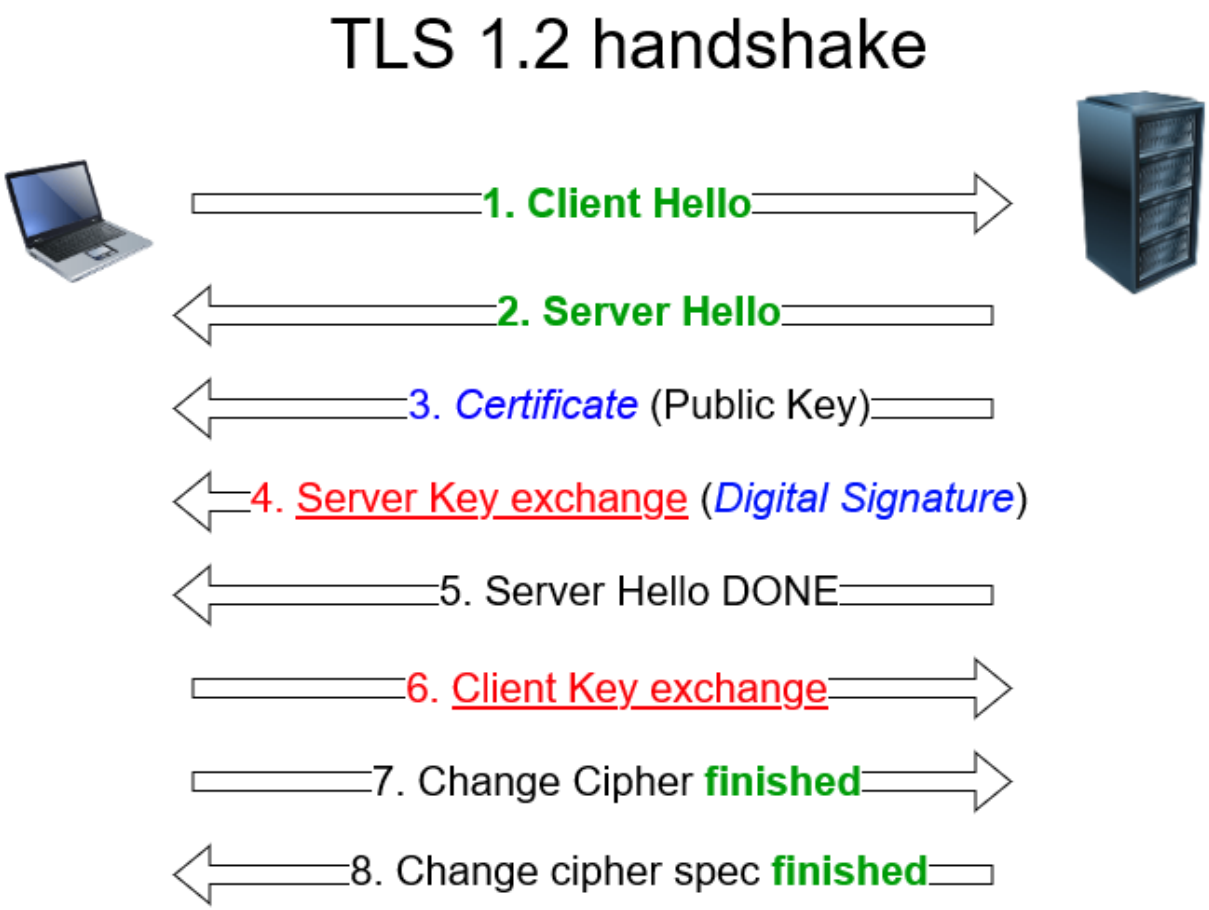
Security: Schemat działania TLS 1.2

(TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, 256-bitowe klucze, TLS 1.2)

Transport Layer Security



Shared Secret (e.g. Elliptic Curve Diffie-Hellman Ephemeral - ECDHE)

Server Authenticity (e.g. Rivest–Shamir–Adleman - RSA)

Mechanism to make sure nobody tampered with the message

TLS 1.2 Handshake

1. Client Hello

Klient inicjuje połączenie, wysyłając wiadomość **ClientHello**, która zawiera:

- obsługiwaną wersję protokołu TLS
- listę wspieranych zestawów szyfrów (cipher suites)

- losowy ciąg bajtów (client random)
- opcjonalne rozszerzenia, takie jak SNI (Server Name Indication)

Celem tej wiadomości jest rozpoczęcie negocjacji parametrów bezpieczeństwa z serwerem.

2. Server Hello

([Microsoft Learn][1])

Serwer odpowiada wiadomością **ServerHello**, która zawiera:([Wikipedia][2])

- wybraną wersję protokołu TLS
- wybrany zestaw szyfrów
- losowy ciąg bajtów (server random)
- opcjonalne rozszerzenia

Ta wiadomość potwierdza wybór wspólnych parametrów bezpieczeństwa dla sesji.

3. Certificate (Public Key)

Serwer przesyła swój certyfikat X.509 zawierający klucz publiczny. Klient wykorzystuje ten certyfikat do:([catchpoint.com][3])

- weryfikacji tożsamości serwera
- uzyskania klucza publicznego do szyfrowania premaster secret([ManageEngine][4])

4. Server Key Exchange (Digital Signature)

W zależności od wybranego zestawu szyfrów, serwer może wysłać wiadomość **ServerKeyExchange**, która zawiera:([Wikipedia][2])

- dodatkowe parametry wymiany kluczy (np. dla DHE lub ECDHE)([Wikipedia][2])
- podpis cyfrowy tych parametrów

Klient weryfikuje podpis, aby upewnić się, że parametry pochodzą od autoryzowanego serwera.

5. Server Hello Done

([Taro][5])

Serwer wysyła wiadomość **ServerHelloDone**, sygnalizując zakończenie swojej części negocjacji. Klient może teraz kontynuować proces handshake.

6. Client Key Exchange

Klient generuje premaster secret i przesyła go do serwera w wiadomości **ClientKeyExchange**. W zależności od metody wymiany kluczy:([ManageEngine][4])

- dla RSA: premaster secret jest szyfrowany kluczem publicznym serwera([Cloudflare][6])
- dla DHE/ECDHE: klient przesyła swoje parametry wymiany kluczy([Taro][5])

Obie strony wykorzystują premaster secret oraz losowe wartości do obliczenia wspólnego master secret.([Wikipedia][2])

7. Change Cipher Spec

([Fortinet Docs][7])

Klient wysyła wiadomość **ChangeCipherSpec**, informując serwer, że od tego momentu wszystkie wiadomości będą szyfrowane przy użyciu uzgodnionych parametrów.([takethenotes.com][8])

8. Finished

([Fortinet Docs][7])

Klient wysyła wiadomość **Finished**, która jest pierwszą zaszyfrowaną wiadomością w sesji. Zawiera ona skrót wszystkich wcześniejszych wiadomości handshake, co umożliwia serwerowi weryfikację integralności i autentyczności negocjacji.

Po otrzymaniu i weryfikacji wiadomości **Finished**, serwer również wysyła swoje wiadomości **ChangeCipherSpec** i **Finished**, kończąc proces handshake.

Od tego momentu komunikacja między klientem a serwerem jest szyfrowana i bezpieczna.

źródła:

1. https://learn.microsoft.com/en-us/windows/win32/secauthn/tls-handshake-protocol?utm_source=chatgpt.com „TLS Handshake Protocol - Win32 apps | Microsoft Learn”
2. https://en.wikipedia.org/wiki/Transport_Layer_Security?utm_source=chatgpt.com „Transport Layer Security - Wikipedia”
3. https://www.catchpoint.com/blog/wireshark-tls-handshake?utm_source=chatgpt.com „Dissecting TLS Using Wireshark”
4. https://www.manageengine.com/key-manager/information-center/what-is-ssl-tls-handshake.html?utm_source=chatgpt.com „What is SSL/TLS handshake? | TLS/SSL handshake protocol - ManageEngine Key Manager Plus”
5. https://www.jointaro.com/interview-insights/google/describe-ssl-key-exchange-in-tls/?utm_source=chatgpt.com „Describe SSL key exchange in TLS Interview Question for Google”
6. https://www.cloudflare.com/pl-pl/learning/ssl/what-happens-in-a-tls-handshake/?utm_source=chatgpt.com „What happens in a TLS handshake? | SSL handshake | Cloudflare”
7. https://docs.fortinet.com/document/fortimail/7.2.2/administration-guide/887607/how-tls-ssl-works?utm_source=chatgpt.com „How TLS/SSL works | FortiMail 7.2.2 | Fortinet Document Library”

8. https://takethenotes.com/ssl-tls/?utm_source=chatgpt.com „SSL/TLS - Unlocking The Secrets Of Secure Communication | Take The Notes”
9. https://www.rfc-editor.org/rfc/rfc5246?utm_source=chatgpt.com „RFC 5246: The Transport Layer Security (TLS) Protocol Version 1.2”
10. https://www.cloudflare.com/learning/ssl/what-happens-in-a-tls-handshake/?utm_source=chatgpt.com „What happens in a TLS handshake? | SSL handshake | Cloudflare”