**3GPP TSG-SA3 Meeting #116 *S3-99999***

Jeju, South Korea, 20th May – 24th May 2024

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  |  | **CR** |  | **rev** |  | **Current version:** |  |  |
|  | | | | | | | | |
| *For* [***HE******LP***](http://www.3gpp.org/3G_Specs/CRs.htm#_blank)*on using this form: comprehensive instructions can be found at* [*http://www.3gpp.org/Change-Requests*](http://www.3gpp.org/Change-Requests)*.* | | | | | | | | |
|  | | | | | | | | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps |  | ME | **X** | Radio Access Network |  | Core Network | **X** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | MPQUIC TLS Annex | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Intel, Nokia?, Cablelabs?, Qualcomm?, Huawei? | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | TEI18 | | | | |  | ***Date:*** | | | 2024-05-10 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | B |  | | | | | ***Release:*** | | | Rel-18 |
|  | *Use one of the following categories:* ***F*** *(correction)* ***A*** *(mirror corresponding to a change in an earlier release)* ***B*** *(addition of feature),* ***C*** *(functional modification of feature)* ***D*** *(editorial modification)*  Detailed explanations of the above categories can be found in 3GPP [TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | | | | | | | | *Use one of the following releases: Rel-8 (Release 8) Rel-9 (Release 9) Rel-10 (Release 10) Rel-11 (Release 11) … Rel-15 (Release 15) Rel-16 (Release 16) Rel-17 (Release 17) Rel-18 (Release 18)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | To enhance the security of multipath communications in 5G networks, particularly when utilizing MPQUIC for ATSSS, the introduction of TLS server authentication based on digital certificates ensures the integrity and authenticity of the UPF. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | This CR proposes adding a clause/Annex specifying the use of TLS server authentication based on digital certificates when MPQUIC is utilized as the multipath protocol for ATSSS. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | . | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | New Annex AA | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **Y** | **N** |  | | | |  | | |
| ***Other specs*** | |  | **X** | Other core specifications | | | | TS/TR ... CR ... | | |
| ***affected:*** | |  | **X** | Test specifications | | | | TS/TR ... CR ... | | |
| ***(show related CRs)*** | |  | **X** | O&M Specifications | | | | TS/TR ... CR ... | | |
|  | |  | | | | | | | | |
| ***Other comments:*** | |  | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | |  | | | | | | | | |

**\*\*\*\* START OF CHANGES \*\*\*\***

Annex AA (informative):   
Security aspects of the Access Traffic Steering, Switching and Splitting

# AA.1 General

This Annex specifies the Security aspects of the Access Traffic Steering, Switching and Splitting (ATSSS). The 5G ATSSS is described in 3GPP TS 23.501 [2].

# AA.2 Server Authentication for MPQUIC in ATSSS

When MPQUIC is used as the multipath protocol for ATSSS, authentication based on digital certificates shall be selected.

NOTE x: Exposing the UPF IP addresses to the UE is against the principle of network topology hiding. It is up to the network to decide whether to compromise on the security to use MPQUIC or the network implementation to use appropriate mechanisms to hide the network topology.

**\*\*\*\* END OF CHANGES \*\*\*\***