**3GPP TSG-SA3 Meeting #113 *S3-23abcd***

Chicago, USA, 6 - 11 November 2023 (revision of S3ah-230013)

**Source: Lenovo, BROADCOM CORPORATION, CableLabs, CATT, Charter Communications, Inc, China Mobile, CISCO, Deutsche Telekom, InterDigital, Inc., LG Electronics, Nokia, Tencent, vivo Mobile Communication Co.,, Xiaomi, ZTE Corporation**

**Title: New SID on Double Layer Security Optimization**

**Document for: Approval**

**Agenda Item: 4**

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: New SID on Double Layer Security Optimization

Acronym: FS\_DoLa\_Sec

Unique identifier:

{A number to be provided by MCC at the plenary}

Potential target Release: Rel-19

# 1 Impacts

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

# 2 Classification of the Work Item and linked work items

## 2.1 Primary classification

### This work item is a …

|  |  |
| --- | --- |
|  | Feature |
|  | Building Block |
|  | *Work Task* |
| X | Study Item |

## 2.2 Parent Work Item

For a brand-new topic, use “N/A” in the table below. Otherwise indicate the parent Work Item.

|  |
| --- |
| Parent Work / Study Items  |
| Acronym | Working Group | Unique ID | Title (as in 3GPP Work Plan) |
| FS\_ATSSS\_Ph3 | SA2 | 940070 | Study on Access Traffic Steering, Switching and Splitting support in the 5G system architecture; Phase 3 |

### 2.3 Other related Work Items and dependencies

|  |
| --- |
| Other related Work /Study Items (if any) |
| Unique ID | Title | Nature of relationship |
|  |  | {optional free text}  |

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

# 3 Justification

SA2 is defining in ATSSS the use of Multipath QUIC (<https://datatracker.ietf.org/doc/draft-ietf-quic-multipath>) between the UE and the UPF in the selected solution #2.2 in TR 23.700-53. MP-QUIC extends QUIC (RFC 9000) to enable the simultaneous use of multiple paths for a single connection. QUIC requires according to RFC 9001 the mandatory usage of TLS 1.3 with encryption according to RFC 8446. This mandatory requirement is reasonable for the intended use of QUIC in the normal client – application server environment in the internet. In the SA2 discussion, the double encryption on QUIC layer and on the access layer was seen as computational burden.

SA2 captured the following Note in the conclusions of KI#2 accordingly:

NOTE 2: SA WG3 can study security optimizations that can improve the user-plane performance, such as whether the encryption in the QUIC layer can be omitted.

This SID intends to study how the double layer security on the QUIC layer between UE and UPF and on the access layer can be avoided, and to study the mechanisms to do so.

The outcome of the study should be applicable also for applications other than QUIC and incorporate feedback from IETF, if necessary.

No further impact to RAN and SA2 is anticipated and foreseen.

# 4 Objective

The objective is to study

* WT1: how the double layer security at the QUIC layer of MPQUIC between UE/UPF and at the AS layer can be avoided, and
* WT2: whether to specify mechanisms to omit encryption/integrity protection/authentication at QUIC layer or at AS layer

## TU estimates and dependencies

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Work Task ID | TU Estimate(Study) | TU Estimate(Normative) | RAN Dependency(Yes/No/Maybe) | Inter Work Tasks Dependency |
| **WT1** | **3** |  | **No** | -- |
| **WT2** |  | **1** | **No** | Depends on outcome of WT1 |

Total TU estimates for the study phase: 3

Total TU estimates for the normative phase: 1

Total TU estimates: 4

# 5 Expected Output and Time scale

|  |
| --- |
| 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 |
| TR | N/A  | Double Layer Security Optimization  | SA#104 | SA#105 | TBD  |

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

# 6 Work item Rapporteur(s)

TBD

# 7 Work item leadership

SA3

# 8 Aspects that involve other WGs

System architecture aspects, i.e. QUIC procedures, will be covered by SA2

# 9 Supporting Individual Members

|  |
| --- |
| Supporting IM name |
| Lenovo |
| BROADCOM CORPORATION |
| CableLabs |
| CATT |
| Charter Communications, Inc |
| China Mobile |
| CISCO |
| Deutsche Telekom |
| InterDigital, Inc. |
| LG Electronics |
| Nokia |
| Tencent |
| vivo Mobile Communication Co., |
| Xiaomi |
| ZTE Corporation |