PMK

- **T**he PMK is a shared secret key used as the foundation for generating encryption keys in a Wi-Fi network.
- Source:
    - In Personal mode (PSK): The PMK is derived from the pre-shared key (passphrase) using a key derivation function (e.g., PBKDF2 in WPA2).
    - In Enterprise mode (802.1X/EAP): The PMK is generated during the authentication process between the client and an authentication server (e.g., RADIUS).
- The PMK is not used directly for encryption but serves as the root key for deriving other keys during the handshake.

Role of PMK in the 4-Way Handshake

The 4-way handshake uses the PMK to derive and distribute the Pairwise Transient Key (PTK), which is used for unicast data encryption, and to confirm that both the client and AP possess the same PMK. Here's how the PMK is involved in each step:

1. Message 1 (AP to Client):
    - The AP generates a random nonce (ANonce) and sends it to the client.
    - The PMK is not transmitted but is already known to both parties (from PSK or EAP authentication).
    - The client uses the PMK, ANonce, its own nonce (SNonce), and other parameters (e.g., MAC addresses) to compute the PTK using a pseudo-random function (PRF).
2. Message 2 (Client to AP):
    - The client generates its own nonce (SNonce) and computes the PTK using the PMK, ANonce, SNonce, and other data.
    - The client sends SNonce and a Message Integrity Code (MIC) to the AP, proving it knows the PMK (the MIC is computed using a key derived from the PTK).
    - The AP verifies the MIC usin**g its own PMK-derived PTK, confirming the client's authenticity.**
3. Message 3 (AP to Client):
    - The AP computes the PTK (using the PMK, ANonce, SNonce, etc.) and derives the Group Temporal Key (GTK) for multicast/broadcast traffic.
    - The AP sends the GTK (encrypted with the PTK) and another MIC to the client, confirming it knows the PMK and instructing the client to install the PTK and GTK.
4. Message 4 (Client to AP):
    - The client sends a final acknowledgment to the AP, confirming receipt and installation of the PTK and GTK.

    - The PMK’s role is complete, as the PTK and GTK are now installed for securing the session.

Key Outcomes Involving the PMK

- PTK Derivation: The PMK is the seed for generating the PTK, which is split into:
    - Key Confirmation Key (KCK): For MICs to verify handshake integrity.
    - Key Encryption Key (KEK): For encrypting keys like the GTK.
    - Temporal Key (TK): For encrypting unicast data.
- Mutual Authentication: The handshake ensures both the client and AP possess the same PMK, preventing unauthorized access.
- Session Security: The PMK enables the creation of fresh, session-specific keys (PTK and GTK), ensuring data confidentiality and integrity without exposing the PMK.

Why the PMK is Critical

- The PMK is the root of trust for the handshake. If it’s compromised (e.g., a weak PSK is brute-forced), the entire session can be decrypted.
- It remains static for the session (or longer in PSK mode), but the PTK and GTK are unique per session, reducing the impact of a single compromised session.
- In WPA3, the PMK’s role is enhanced by the Simultaneous Authentication of Equals (SAE) handshake, which strengthens PMK derivation against offline attacks.