**3GPP TSG-SA3 Meeting #123 S3-252961**

**Goteborg, Sweden, 25 – 29 August 2025**

**Source:** **Huawei, HiSilicon, CableLabs, Charter Communications,** **Lenovo, Nokia, Nokia Shanghai Bell,** **InterDigital**

**Title:** **New SID on security aspects for QUIC/TLS**

**Document for: Discussion**

**Agenda Item: 6.3**

3GPP™ Work Item Description

Information on Work Items can be found at <http://www.3gpp.org/Work-Items>   
See also the [3GPP Working Procedures](http://www.3gpp.org/specifications-groups/working-procedures), article 39 and the TSG Working Methods in [3GPP TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm)

Title: Study on providing a PSK to enable the security for MPQUIC

Acronym: FS\_PSK\_MPQUIC\_Sec

Unique identifier:

Potential target Release: Rel-20

# 1 Impacts

{For Normative work, identify the anticipated impacts. For a Study, identify the scope of the study}

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Affects: | UICC apps | ME | AN | CN | Others (specify) |
| Yes |  | X |  | X |  |
| No | X |  | X |  | X |
| Don't know |  |  |  |  |  |

# 2 Classification of the Work Item and linked work items

## 2.1 Primary classification

### This work item is a …

|  |  |
| --- | --- |
| X | Study |
|  | Normative – Stage 1 |
|  | Normative – Stage 2 |
|  | Normative – Stage 3 |
|  | Normative – Other\* |

**\* Other = e.g. testing**

## 2.2 Parent Work Item

|  |  |  |  |
| --- | --- | --- | --- |
| Parent Work / Study Items | | | |
| Acronym | Working Group | Unique ID | Title (as in 3GPP Work Plan) |
| N/A |  |  |  |

### 2.3 Other related Work Items and dependencies

|  |  |  |
| --- | --- | --- |
| Other related Work /Study Items (if any) | | |
| Unique ID | Title | Nature of relationship |
| N/A |  |  |

**Dependency on non-3GPP (draft) specification:**

N/A

# 3 Justification

In Release 18, SA2 specified MPQUIC in clause 5.32.6.2.2 of TS 23.501for steering, switching, and splitting of UDP traffic between the UE and UPF. In Release 19, SA2 specified MPQUIC in clause 5.32.6.2.2 of TS 23.501 for steering, switching, and splitting of non-UDP traffic between the UE and UPF. MPQUIC uses QUIC, which further uses TLS for transport layer security protection of traffic between the UE and UPF.

During the SA3#117 meeting, it was decided to add an annex to describe that TLS security is used in MPQUIC in ATSSS. However, neither the management of certificates nor other types of authentication mechanisms (e.g. pre-shared key mode) are specified. Pre-shared-key (PSK) mode can save on computation and communication. Furthermore, it can be flexibly deployed and would enable Early Data (0-RTT) in QUIC protocol. This is a major advantage of such mode.

For PSK mode, in 3GPP, the PSK between the UE and the UPF can be obtained in multiple manners, for example, through pre-configuration or derivation from the security context between the UE and the network. When and how to obtain the PSK should be discussed. And the complexity of different approaches may be compared in order to provide further reference for specific deployments.

# 4 Objective

Based on the above justification, the following objectives will be studied:

WT#1: Study the support of PSK mode, in particular:

- Study key derivation and delivery for UPF.

NOTE: the impact to the 5GS should be minimized.

## TU estimates and dependencies

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Work Task ID | TU Estimate  (Study) | TU Estimate  (Normative) | RAN Dependency  (Yes/No/Maybe) | Inter Work Tasks Dependency  Editor’s Note: This column should highlight if WT#x is self-contained, or is dependent on completion of other WTs |
| WT#1 | 1 | 0.5 | No | WT#1 is self-contained |

Total TU estimates for the study phase: 1

Total TU estimates for the normative phase: 0.5

Total TU estimates: 1.5

# 5 Expected Output and Time scale

***{If this WID covers both stage 2 and stage 3, clearly indicate the different completion dates.}***

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| New specifications {One line per specification. Create/delete lines as needed} | | | | | |
| Type | TS/TR number | Title | For info  at TSG# | For approval at TSG# | Rapporteur |
| Internal TR | 33.xxx | Study on providing a PSK to enable the security for MPQUIC | SA#110 (Dec 25) | SA#111 (Mar 26) | X |
|  |  |  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Impacted existing TS/TR {One line per specification. Create/delete lines as needed} | | | |
| TS/TR No. | Description of change | Target completion plenary# | Remarks |
|  |  |  |  |
|  |  |  |  |

# 6 Work item Rapporteur(s)

X

# 7 Work item leadership

SA3

# 8 Aspects that involve other WGs

Stage 3 aspects covered by CT WGs. Potential interaction with SA2 WG for architecture aspects.

# 9 Supporting Individual Members

|  |
| --- |
| Supporting IM name |
| Huawei |
| HiSilicon |
| CableLabs |
| Charter Communications |
| Lenovo |
| Nokia |
| Nokia Shanghai Bell |
| InterDigital |
| ZTE |