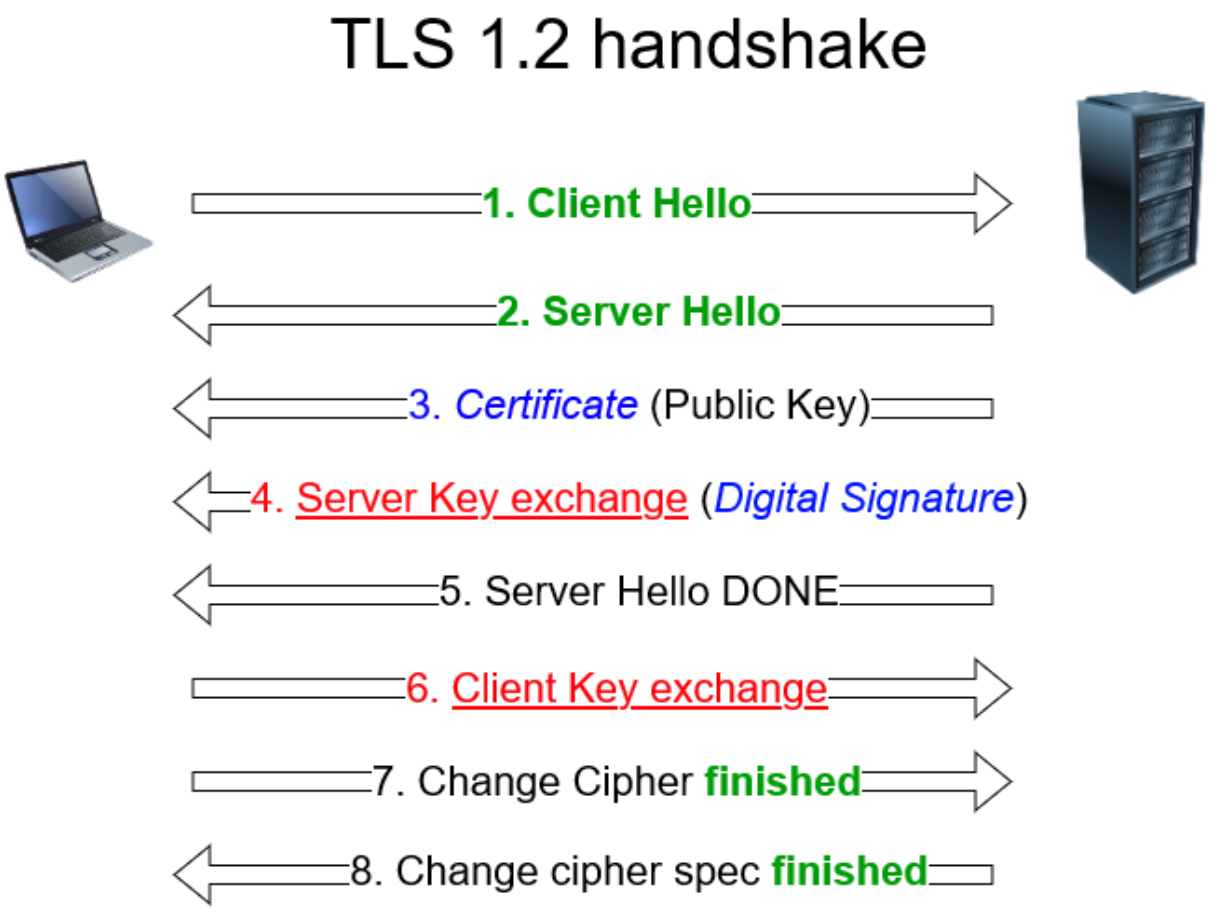
Security: TLS 1.2 operating scheme

(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

The client initiates the connection by sending the message **ClientHello**message, which contains:

- the supported version of the TLS protocol
- list of supported cipher suites

- random byte string (client random)
- optional extensions such as SNI (Server Name Indication)

The purpose of this message is to start negotiating security parameters with the server.

Server Hello

([Microsoft Learn][1])

The server responds with the message **ServerHello**message which contains:([Wikipedia][2])

- the selected TLS protocol version
- the selected cipher suite
- random sequence of bytes (server random)
- optional extensions

This message confirms the selection of common security parameters for the session.

3 Certificate (Public Key)

The server sends its X.509 certificate containing the public key. The client uses this certificate to:([catchpoint.com][3])

- verify the identity of the server
- obtain the public key for encrypting the premaster secret([ManageEngine][4])

4th Server Key Exchange (Digital Signature)

Depending on the selected cipher suite, the server can send a message **ServerKeyExchange**message that contains:([Wikipedia][2])

- additional key exchange parameters (e.g. for DHE or ECDHE)([Wikipedia][2]).
- the digital signature of these parameters

The client verifies the signature to ensure that the parameters come from an authorised server.

5 Server Hello Done

([Taro][5])

The server sends a message **ServerHelloDone**message, signalling the end of its part of the negotiation. The client can now continue with the handshake process.

6 Client Key Exchange

The client generates a premaster secret and sends it to the server in a message **ClientKeyExchange**. Depending on the key exchange method:([ManageEngine][4])

- for RSA: the premaster secret is encrypted with the server's public key([Cloudflare][6])
- for DHE/ECDHE: the client sends its key exchange parameters([Taro][5])

Both parties use the premaster secret and random values to compute the shared master secret.([Wikipedia][2])

7 Change Cipher Spec

([Fortinet Docs][7])

The client sends a message **ChangeCipherSpec**, informing the server that from this point onwards all messages will be encrypted using the agreed parameters.([takethenotes.com][8])

8 Finished

([Fortinet Docs][7])

The client sends a message **Finished**message, which is the first encrypted message in the session. It contains a digest of all previous handshake messages, allowing the server to verify the integrity and authenticity of the negotiation.

After receiving and verifying the message **Finished**message, the server also sends its **ChangeCipherSpec** i **Finished**message, completing the handshake process.

From this point onwards, the communication between client and server is encrypted and secure.

sources:

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”