**SA WG2 Meeting #162 S2-2405273**

**15 April - 19 April 2024, Changsha, China**

**Source: CableLabs, Charter Communications, Deutsche Telekom**

**Title: New Solution for KI#2.2: NULL Encryption IPSec User Plane Tunnelling for MA PDU Session using MPQUIC based steering**

**Document for: Approval**

**Agenda Item: 19.13**

**Work Item / Release: FS\_MASSS / Rel-19**

*Abstract of the contribution: This paper proposes a new Solution for KI#2.2 reducing the cost of user plane data over untrusted non-3GPP access for a MA PDU Session using MPQUIC based steering only. It uses null-encryption for user plane IPSec tunnelling between UE and N3IWF.*

# 1 Discussion

Release 19 FS\_MASSS brings in new steering capabilities for ATSSS Multi access PDU Sessions for both IP and Ethernet. These are based on a QUIC transport between UE and anchoring UPF. Each QUIC payload is encrypted end to end between UE and UPF using TLS encryption. As a result, when non-3GPP untrusted access is used as one of the MA PDU Session accesses, every data payload between UE and N3IWF is encrypted at least twice.  
It has drawbacks due to high energy consumption and computation on both UE and network as well as potential increase in packet latency due to extra computation for each packet.

This solution addresses the double encryption case over the untrusted non-3GPP access for Multi Access PDU Sessions using MPQUIC steering functionality of Release 19. It proposes a mechanism that allows the UE and N3IWF to establish a NULL encryption for user plane IPSec tunnels associated with this MA PDU Session once they get notified by the network that the MA PDU Session uses MPQUIC steering functionality only .

# 2 Proposal

It is proposed to include the following changes in TR 23.700-54 V0.2.0.

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

6.0 Mapping of Solutions to Key Issues

**Table 6.0-1: Mapping of DualSteer Solutions to Key Issues**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Key Issues for DualSteer** | | | |
| **Solution#** | **<Key Issue #1.1>** | **<Key Issue #1.2>** |  |  |
| **#X** |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Table 6.0-2: Mapping of ATSSS\_Ph4 Solutions to Key Issues

|  |  |  |
| --- | --- | --- |
|  | Key Issues for ATSSS\_Ph4 | |
| Solution# | <Key Issue #2.1> | <Key Issue #2.2> |
| #2.1 | **X** |  |
| #2.2 |  | **X** |
| #2.3 | **X** |  |
| #2.4 | **X** |  |
| #2.5 | **X** |  |
| #2.6 |  | **X** |
| #2.7 |  | **X** |
| #2.8 |  | **X** |
| #2.Y |  | X |

**\* \* \* \* Second Change (all new text) \* \* \* \***

6.2.Y Solution #Y: **NULL Encryption IPSec User Plane Tunnelling for MA PDU Session using MPQUIC based steering and switching**

#### 6.2.Y.1 Description

This solution addresses the Key Issue#2.2 "Simplified ATSSS architecture over non-3GPP access" that related to eliminate IPSec tunnel encapsulation.

#### 6.2.Y.2 Procedures

As an example, we detail the procedure to establish user plane resources over untrusted non-3GPP access for a Multi-Access PDU Session using only MPQUIC based steering and switching functionality. We assume that other procedures follow a similar pattern in which the network once it determines that user plane resources must be established over non-3GPP access for a MA PDU Session using MPQUIC based steering and switching functionality, it informs the N3IWF, via N2 signalling, to use NULL encryption for all the user plane traffic associated with the MA PDU Session.

On the receive of this notification, N3IWF and the UE use IKE signalling to establish NULL encryption IPSec tunnels for the MA PDU Session user plane traffic between UE and N3IWF.

The simplified call flow in Figure 6.2.Y.2.-1 describes the UE initiated PDU Session Establishment and user plane resource allocation over non-3GPP untrusted access. It is based on the procedure described in 3GPP TS 23.502 Section 4.22.2.1 with the following updates:



**Figure 6.2.Y.2-1: UE initiated PDU Session Establishment with user plane resource allocation, using NULL encrypted IPSec tunnels over non-3GPP access.**

Step 1: UE requests the establishment of a MA PDU Session using MPQUIC based steering and switching capabilities for ATSSS.

Step 2a: Based on the MA PDU Session from the UE and network ATSSS capabilities it determines to setup a MA PDU Session using only MPQUIC based steering and switching.

Step 2b: SMF (via AMF) signals to N3IWF to setup user plane resources for a PDU session using NULL encryption for all IPSec user plane tunnels.

Step 3-4: N3IWF and UE use IKE signalling to establish IPSec tunnels for user plane data using NULL encryption.

Editor’s Note: SA3 should confirm whether and how to support NULL encryption for IPSec tunnels for user plane data and any potential security related issues, if and when needed.

#### 6.2.Y.3 Impacts on services, entities and interfaces

Editor's note: This clause captures impacts on existing 3GPP services, entities and interfaces.

This solution assumes as a prerequisite the implementation of the solutions addressing KI#2.1 in both UE and the network.

**AMF:**

* Supports extension of the N2 PDU Session signalling between the AMF and N3IWF with an optional field that indicates that NULL encryption may be applied between UE and N3IWF for all the user plane traffic associated with this PDU Session.

**SMF:**

* Supports extension of the PDU Session signalling to the AMF for indicating that only MPQUIC based steering is supported.

**N3IWF:**

* Supports extension of the N2 PDU Session signalling between the AMF and N3IWF with an optional field that indicates that NULL user plane encryption may be applied for user plane traffic, between UE and N3IWF, associated with this PDU Session.

No other impacts are envisioned for this solution.

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