White Paper

Przewodnik po Certyfikatach SSL

Jak dokonać najlepszego wyboru,
zabezpieczając swoją stronę www.

Symantec

https://certyfikatyssl.pl

Norton SECURED
powered by VeriSign

Wprowadzenie:

Bez względu na to, czy jesteś osobą prywatną czy przedsiębiorcą, powinieneś traktować bezpieczeństwo on-line na równi z fizycznym bezpieczeństwem Swojego domu lub firmy. Nie tylko Ty musisz czuć się w nich bezpiecznie, ale również wszyscy, którzy odwiedzają Twój dom, firmę, czy też stronę www. Ważne jest, aby znać potencjalne zagrożenia, a następnie upewnić się, że jesteś przed nimi zabezpieczony. W szybko zmieniającym się świecie, nie łatwo jest być na bieżąco ze wszystkimi nowinkami. Dlatego rozsądnie jest wybrać renomowanego partnera.

Poniższy przewodnik ma objaśnić Ci technologię SSL i przekazać informacje, których potrzebujesz, aby dokonać najlepszego wyboru, zabezpieczając swoją stronę www.

Czym jest certyfikat SSL?

Certyfikat SSL jest cyfrowym dokumentem (lub fragmentem kodu), który ma dwie funkcje:

1. Autoryzacja i weryfikacja: Certyfikat SSL zawiera informacje na temat autentyczności niektórych danych osób fizycznych, firm lub stron www, które wyświetlane są odwiedzającym stronę po kliknięciu w symbol kłódki lub pieczęć bezpieczeństwa (np. Norton™ Secured Seal). Najbardziej rygorystyczne kryteria, dotyczące weryfikacji tego, czy certyfikat SSL może zostać wydany, związane są z certyfikatem typu EV (Extended Validation), czyniąc go najbardziej zaufanym spośród dostępnych certyfikatów SSL.

2. Szyfrowanie: Certyfikat SSL umożliwia szyfrowanie, co oznacza, że wymiana wrażliwych informacji przez stronę www nie może zostać przejęta i odczytana przez nikogo innego niż zamierzonego odbiorcę.

Podobnie jak dowód osobisty lub paszport może zostać wydany jedynie przez uprawnione do tego instytucje państwowe, certyfikat SSL jest wiarygodny, gdy wydaje go zaufany urząd certyfikujący (CA - Certificate Authority). CA stosuje rygorystyczne reguły w procesie przyznawania certyfikatu SSL. Certyfikat wydany przez zaufany urząd oznacza wyższą wiarygodność wśród klientów i partnerów.

Jak działa szyfrowanie SSL?

Tak jak zamykasz i otwierasz drzwi kluczem, szyfrowanie umożliwia zamknięcie i otwarcie informacji. Jeżeli nie posiadasz odpowiedniego klucza, nie będziesz mógł „otworzyć" informacji.

Każda sesja SSL uwzględnia dwa klucze:

- klucz publiczny używany do zaszyfrowania informacji.
- klucz prywatny używany do odszyfrowania informacji i przywrócenia jej do pierwotnej formy, aby mogła być odczytana.

Proces: Każdy certyfikat SSL wydawany dla zweryfikowanego przez CA podmiotu zawiera informację o serwerze i domenie (adresie www), dla których został wystawiony. Gdy Internauta wpisuje w swoją przeglądarkę adres strony www posiadającej certyfikat, następuje powitanie (tzw. „handshake") pomiędzy przeglądarką i serwerem.

SSL (Secure Socket Layer) jest technologią, która ustanawia bezpieczne połączenie pomiędzy Twoją stroną www a odwiedzającym ją użytkownikiem, aby cała komunikacja przesyłana przez nie była szyfrowana i bezpieczna. SSL jest również używany do bezpiecznego przesyłania poczty e-mail, plików i innych form informacji.

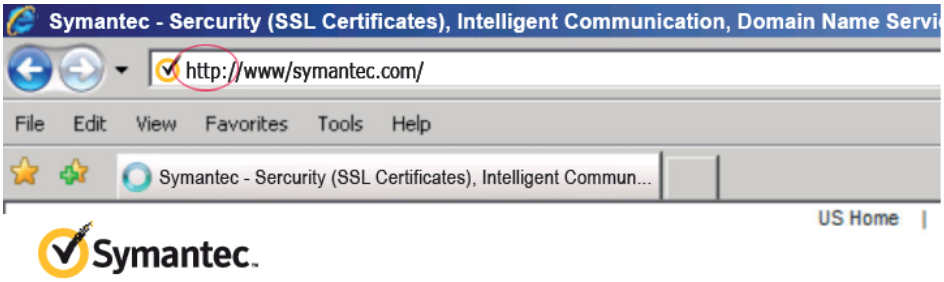
Czy wysyłałbyś komuś swoje prywatne dane albo informacje bankowe na pocztówce?

SSL tworzy bezpieczny i prywatny kanał komunikacji.

Serwer wysyła żądane informacje, które następnie są widoczne w oknie przeglądarki. Zauważysz zmiany, które wskazują, że bezpieczna sesja została zainicjowana, np. pojawi się znak bezpieczeństwa. Po kliknięciu go zobaczysz dodatkowe informacje, np. okres ważności certyfikatu, nazwę zabezpieczonej domeny, rodzaj certyfikatu i jego wystawcę. Wszystko to oznacza, że zostało nawiązane bezpieczne połączenie dla sesji z unikalnym kluczem i komunikacja może przebiegać bezpiecznie.

Skąd mam wiedzieć, że strona ma ważny certyfikat SSL?

1. Standardowa strona bez SSL wyświetla „http://" przed adresem www. Skrót ten oznacza „Hypertext Transfer Protocol" i jest powszechnym protokołem transmisji danych w Internecie.



Natomiast strona zabezpieczona certyfikatem SSL wyświetla „https://". Oznacza to "Secure HTTP".

2. Zobaczysz również symbol kłódki u góry lub na dole przeglądarki internetowej (w zależności od stosowanej przeglądarki).

3. Często zauważysz też znaki bezpieczeństwa wyświetlane na stronie. W przypadku produktów Symantec™ klienci używają pieczęci Norton Secured Seal. Gdy klikniesz w nią lub w symbol kłódki, wyświetlone zostaną szczegóły certyfikatu oraz dane identyfikacyjne firmy, które zostały sprawdzone i potwierdzone przez CA.

4. Nowoczesne przeglądarki, gdy wykryją certyfikat EV, automatycznie wyświetlają nazwę zweryfikowanej organizacji i zielony pasek adresu. Jeżeli informacje nie zgadzają się lub certyfikat wygasł, przeglądarka wyświetla komunikat o błędzie lub ostrzeżenie.

Gdzie mógłbym użyć certyfikatu SSL?

Najkrótsza odpowiedź na to pytanie brzmi: wszędzie, gdzie chciałbyś przesyłać informacje w sposób niejawny.

Oto kilka przykładów:

- zabezpieczenie połączenia klientów z Twoją stroną www.
- zabezpieczenie wewnętrznej komunikacji w ramach firmowego intranetu.
- zabezpieczenie komunikacji e-mail wysyłanej z i na Twoją pocztę firmowa lub prywatną.
- zabezpieczanie informacji przesyłanych pomiędzy serwerami (zarówno w obiegu wewnętrznym, jak i zewnętrznym).
- zabezpieczanie informacji wysyłanych i otrzymywanych za pomocą urządzeń mobilnych.

Typy certyfikatów SSL

Obecnie na rynku dostępnych jest wiele typów certyfikatów SSL.

- Pierwszy rodzaj stanowią certyfikaty self-sign. Są to certyfikaty wystawiane dla celów własnych i nie są one generowane przez urząd certyfikujący (CA). Ponieważ wystawia go sam właściciel strony, nie jest on równoważny z pełnoprawnym certyfikatem weryfikowanym przez zaufane CA.

- Certyfikaty domenowe (DV - Domain Validated) uważane są za podstawowy rodzaj certyfikatu SSL i mogą być wydane bardzo szybko. Weryfikacja polega na sprawdzeniu czy wnioskodawca jest właścicielem domeny, dla której wystawiany jest certyfikat. Nie ma miejsca dodatkowa weryfikacja, która sprawdziłaby czy podmiot ten ma prawdziwą osobowość prawną.

- W pełni weryfikowany certyfikat SSL jest pierwszym krokiem do prawdziwego bezpieczeństwa on line i budowania wiarygodności. Mówiąc konkretnie, ten typ certyfikatów jest jedynym gwarantem, że organizacja przeszła liczne procedury weryfikacyjne, sprawdzające: istnienie firmy, własność domeny i uprawnienie wnioskodawcy do ubiegania się o certyfikat.

Wszystkie certyfikaty SSL Symantec są w pełni weryfikowane

- Mimo, że certyfikat SSL jest w stanie obsłużyć 128- lub 256-bitowe szyfrowanie, niektóre starsze przeglądarki i systemy operacyjne nadal nie mogą osiągnąć tego poziomu bezpieczeństwa. Certyfikaty SSL wyposażone w technologię Server-Gated Cryptography (SGC) umożliwiają osiągnięcie 128- lub 256- bitowego szyfrowania ponad 99,9% odwiedzającym. Bez certyfikatu SGC, przeglądarki i systemy operacyjne, które nie obsługują 128-bitowego szyfrowania, uzyskałyby jedynie 40- lub 56-bitowe. Użytkownicy starszych przeglądarek i systemów na czas korzystania ze strony www, posiadającej certyfikat SSL z technologią SGC, mają tymczasowy dostęp do 128-bitowego szyfrowania.

- Domena jest często używana z licznymi prefiksami. Z tego powodu możesz użyć certyfikatu Wildcard, który pozwala zapewnić pełną ochronę SSL dla subdomen twojego adresu www, np. subdomena.twoja-domena.com (gdzie „subdomena" może być dowolna, a „twoja-domena.com" jest stała).

- Podobnie do certyfikatów Wildcard, ale trochę bardziej wszechstronnie działają certyfikaty z opcją SAN (Subject Alternative Name), które umożliwiają dodanie więcej niż jednej domeny do certyfikatu.

- Certyfikaty Code Signing są stworzone specjalnie w celu zapewnienia, że oprogramowanie, które pobrałeś nie zostało zmodyfikowane podczas przesyłania. Wielu cyberprzestępców próbuje zmienić programy dostępne w Internecie. Mogą oni załączyć wirusa lub inne złośliwe oprogramowanie do pobieranego pakietu. Certyfikat gwarantuje, że do tego nie doszło

- Certyfikaty SSL typu EV oferują najwyższy poziom walidacji i zapewniają największe zaufanie klientów. Gdy użytkownik odwiedza stronę z certyfikatem EV, pasek adresowy zmienia się na zielony i pojawia się pole z nazwą właściciela strony i wystawcą certyfikatu. Ten element pomaga podnieść zaufanie konsumentów do handlu elektronicznego..

Podsumowanie

Zaufanie ma ogromne znaczenie w biznesie. Inwestowanie w technologie, które służą ochronie klientów i pozyskaniu ich zaufania, jest kluczowym czynnikiem sukcesu dla każdej firmy, która działa online lub posiada stronę www o charakterze e-commerce.

Skuteczne wdrażanie certyfikatu SSL oraz prawidłowe umieszczenie i zastosowanie znaków bezpieczeństwa, to sprawdzony sposób na budowanie zaufania klientów.

Wraz z przejęciem części VeriSign, Symantec stał się wiodącym dostawcą certyfikatów SSL na całym świecie, zapewniając klientom bezpieczeństwo począwszy od wyszukiwania, przez przeglądanie, zakup, aż po rejestrację. Symantec zabezpiecza ponad milion serwerów na całym świecie. Symantec zabezpiecza również ponad 2/3 stron www stosujących certyfikat EV, w tym największe banki i firmy e-commerce. Wybierając Symantec możesz być pewny, że Twoja strona www i Twoja reputacja są chronione przez CA z udokumentowanym doświadczeniem i najbardziej rozpoznawanym znakiem zaufania w Internecie.

Typy certyfikatów SSL

Symantec jest światowym liderem w dziedzinie zabezpieczeń, przechowywania danych i systemów zarządzania, pomagając klientom indywidualnym i firmom w bezpieczny sposób zarządzać informacją w globalnej sieci. Nasze produkty i usługi chronią przed większością zagrożeń różnego typu, pełniej i skuteczniej, zapewniając spokój gdziekolwiek informacje są używane lub przechowywane.

Symantec Corporation

350 Ellis Street
Mountain View, CA 94043 USA
1 (866) 893 6565
www.symantec.com