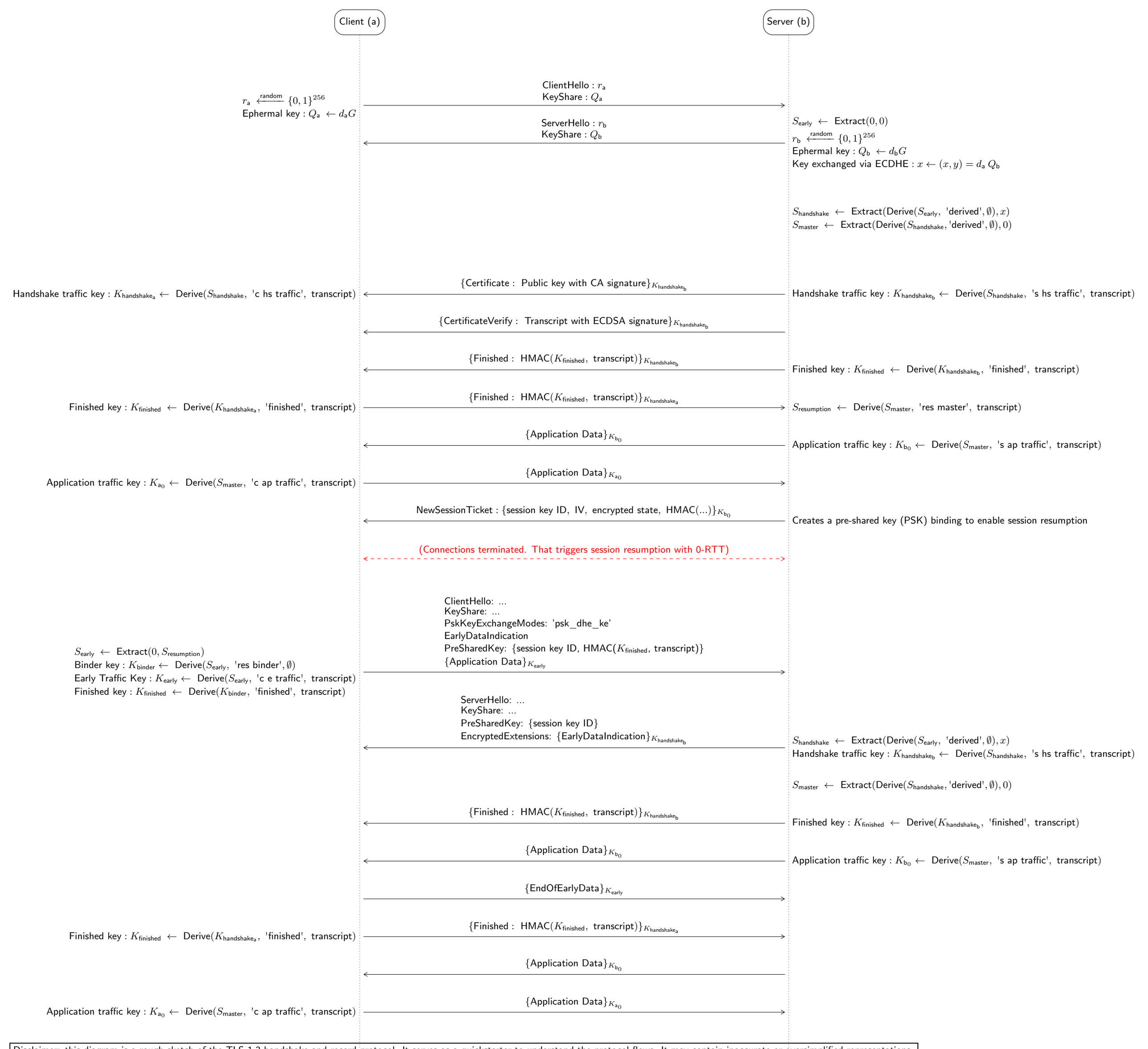

Disclaimer: this diagram is a rough sketch of the TLS 1.3 handshake and record protocol. It serves as a quickstarter to understand the protocol flows. It may contain inaccurate or oversimplified representations.
1) TLS Settings
Cipher Suite: TLS_AES_128_GCM_SHA256
Digital Signature: ecdsa_secp256r1_sha256
Key Exchange: secp256r1 (NIST P-256) with (G, n) as part of domain parameters, with public and private key in the form of (Q, d)
Pre-Shared Key Cipher: TLS_ECDHE_PSK_WITH_AES_256_CBC_SHA384
2) Protocol Notations
Key Extraction Function: Extract(salt, keying material)
Key Derive Function: Derive(secret, label, transcript), where transcript is the concatenation of each included handshake message.
Encryption: $\{\text{plaintext}\}_{key}$, which denotes an AEAD-Encrypt operation with write key and IV generated from key.