Mutual authentication means both the client verifies the AP's legitimacy and the AP verifies the client's legitimacy.

The 4-way handshake uses the shared PMK (established via a Pre-Shared Key in Personal mode or 802.1X/EAP in Enterprise mode) to generate and validate cryptographic keys, ensuring both parties are authorized**.**

Mutual Authentication is Ensured

- **Shared PMK as the Root of Trust:**
    - Both the AP and client must possess the same PMK (from PSK or EAP authentication). The handshake tests this by requiring both to derive the same PTK, which depends on the PMK, ANonce, SNonce, and other parameters.
    - If either party has an incorrect PMK, the PTK and MICs will mismatch, causing the handshake to fail.
- **MIC for Integrity and Authenticity:**
    - The MIC in Messages 2, 3, and 4 is a cryptographic hash (using the KCK from the PTK) that verifies the integrity of the handshake messages and proves each party's knowledge of the PMK.
    - The client's MIC in Message 2 authenticates the client to the AP.
    - The AP's MIC in Message 3 authenticates the AP to the client.
- **Nonces for Freshness:**
    - The random ANonce and SNonce ensure the handshake is unique for each session, preventing replay attacks where an attacker reuses old handshake messages to impersonate the AP or client.
    - Both parties contribute nonces to the PTK derivation, ensuring both are actively participating and not replaying pre-recorded messages.
- **No PMK Transmission:**
    - The PMK is never sent over the air, reducing the risk of interception. Instead, the handshake relies on derived keys (PTK) and MICs to prove PMK knowledge, maintaining security.