Aalto University

Network Security:
TLS 1.3 PSK and session resumption

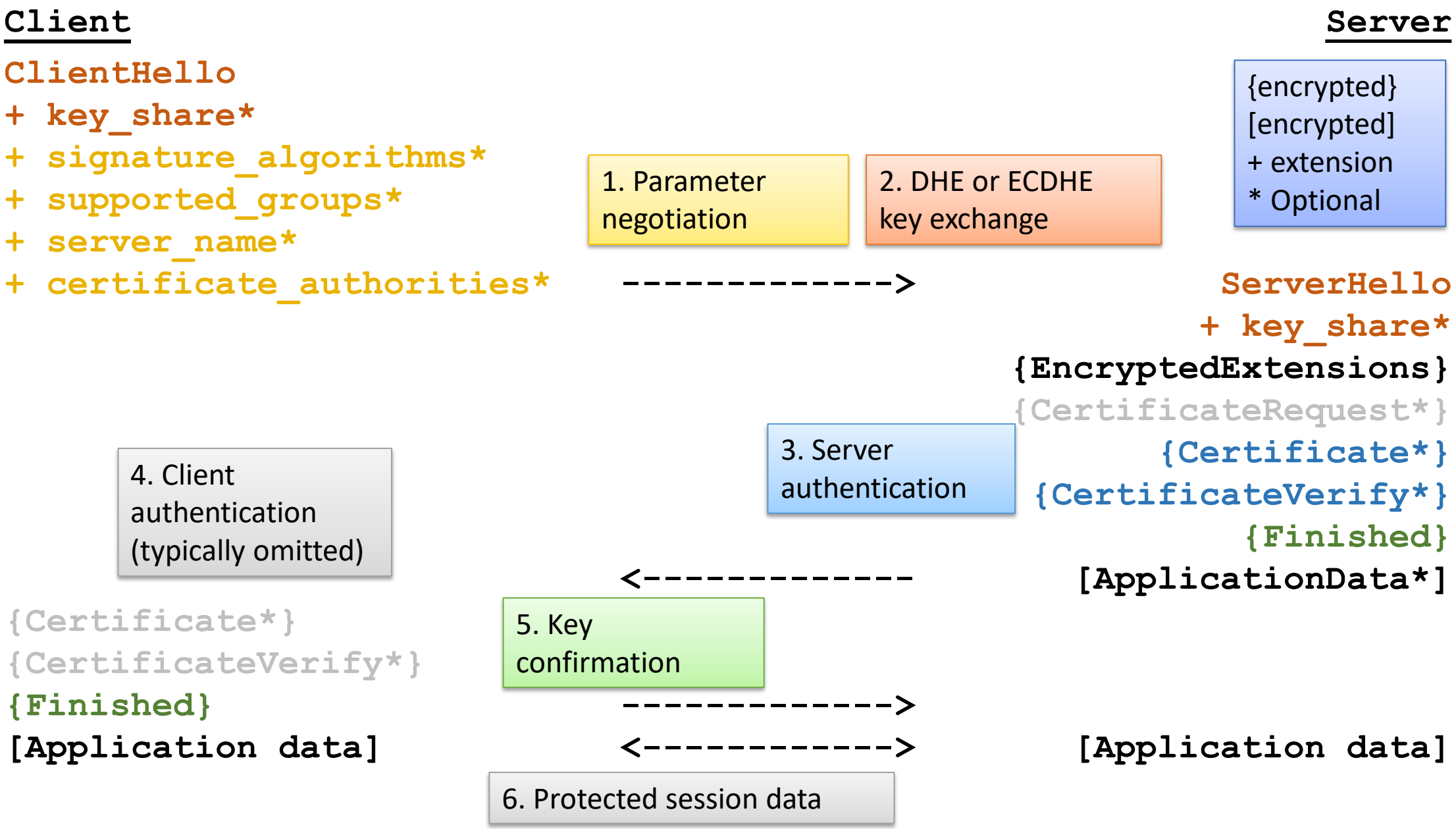
Tuomas Aura, Aalto University

CS-E4300 Network security

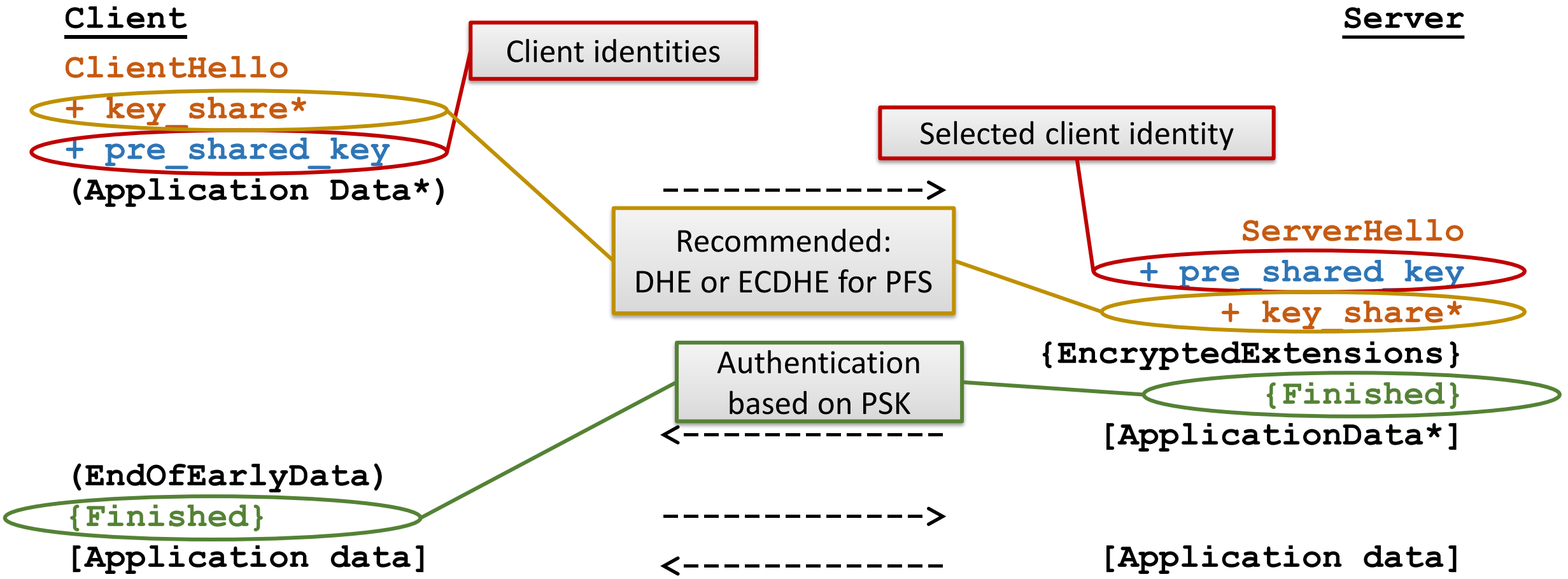
Outline

- Recall TLS 1.3 full handshake
- Pre-shared key (PSK) mode
- Session resumption

TLS 1.3 full handshake



Pre-shared key (PSK) mode

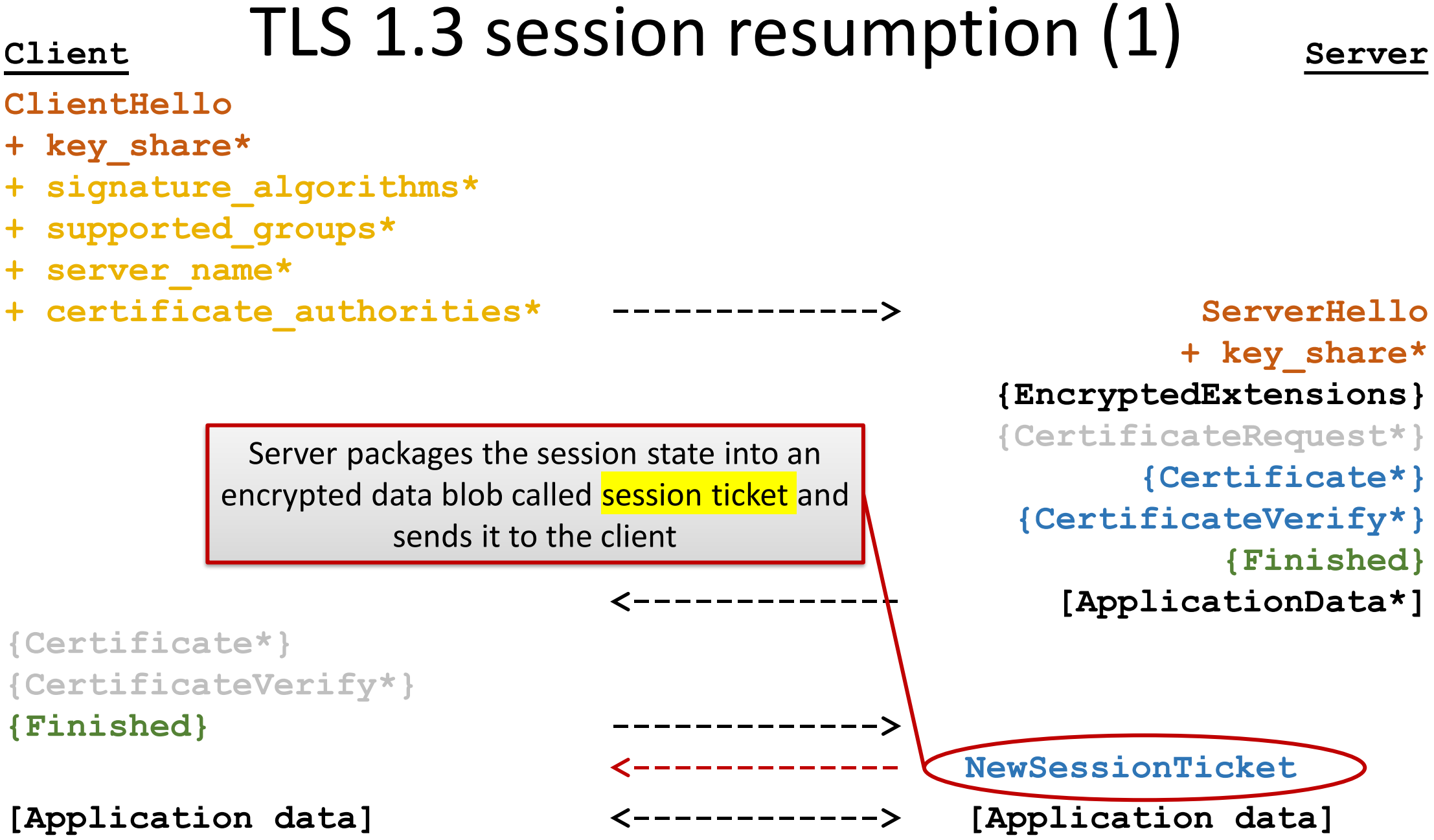


Pre-shared key (PSK) mode

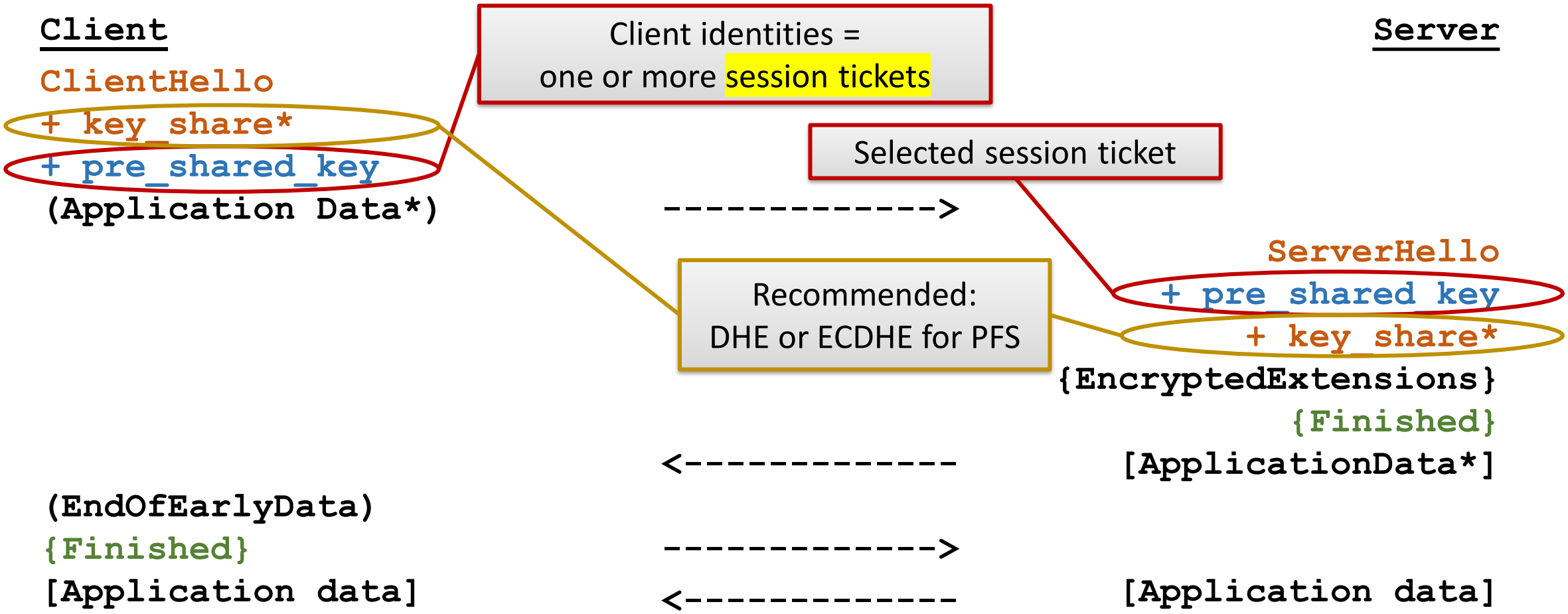
1. C → S: N_C , g^x, ClientIdentity
2. S → C: N_S , g^y, $HMAC_{Kfks}(TH)$, early data
3. C → S: $HMAC_{Kfkc}(TH)$

- Mutual authentication based on a pre-established identity and session key (*external PSK*)
  - PSK = pre-established shared key between C and S
  - HMAC keys K_{fks} and $K_{fkc\ in}$ for the Finished message are derived from PSK, g^{xy} and TH; and so are the session keys

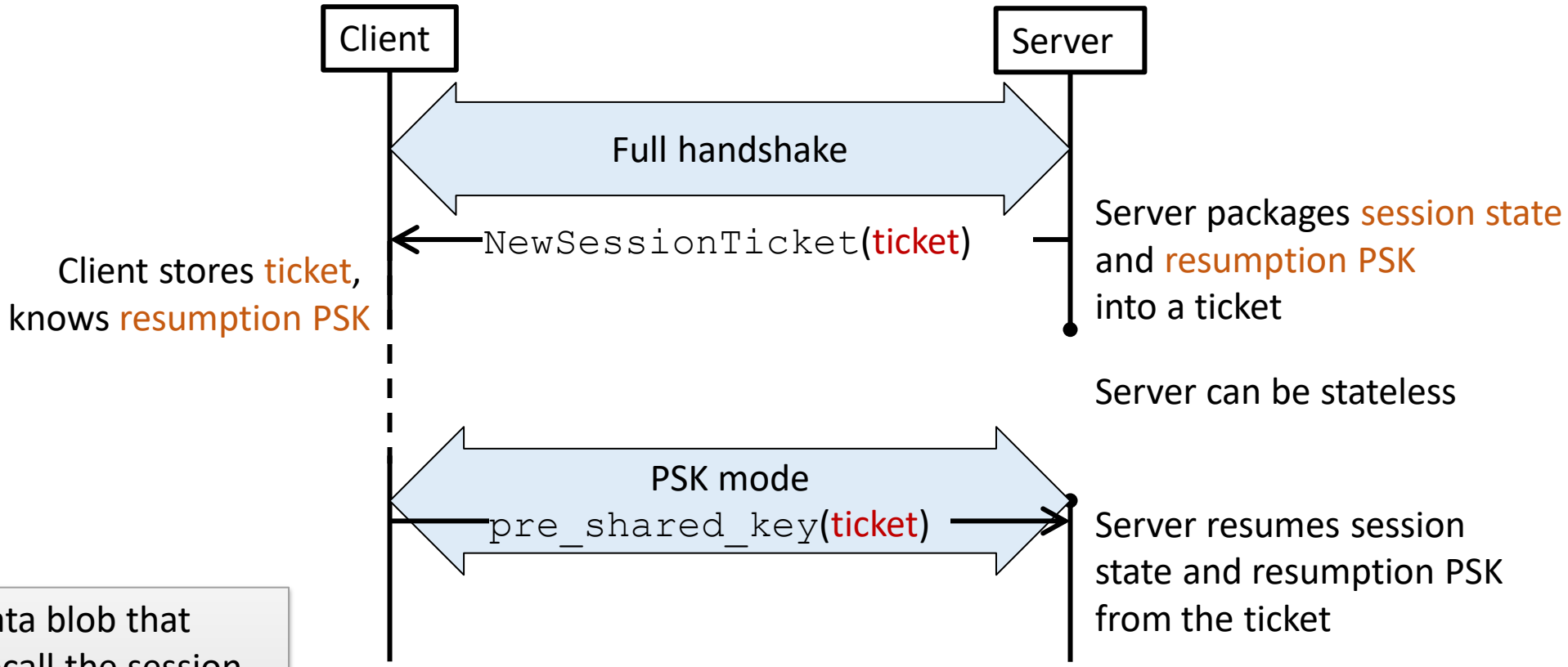
TLS 1.3 session resumption (1)



TLS 1.3 session resumption (2)



TLS 1.3 session resumption timeline



Ticket = opaque data blob that helps the server recall the session. Typically contains encrypted session state and resumption PSK. Only the server itself can decrypt the tickets that has created

TLS 1.3 session resumption uses

- TLS 1.3 session resumption = PSK mode handshake with ticket as client identity and resumption key as the PSK
  - Currently the main purpose of the PSK mode
- When useful?
  - Server does not want to store the TLS sessions over idle periods
  - If client is authenticated with smartcard, avoids repeated user action
  - Mobile clients keep changing their IP address and need frequent reconnection
  - Resume the session with a different server instance in the cloud

Key derivation

Inputs to key derivation:

1. PSK (external PSK or resumption PSK)
2. DHE/ECDHE secret

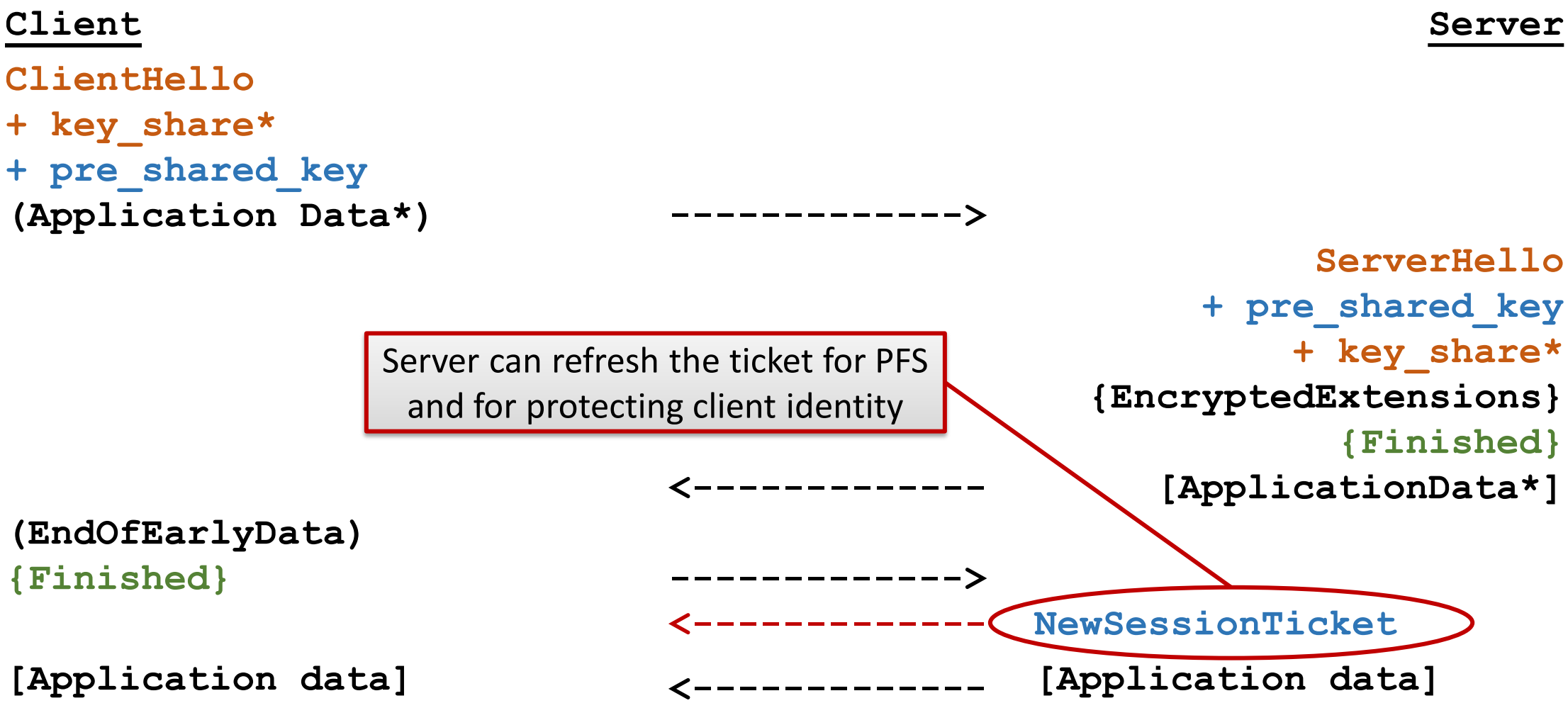
} one or both, as available

3. Transcript of handshake messages, up to the point where the key is derived

Keys:

- client_early_traffic_secret → used to derive AEAD keys for early data in 0-RTT (…)
- client/server_handshake_traffic_secret → used to derive AEAD keys for handshake messages {…} and Finished HMAC keys
- client/server_application_traffic_secret_N → used to derive AEAD encryption keys for post-handshake application data and messages […]
- resumption_master_secret and ticket_nonce → derive resumption PSK
- exporter_master_secret → used to create keys for the application layer

TLS 1.3 session resumption and identity

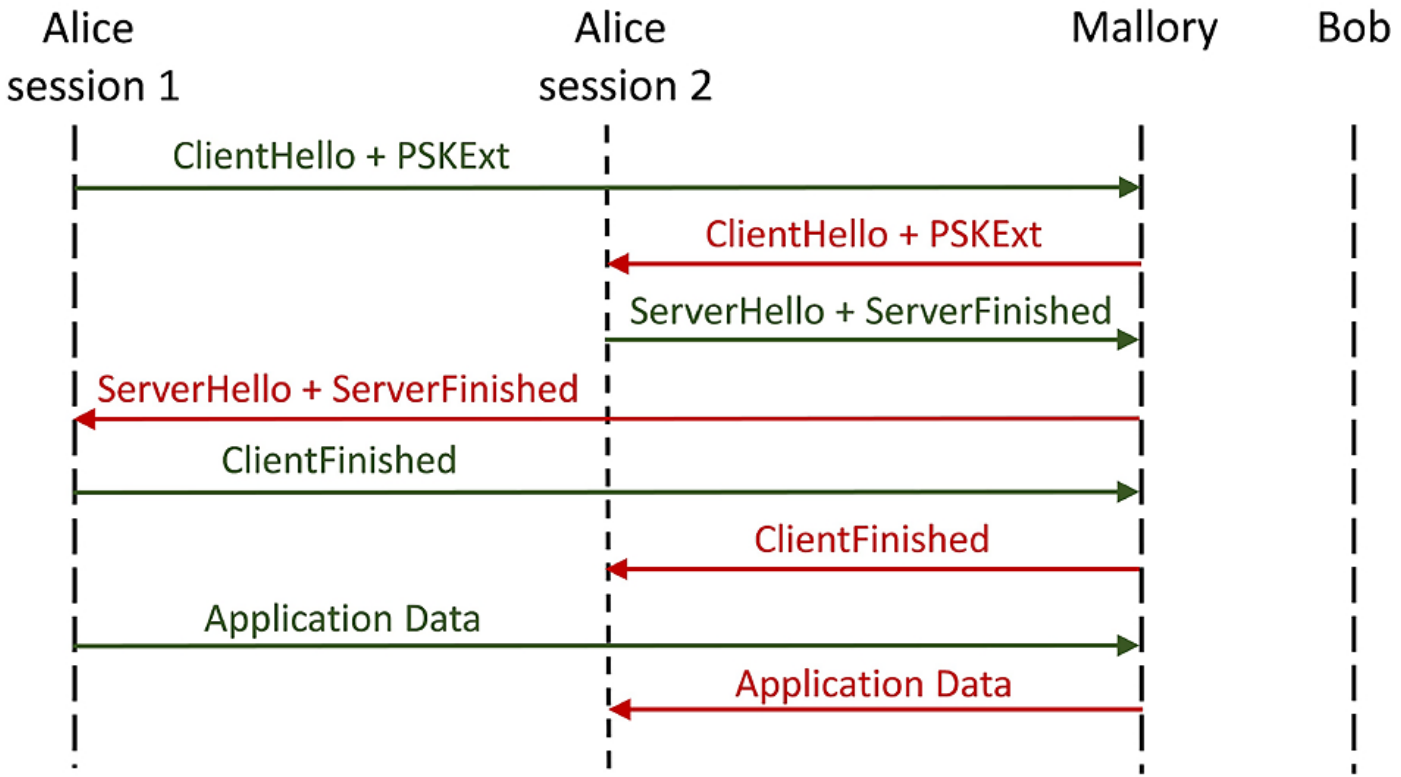


Identity protection?

- Session tickets are encrypted
- Session ticket can become a pseudo-identifier
  → Server should regularly refresh ticket

“Selfie attack”

- Reflection attack against external (out-of-band) PSK
  - Trick the client to connect to itself
  - Assumes the same entity can be both client and server
- PSK used mistakenly as a group key for two parties
  - Group key only authenticates the group, not the individual
- Solution: Use different PSK for each direction
  - For each PSK, Alice is either the client or server, never both for the same PSK



[Nir Drucker & Shay Gueron, Selfie: reflections on TLS 1.3 with PSK, 2019]