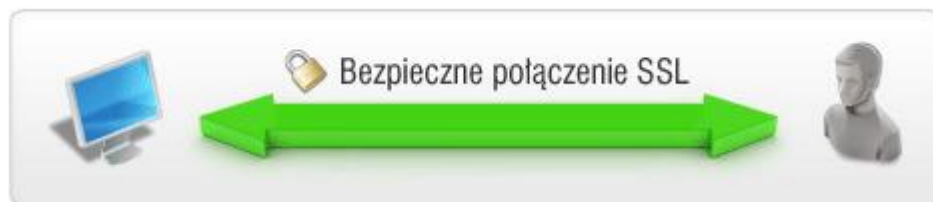


Wszystkie przesyłane przez naszych klientów informacje są chronione certyfikatem homeSSL

SSL (ang. **Secure Socket Layer**) jest protokołem opracowanym przez firmę Netscape Communications Corporation pozwalającym na szyfrowanie przesyłanych informacji. Aktualnym rozwinięciem tego protokołu jest **TLS (Transport Layer Security)**.



Głównym celem jest zapewnienie poufności i integralności transmisji danych oraz zapewnienie uwierzytelnienia. Technologia wykorzystuje szyfrowanie asymetryczne (przy wykorzystaniu klucza publicznego) oraz certyfikaty w standardzie X.509. Dzięki wykorzystaniu warstwy **TCP** możliwe jest zastosowanie certyfikatów SSL nie tylko do ochrony transmisji **HTTP** (co jest najpopularniejszym zastosowaniem), ale także do protokołów **IMAP, SMTP, POP3, FTP** i wielu innych.

W ciągu kilkunastu lat nastąpił znaczny rozwój technologii. Wyznacznikiem jest tutaj m.in. długość klucza stosowanego do szyfrowania. Im jest on dłuższy, tym trudniej odszyfrować treść transmisji. Obecne certyfikaty pozwalają na szyfrowanie o sile do 128/256 bit.

Zasada transmisji danych w Internecie powoduje, że wysyłana treść nie trafia bezpośrednio od użytkownika do serwera (i odwrotnie). Na swojej drodze spotyka ona wiele elementów pośredniczących (także przy korzystaniu z punktów bezprzewodowego dostępu do sieci Internet) które kierują ją pod docelowy adres.

Na każdym z etapów może znaleźć się niebezpieczny element, który przechwyci przesyłane dane. Tak właśnie w niepowołane ręce mogą trafić dane kart kredytowych, płatności, hasła do logowania i wiele innych informacji, które codziennie przesyłane są przez sieć. Należy pamiętać, że tak zdobyta informacja może spowodować wiele szkód.

Certyfikat zainstalowany na serwerze pozwala szyfrować przesyłane informacje między stroną wysyłającą, a odbierającą poufną treść (i odwrotnie). Oznacza to, że przykładowo dane Twojej karty kredytowej nie trafią w niepowołane ręce, loginy i hasła pozostaną nieznane dla potencjalnych włamywaczy. Dzięki szyfrowaniu, dane będą mogły zostać odczytane tylko przez serwer i użytkownika, który się z nim komunikuje.