**SA WG2 Meeting #161 S2-2403002**

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

**Source: InterDigital Inc.**

**Title: Key Issue #4, New Solution, UE 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: UE 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 UE detects a new unauthorized non-3GPP device generating uplink traffic by detecting traffic from a new source IP Address, Port Number, or MAC Address, the UE 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, 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 UE detects a new source address and may trigger the authentication procedure again.

Once the user identity of the non-3GPP device is authenticated and authorized, 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 that will be used for traffic to/from non-3GPP devices. During PDU Session Establishment, the SMF indicates to the UPF, that no IP Addresses/Prefixes or MAC Addresses are currently authorized to generate traffic in the PDU Session..
2. A non-3gpp device associates with the UE or attempts to send an uplink packet to the UE.
3. The UE detects that the source IP address/Prefix or MAC address is not authorized to send uplink packet in the PDU Session towards the PSA UPF.
4. The UE sends an “Unauthorized traffic or Unauthorized source IP/MAC address detected” message to the SMF. The message includes the source IP Address, Port Number, or MAC Address.
5. The “Unauthorized traffic or Unauthorized source IP/MAC address detected” message causes the SMF to trigger EAP Authentication of the non-3GPP device. The SMF will trigger the procedure by sending a NAS-SM message (e.g. a PDU Session Modification Command) to the UE via the AMF. The message will include the source address (i.e. the IP address/Prefix and port number or MAC Address that was received from the UE), and an EAP payload. The EAP payload will carry an EAP Identity Request.
6. The UE receives the NAS-SM message. The UE will use 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 will be sent to the device via the access link between the device and UE (e.g. ethernet, Wi-Fi, or Bluetooth).
7. 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.
8. 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 via AMF. The UE will also include the source address (i.e. the IP address/Prefix and port number or MAC Address that was reported by the UE in step 3) in the NAS-SM message.
9. The SMF receives the NAS-SM message from the UE. The SMF uses the source address (i.e. source IP address/Prefix and port number or MAC Address that was reported by the UE in step 3) in the NAS-SM message to determine what request the identity response is associated with.
10. The SMF uses the user identity from the EAP Identity Response to select AAA Server to forward the EAP Identity Response message. The SMF can query the user profile of the user identity to check that the user identity and UE subscription are linked.

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 take 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 (i.e. source IP address/Prefix and port number or MAC Address that was reported by the UE in step 3) to allow the UE to route the EAP messages to the proper 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.
4. The SMF notifies the UPF that traffic to and from the source address (i.e. source IP address/Prefix and port number or MAC Address that was reported by the UE in step 3) is now allowed. Before notifying the UPF that the traffic is allowed, the SMF can obtains 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. 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.

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

1. The SMF sends a NAS-SM message to the UE to inform the UE that the device that is using the source IP address/Prefix or MAC address is authorized.
2. The device sends and receives traffic via the UE and the PDU Session. The traffic continues with authorized source address and at some point, the device’s address can change. When the UE receives a packet with the new source IP address/Prefix or MAC Address, the procedures continues to step 16.
3. The UE receives the packet with new source address and detects that the source MAC Address or IP address/Prefix is not an authorized address. This will cause the UE to repeat Steps 2 to 11.
4. EAP Authentication take place between the non-3GPP device and AAA-S.
5. When the EAP authentication procedure is complete, the AAA Server notifies the SMF that the device has been successfully authenticated and authorized.
6. The SMF notifies the UPF that traffic to and from the source address (i.e. source IP address/Prefix and port number or MAC Address that was reported by the UE in step 3) 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 (i.e. source IP address/Prefix and port number or MAC Address that was reported by the UE in step 3) so that the UPF can include the user identity in CDRs.
7. The SMF sends a NAS-SM message to the UE to inform the UE that the device that is using the source IP address/Prefix or MAC address is authorized and that the old address is no longer authorized.

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

UPF:

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

SMF:

* Receives a message from the UE when a unauthorized source address 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.
* Sends a NAS-SM message from the SMF when a Source Address is Authorized and/or when a Source Address is no loner authorized.

RG:

* Notifies the SMF when a unauthorized source address is detected
* 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.
* Recevies a NAS-SM message from the SMF when a Source Address is Authorized and/or when a Source Address is no loner authorized.

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