**2. Detailed Test Case Elaboration**

**Test Case ID: TC02**

**Title: Authentication Vector Generation**

**Objective:**

To verify that the HSS generates the correct authentication vectors (AVs) in response to authentication requests from the Mobility Management Entity (MME) via the HLR proxy.

**Preconditions:**

* HSS and HLR integrated over Diameter (S6a interface).
* A valid subscriber profile (IMSI, K, OPC, AMBR, etc.) exists in the HSS database.

**Test Steps:**

1. Power on a UE with a valid eSIM.
2. The UE sends an Attach Request to the network.
3. MME initiates an Authentication Information Request (AIR) towards the HSS.
4. HSS generates authentication vectors (RAND, AUTN, XRES, KASME) using stored credentials.
5. HSS sends an Authentication Information Answer (AIA) back to the MME with AVs.
6. MME forwards the AVs to the UE.
7. UE computes the response and sends it to the MME.
8. MME compares the UE response with XRES received from HSS.

**Expected Results:**

* Authentication vectors are correctly generated by the HSS.
* The UE and MME successfully complete mutual authentication.
* Attach procedure continues successfully.

**Postconditions:**

* Subscriber session is active.
* Data session can be initiated.

**3. Roaming Registration Failure Troubleshooting**

**Scenario:**

An eSIM fails to register on a visited network during roaming tests.

**Troubleshooting Methodology:**

1. **Verify IMSI Reachability:**
   * Check if the visited network is correctly routing S6a requests to the home HSS.
   * Use trace tools to confirm Diameter requests (ULR/AIR) reach HSS.
2. **Check Roaming Agreements:**
   * Validate that roaming agreements exist between home and visited networks.
   * Confirm IMSI ranges are shared and accepted.
3. **Analyze Subscriber Profile:**
   * Ensure the roaming feature is enabled in the subscriber's HSS profile.
   * Check for barring flags or incorrect configurations (e.g., roaming not allowed).
4. **Monitor Authentication Flows:**
   * Inspect Diameter messages (AIR/AIA).
   * Ensure authentication vectors are generated and valid.
5. **SIM/eSIM Status:**
   * Validate if the eSIM profile is active and not locked or expired.

**Possible Causes:**

* No S6a connection between VPLMN and HPLMN.
* Roaming not permitted in subscriber profile.
* Authentication vector mismatch due to outdated keys.
* IMSI not recognized or provisioned incorrectly.

**4. Roaming Data Traffic Failure Troubleshooting**

**Scenario:**

eSIM successfully registers on the roaming network but cannot initiate or maintain data sessions.

**Troubleshooting Steps:**

1. **Verify Bearer Establishment:**
   * Confirm that the EPS bearer is created correctly by the PGW.
   * Check for Create Session and Modify Bearer Request/Response flows.
2. **Inspect APN Configuration:**
   * Ensure correct APN is selected and DNS resolution works.
   * Validate APN mappings in the HSS profile.
3. **Check GTP-U Path:**
   * Verify user plane (GTP-U) tunnel between SGW and PGW is established.
   * Ping or trace between eNodeB and PGW to check latency or drops.
4. **QoS & Policy Issues:**
   * Validate if the PCC rules allow internet traffic.
   * Check PCRF policies assigned to the subscriber.
5. **Firewall/NAT Inspection:**
   * Check whether firewalls block traffic at the PGW or interconnect level.
   * Analyze NAT translation correctness.

**Possible Causes:**

* APN misconfiguration.
* GTP-C tunnel established but GTP-U path failure.
* Incorrect PCC rules or blocked traffic by firewall.
* MTU mismatch causing packet drops.

**5.Please analyze the attached Diameter captures (port 3878) (***failure3878.pcap***) and provide answers to the following:**

**Steps to Analyze the PCAP Locally Using Wireshark:**

1. **Open the PCAP File:**
   * Use Wireshark and open failure3878 (1).pcap.
2. **Apply a Filter:**
   * Use this display filter:

Nginx = diameter

1. **Look at the First Few Diameter Messages:**
   * Focus on messages like:
     + Update-Location-Request (ULR)
     + Update-Location-Answer (ULA)
     + Authentication-Information-Request (AIR)
     + Authentication-Information-Answer (AIA)
2. **Identify Key Fields:**
   * AVP: Result-Code
   * AVP: Experimental-Result-Code
   * Any AVP with error messages or flags

**📋 What to Collect and Share:**

If you want me to help further, you can share the following from Wireshark:

* A screenshot or list of the first few Diameter packets and their **Result-Code** values.
* Any **error messages** shown in the AVPs.
* Source and Destination IPs (helps identify network elements).

**🔍 Based on a Typical Diameter Failure Scenario:**

If you saw a **Result-Code like 5001** or DIAMETER\_ERROR\_UNKNOWN\_USER, here's a sample answer to your original questions:

**PCAP Analysis (Based on Common Failure)**

* **Network Elements Involved:**
  + **MME (Mobility Management Entity)** – initiates the authentication and location update.
  + **HSS (Home Subscriber Server)** – handles subscriber data and authentication vectors.
* **Protocol Used:**
  + **Diameter** over TCP (Port **3878**).
* **Purpose of the Protocol:**
  + Diameter (S6a interface) is used for exchanging authentication, subscriber profile, and mobility management information between MME and HSS.
* **Reason for Failure:**
  + The Update-Location-Answer (ULA) or Authentication-Information-Answer (AIA) contains a **Result-Code** like 5001 (DIAMETER\_ERROR\_UNKNOWN\_USER), which means:
    - The IMSI is not recognized in the HSS.
    - Likely due to the eSIM not being provisioned or a database sync issue.