

Certyfikaty TLS

HTTPS - HyperText Transfer Protocol Secure

- [HTTPS](#) - wersja protokołu HTTP wykorzystująca szyfrowanie
- wykorzystuje protokół [TLS](#) - Transport Layer Security
- wymaga certyfikatu TLS oraz klucza prywatnego
- certyfikat może być wystawiony przez [CA](#) - Certificate Authority lub samodzielnie
- wykorzystuje szyfrowanie symetryczne oraz asymetryczne
- zabezpiecza przed atakami typu *Man in The Middle*

TLS - Transport Layer Security

- na początku połączenia odbywa się proces [TLS Handshake](#)
- w trakcie procesu następuje:
 - weryfikacja certyfikatu
 - ustalenie algorytmów szyfrowania
 - wymiana kluczy
- podczas wymiany danych, pakiety TCP są zaszyfrowane

Certyfikat TLS

- certyfikat zawiera:
 - klucz publiczny
 - dane o właścicielu
 - dane o CA
 - datę ważności
- można go uzyskać samodzielnie lub za pośrednictwem CA
- może być pozyskany za darmo lub za opłatą
- opcja bezpłatna: [Let's Encrypt](#)

Let's Encrypt

- [Let's Encrypt](#) - organizacja non-profit wystawiająca bezpłatnie certyfikaty TLS
- certyfikaty ważne są przez 90 dni
- aby pozyskać lub odnowić certyfikat, należy udowodnić, że jesteśmy właścicielem domeny, poprzez:
 - dodanie określonego pliku do serwera
 - dodanie rekordu DNS
- proces pozyskania oraz odnowienia certyfikatu może być zautomatyzowany poprzez narzędzie [Certbot](#)