

CERTYFIKAT SSL 2018

WSZYSTKO, CO POWINIENIEŚ WIEDZIEĆ O CERTYFIKATACH SSL, ALE WSTYDZISZ SIĘ ZAPYTAĆ

CO DAJE CI CERTYFIKAT SSL?

WIARYGODNOŚĆ

Potwierdza kto jest właścicielem strony www, dla której został wystawiony. Certyfikat wydawany jest po sprawdzeniu firmy, a następnie wyświetla jej dane.



BEZPIECZEŃSTWO

Szyfruje informacje przesyłane między użytkownikami strony www, a serwerem na którym jest ona umieszczona. Uniemożliwia dostęp do danych osobom niepowołanym.

CZY TWOJA STRONA WWW POTRZEBUJE CERTYFIKATU SSL?

Od lipca 2018 najpopularniejsza przeglądarka internetowa Chrome wszystkie strony www bez certyfikatu SSL oznaczy jako **“Niebezpieczne”**.

Tak, Twoja strona potrzebuje certyfikatu!

JAKI CERTYFIKAT WYBRAĆ?



LICZBA DOMEN

Jeżeli posiadasz jedną domenę np. certyfikatyssl.pl wybierz certyfikat standardowy. Zwróć uwagę, aby chronił domenę zarówno z www, jak i bez www. Gdy masz więcej domen skorzystaj z opcji MULTI-DOMAIN (chroni wiele różnych adresów www) lub WILDCARD (chroni główny adres oraz wszystkie subdomeny 1-go poziomu np. login.certyfikatyssl.pl, sklep.certyfikatyssl.pl, itd.).



WIDOCZNOŚĆ CERTYFIKATU

Zależy od rodzaju certyfikatu, które dzielimy na: DV, OV i EV. Różnią się one procesem weryfikacji podmiotu, który ubiega się o wydanie certyfikatu. Jeżeli zdecydujesz się na pełne potwierdzenie tożsamości wybierając certyfikat EV, Twój adres w przeglądarce zyska zieloną nazwę organizacji. Klienci dostrzegą to natychmiast. Z tego powodu EV wybierany jest przez banki.



MARKA SSL

Od wystawcy certyfikatu zależy: gwarancja, szybkość wystawienia certyfikatu oraz język weryfikacji. Jeżeli zależy ci na walidacji w języku polskim, wybieraj polskie certyfikaty, np. SuperFast SSL.



OKRES WAŻNOŚCI

Najczęściej certyfikaty kupowane są na okres jednego roku, jednak możesz zamówić go od razu na dwa lata. W ten sposób możesz zmniejszyć swoje wydatki w dłuższym okresie i zapewnić sobie bezpieczeństwo i spokój z góry na 2 lata.



CENA

Zależy od wcześniej wymienionych elementów, czyli typu certyfikatu, dodatkowych opcji, jego wystawcy, okresu ważności, etc. Ceny zaczynają się już od 92 zł za rok.

JAK ZABEZPIECZYĆ STRONĘ WWW?

ZAKUP CERTYFIKATU

W poszukiwaniu najlepszej opcji dla swojej strony wybierz usługodawcę, który ma szeroki wybór oraz jest w stanie zapewnić pomoc przy zakupie i profesjonalne wsparcie przy instalacji i w trakcie użytkowania. Po wyborze certyfikatu zamów go i opłać.



GENEROWANIE PLIKU CSR

CSR (Certificate Signing Request) jest niezbędne do zamówienia i utworzenia certyfikacji SSL. Plik może zostać wygenerowany na serwerze lub przy pomocy narzędzi, udostępnianych przez dystrybutorów certyfikatów. W oparciu o dane zawarte w pliku CSR wystawiony będzie certyfikat SSL. Generator CSR znajdziesz tu: <https://certyfikatyssl.pl/ssl-tools/csr-generator.html>.



PRZESŁANIE PLIKU CSR I WERYFIKACJA

Gdy masz już CSR prześlij go do obsługi serwisu. Następnie zweryfikowana zostanie autentyczność danych w oparciu o informacje dostępne w bazach i rejestrach.

Pamiętaj, że dane te muszą być zgodne. Jeżeli zmienić się adres, musisz go podać zgodnie ze stanem faktycznym lub zaktualizować wcześniej wpisy. Zwróć też uwagę na poprawność nazwy firmy.



POBIERANIE CERTYFIKATU

Po pozytywnym zweryfikowaniu danych firmy, otrzymasz certyfikat, który może zostać wysłany na adres e-mail lub będzie dostępny do pobrania w panelu klienta. Pamiętaj wraz z certyfikatem pobrać certyfikaty pośredniczące i certyfikat root, które tworzą tzw. taj, aby łańcuch certyfikacji.



INSTALACJA CERTYFIKATÓW NA SERWERZE

Pobrane wcześniej certyfikaty zainstaluj na serwerze. Sposób instalacji uzależniony jest od typu serwera i jego oprogramowania. Instrukcje instalacji na najpopularniejszych serwerach znajdziesz pod adresem: <https://certyfikatyssl.pl/faq/instalacje-certyfikatow-ssl.html>



WPROWADZENIE PROTOKOŁU „HTTPS://” NA STRONIE

Po zainstalowaniu certyfikatu na serwerze przystąp do wprowadzania szyfrowania na stronie. W tym celu należy do linków, prowadzących do chronionych stron, dodać w adresie https://.. Zmiana taka powinna objąć wszystkie strony, na których klient podaje swoje dane: logowanie, rejestracja, finalizacja zakupów, formularz kontaktowy.

Aby SSL działał prawidłowo, na szyfrowanych stronach nie może być linków, które zawierają protokół nieszyfrowany „http://”



ZABEZPIECZYŁEŚ STRONĘ? POINFORMUJ O TYM KLIENTÓW.

Jeżeli twój e-sklep jest już bezpieczny, powiedz o tym swoim klientom. Na stronie możesz zainstalować znaki bezpieczeństwa, tzw. „Trust Sign” lub „Site Seal”. Znajdziesz je na stronie wystawcy certyfikatu. Wystarczy go pobrać i dodać na zabezpieczonych stronach.



GRATULUJEMY! DOŁĄCZYŁEŚ DO GRONA WIARYGODNYCH SPRZEDAWCÓW.