# **WPA3 Process as a Scenario**

### **1. Password → The Secret Invite**

* You and your friend both know the *secret word* to enter the club (“Phoenix”).
* This isn’t shouted out — you never say it directly.

### **2. SAE (Dragonfly/ECDH) → Proving You Know the Password Without Saying It**

* At the door, the bouncer (AP) and you (Client) play a challenge game:  
  + You both roll dice (random numbers = **nonces**).
  + You each combine your dice rolls + the secret word in a special way (ECDH math).
  + You show each other the result, not the dice or the password.
* If your answers match, the bouncer knows **you really have the password**, even though you never said it.

*(This stops an eavesdropper outside the club — they see your moves, but can’t figure out the secret word.)*

### **3. PMK → The VIP Bracelet**

* Once you pass the game, the bouncer gives you a **VIP bracelet** (the Pairwise Master Key).
* This bracelet is unique for tonight only. Tomorrow, you’ll get a new one.
* Nobody else can copy it because it’s tied to your random rolls.

### **4. 4-Way Handshake → Double-Checking the Bracelet**

* Before you step inside, security checks your bracelet in **4 quick steps** (the handshake).
* Both sides prove they have the same bracelet without taking it off.
* Now they trust each other fully.

### **5. AES-GCM + Forward Secrecy → Secure Party Inside**

* Inside the club, all conversations are encrypted with **AES-GCM**.
* Even if someone records the whole party, they can’t decode it.
* When you leave, your bracelet is destroyed (**forward secrecy**) so old recordings are useless.

# **Sticky Takeaway**

WPA3 is like a **nightclub**:

* Password = secret invite.
* SAE/Dragonfly = proving you know the invite without saying it.
* PMK = VIP bracelet (session key).
* 4-way handshake = double-checking bracelet.
* AES-GCM + Forward Secrecy = safe party where past recordings are meaningless.