가 길수록 더욱 강력한 암호화가 적용됩니다.

Browser(브라우저): 인터넷에 액세스할 때 사용하는 소프트웨어 프로그램입니다. 예를 들면 Microsoft Internet Explorer(IE), Mozilla Firefox, Apple Safari, RockMelt, Google Chrome이 있습니다.

결론

신뢰가 온라인 비즈니스의 성패를 결정합니다. 온라인 비즈니스를 운영하거나 전자 상거래 사이트를 호스팅하는 기업이 성공하려면 고객 보호를 위한 기술에 투자하여 고객 신뢰를 쌓아야 합니다. SSL 인증서와 인증 마크를 사용하면 고객의 신뢰가 높아진다는 것은 이미 입증된 사실입니다.

시만텍은 Symantec Authentication Services를 인수하여 세계 최고의 SSL 인증서 제공업체로 자리매김했으며 고객이 안심하고 로그인, 서핑, 구매할 수 있도록 지원합니다*. 시만텍은 전 세계에서 다른 어떤 CA보다 많은 1백만 개 이상의 웹 서버를 보호하고 있습니다*. 또한 시만텍은 대표적인 전자 상거래 및 बैं킹 사이트를 포함하여 전체 웹 사이트의 2/3 이상을 Extended Validation SSL로 보호합니다*. 시만텍 솔루션을 사용하면 가장 신뢰받는 인증 기관과 가장 인정받는 인터넷 인증 마크로 귀사의 웹 사이트와 평판을 보호할 수 있습니다.

자세한 내용은 www.symantec.co.kr/ssl-certificates에서 확인하십시오.

*시만텍 자회사, 계열사, 리셀러를 포함합니다.

추가 정보

웹 사이트

www.symantec.co.kr/ssl-certificates

Product Specialist에게 제품 문의

TEL: +61 3 9674 5500

시만텍 소개

시만텍은 보안, 스토리지 및 시스템 관리 솔루션을 제공하는 세계적 선두 기업으로, 기업 및 개인이 정보를 보호하고 관리할 수 있도록 지원합니다. 시만텍의 솔루션과 서비스는 다양한 위협으로부터 완벽하고 효율적인 보호를 제공하며 정보가 사용되거나 저장되는 장소에 상관없이 기업과 개인이 정보에 대한 확신을 가질 수 있도록 돕습니다. 보다 자세한 정보는 www.symantec.co.kr에서 확인하실 수 있습니다.

지역 본사

134 Moray St.
South Melbourne,
Victoria 3205,
Australia

