**SA WG2 Meeting #161 S2-2402996**

**February 26 – March 1, 2024, Athens, Greece**

**Source: InterDigital Inc.**

**Title: Key Issue #4, New Solution, Network initiated User Identity Authentication for non-3GPP devices behind UE or 5G-RG**

**Document for: Approval**

**Agenda Item: 19.8**

**Work Item / Release: FS\_UIA\_ARC / Rel-19**

*Abstract of the contribution:* *This paper proposes solution for Key Issue #4.*

# 1 Discussion

This paper proposes solution to Key Issue #4: "Identifying non-3GPP Devices Connecting behind a UE or 5G-RG".

# 2 Proposal

It is proposed to include the following changes in TR 23.700-32 V0.1.0.

 **\* \* \* \* Start of Changes \* \* \* \***

## 6.0 Mapping of Solutions to Key Issues

Table 6.0-1: Mapping of Solutions to Key Issues

|  |  |  |
| --- | --- | --- |
| Solutions |  |  |
|  | <Key Issue #1> | <Key Issue #2> | <Key Issue #3> | <Key Issue #4> |
| #1 |  |  |  |  |
| #2 |  |  |  |  |
| #x |  |  |  | x |

 **\* \* \* \* Next Change – All New Text \* \* \* \***

## 6.X Solution #X: Network initiated Authentication for non-3GPP devices behind UE or 5G-RG

### 6.X.1 Key Issue mapping

This solution addresses Key Issue #4: "Identifying non-3GPP Devices Connecting behind a UE or 5G-RG".

### 6.X.2 Description

In this solution, the UE establishes a PDU Session that can be used for forwarding traffic to and from non-3GPP devices that are associated with a user identity. When the UPF detects a new unauthorized non-3GPP device generating uplink traffic by detecting a new source IP Address, Port Number, or MAC Address, the UPF notifies the SMF and the SMF can initiate EAP Authentication between the non-3GPP device and a AAA Server. Once the non-3GPP device is authenticated and authorized by the AAA, the SMF can inform the UPF to allow traffic to and from the new non-3GPP device.

NOTE: In the scenario where a MAC Address changes (i.e. due to randomized MAC addresses), the UPF detects a new source address and notifies the SMF which initiates the authentication procedure again.

Once the user identity of the non-3GPP device is authenticated, the SMF can use policy information from the user profile to update the PDU Session’s QoS Rules, QoS Profile, and N4 Rules for the non-3GPP device’s traffic.

The UE in this solution can be a 5G-RG.

### 6.X.3 Procedures

The procedure Figure 6.x.3-1 includes the following pre-conditions.

* The UE is pre-configured with a DNN/S-NSSAI combination that can be used for forwarding traffic to and from non-3GPP devices that have a user identity.
* The non-3GPP devices are pre-configured with a user identifier and credentials necessary to perform an EAP authentication procedure with the AAA Server.

 

Figure 6.x.3-1: Network initiated non-3GPP device authentication

1. The UE establishes a PDU session to be used for traffic to/from non-3GPP devices. During PDU Session Establishment, the SMF indicates that no IP Addresses/Prefixes or MAC Addresses are currently authorized to generate traffic in the PDU Session and the SMF requests the UPF to notify the SMF when detecting unauthorized traffic for this PDU Session (i.e. when a packet is detected from an unauthorized address).
2. A non-3gpp device sends an uplink packet to the UE.
3. The UE forwards the uplink packet in the PDU Session towards the PSA UPF.

1. The UPF detects that the source IP address/Prefix or MAC address is not authorized.

1. The UPF sends an “Unauthorized traffic detected” message to the SMF. The message includes the source IP Address, IP Address and Port Number, or MAC Address.
2. The “Unauthorized traffic detected” message causes the SMF to trigger EAP Authentication of the non-3GPP device. The SMF triggers the procedure by sending a NAS-SM message (e.g. a PDU Session Modification Command) to the UE. The message includes the source address (i.e. the IP address/Prefix and port number or MAC Address that was received from the UPF), and an EAP payload. The EAP payload carries an EAP Identity Request.
3. The UE receives the NAS-SM message. The UE uses the address from the NAS-SM message to forward the EAP Identity request to the non-3GPP device that generated the packet. The EAP Identity Request is sent to the device via the access link between the device and UE (e.g. ethernet, Wi-Fi, or Bluetooth).
4. The device receives the EAP payload from the UE and responds by sending an EAP Identity Response payload. The EAP Identity Response includes the User Identity of the device.
5. The UE receives the EAP Identity Response from the device. The UE forwards the EAP Identity Response to the SMF in a NAS-SM message. The UE also includes the source address in the NAS-SM message.
6. The SMF receives the NAS-SM message from the UE. The SMF uses the source address in the NAS-SM message to determine what request the identity response is associated with.
7. The SMF queries the user profile of the user identity to check that the user identity and UE subscription are linked, If they are linked, the SMF uses the user identity from the EAP Identity Response to select the AAA Server to forward the EAP Identity Response message to.

NOTE 1: As described in RFC 3748 [x], the content of the EAP Identity Response is sent in cleartext.

NOTE 2: How the SMF checks that the user identity and UE subscription are linked can be based on Key Issue #1 solutions.

1. The SMF forwards the EAP Identity Response to the AAA-S.
2. EAP Authentication takes place between the non-3GPP device and AAA-S. The EAP messages that are sent from the AAA-S are sent to the SMF, forwarded to the UE in a NAS-SM message and forwarded to the device by the UE. The EAP messages that are sent from the device are sent to the UE, forwarded to the SMF in a NAS-SM message and forwarded to the AAA-S by the SMF. The NAS messages that carry the EAP messages include the source address to allow the UE to route the EAP messages to the non-3GPP device.
3. When the EAP authentication procedure is complete, the AAA Server notifies the SMF about the result i.e., the device has been successfully authenticated and the source address is allowed.
4. The SMF notifies the UPF that traffic to and from the source address is now allowed. The notification also includes the user identity that is authenticated and authorized for the source address so that the UPF can include the user identity in CDRs. The SMF can obtain policy information from the user profile of the non-3GPP device and use the policy information to update the PDU Session’s QoS Rules, QoS Profile and N4 Rules for the traffic.

NOTE 3: How the SMF obtains policy information from the user profile can be based on Key Issue #1 solutions.

1. The device sends and receives traffic via the UE and the PDU Session. At some point, the IP address/Prefix or MAC Address may change. The device may send a packet with its new MAC Address or IP address/Prefix. The first packet with the new IP address/Prefix or MAC Address is received by the UPF in step 16.
2. The UPF receives the packet and detects that the source MAC Address or IP address/Prefix is not an authorized address. This causes the UPF to repeat Steps 4 to 12.
3. When the EAP authentication procedure is complete, the AAA Server notifies the SMF that the device has been successfully authenticated and authorized.
4. The SMF notifies the UPF that traffic to and from the source address is allowed and that the traffic from the old source address is no longer allowed. The notification also includes the user identity that is authenticated and authorized for the source address so that the UPF can include the user identity in CDRs.

### 6.X.4 Impacts on services, entities and interfaces

UPF:

* Notifies the SMF when a unauthorized source address is detected.
* Receives a notification from the SMF when a source address is authorized.

SMF:

* Receives a notification from the UPF when a source address that is not yet authorized is detected.
* Sends a NAS-SM message to the UE with the source address and an EAP Identity Request
* Receives the EAP-Identity Response and uses the user identity from the EAP Identity Response to select a AAA Server.
* Sends the EAP-Identity Response to the AAA Server.
* Forwards EAP messages between the UE and AAA Server.
* Receives a notification from AAA Server if the user identity is allowed.
* Sends a notification to the UPF when a source address is authorized.

RG:

* Receives a NAS-SM message from the SMF with the source address and an EAP Identity Request.
* Forwards the EAP-Identity Request to the non-3GPP device.
* Forwards EAP messages between the non-3GPP device and SMF.

 **\* \* \* \* End of Change \* \* \* \***

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 22.101: "Service aspects; Service principles".

[3] 3GPP TS 22.115: "Service aspects; Charging and billing".

[4] 3GPP TS 23.501: "System Architecture for the 5G System (5GS); Stage 2".

[5] 3GPP TS 23.502: "Procedures for the 5G System; Stage 2".

[6] 3GPP TS 23.503: "Policy and charging control framework for the 5G System (5GS); Stage 2".

[7] 3GPP TS 23.316: "Wireless and wireline convergence access support for the 5G System (5GS)".

[x] IETF RFC 3748: "Extensible Authentication Protocol (EAP)".

**\* \* \* \* End of Changes \* \* \* \***