ESP32 BUG REPORT TEMPLATE

1. Bug 名称 / Bug Name
   Transition Disable SAE-PK → SAE not Working

2. ESP-IDF 版本号/ ESP-IDF Version
   Espressif IDF v5.1.1

3. 硬件模块 / Hardware Information
   Keystudio ESP32 Core Board, with ESP32-WROOM-32

4. Bug 描述 / Bug Description
   I was working with SAE-PK. If i enable SAE-PK in Automatic Mode, and connect to an AP with Transition disable 0x03 (thus preventing downgrade from WPA3 → WPA2 and from SAE-PK → SAE), the SAE-PK Transition Mode bit is ignored. The transition disable mechanism works for WPA3 → WPA2. On the other hand, if I consider Transition Disable between SAE-PK → SAE, then I am able to make the board connect to an AP with just SAE (not SAE-PK).

   This is the scenario: Let's suppose to have a public café with a WPA3 with SAE-PK AP, for which the password is written on a sign. An attacker can easily create an evil-twin (with just SAE, but with the right password) and induce the ESP32 to connect it. Indeed, even though the ESP32 supports SAE-PK, it is useless if it is set in "automatic mode" (the default mode for what I understand). The ESP32 can connect to the real AP, but nothing will prevent it to join the rogue network (because the transition disable seems not to be working properly, thus nothing is preventing ESP32 to be downgraded).

5. 详细的测试流程 / Test Steps
   1. Launch an AP (with Hostapd) with SAE-PK and Transition Disable 0x03.
   2. Make the ESP32 board connect to it (in SAE-PK Automatic mode). (It connects)
   3. Stop the AP without turning off the ESP32 board, and then launch an evil-twin AP with same password, but without SAE-PK (se WPA3 with plain SAE).
   4. Wait for the ESP32 board to connect. (It connects...)

   I Tried the same experiment with wpa-supplicant, and it is not affected by this problem.

6. 参考代码 及 log 输出 / Test Codes & Log Output
   基于 ESP-IDF 请提供可复现问题的参考代码、log 输出
   Please find attached to the email the logs from VSCode terminal and from hostapd.

   注：参考代码是编译后可直接运行并复现问题的，请将参考代码 *.c/*.h 以附件形式提交。
   Note: Test codes should be able to run after compilation and also help reproduce the bug. You can provide reference codes *.c/*.h as an attachment.
   I have used the code from the ESP-IDF example “station” (available in Visual Studio Code). It has been slightly modified to explicitly select the SAE-PK mode (between automatic, only and disabled), and activate the Transition Disable mechanism.
   Please find attached to the email the code that I used.

7. 其它 / Others
   I started inspecting the source code (the one that I found in esp-idf/* folders), and I narrowed the problem down to the esp_wpas_glue.c file. I noticed that it is the counterpart of the official wpa-supplicant wpas_glue.c file. In particular, I compared these two functions from the two files. Please find attached the comparison file.