**Title: Informal feedback on companies' position in FS\_UIA\_ARC (TR 23.700-32 v0.2.0)**

# 1 Overall description

TR 23.700-32 v0.2.0 contains 16 solutions. The solutions cover key issues #1, #2 and #3. No solutions cover key issue #4.

The survey is only asking for company feedback on the solutions that are currently documented in TR 23.700-32 v0.2.0. The purpose of the survey is to see if there are general principles that are agreeable for key issues #1, #2, and #3. Any agreeable principles could be documented in TR 23.700-32 at SA2 #162 or used as a starting point for discussions leading up to SA2 #163.

Each company is asked to give their view towards these questions. This is not an evaluation for each of the solutions that are currently documented. It is mainly to seek your view on how each key issue can be addressed, based on the content of TR 23.700-32 so far.

**Key Issue #1**

|  |  |
| --- | --- |
| Key area | Company Input |
| (1a): Where is the user profile stored? (e.g. UDM/UDR, in a different NF, outside of the 5GC) |  |
| (1b): How are user identities linked with a subscription? (e.g. based on a request received via an NEF API) |  |
| (1c): When does the UE provide the user identity to the 5GC in order to become “active”? (e.g. in a Registration Procedure, in a PDU Session Establishment Procedure) |  |
| (1d): How are user specific policies considered when configuring QoS for a PDU Session? |  |
| (1e): Whether and how is the user identity considered in services that exist outside of a PDU Session (i.e. SMS)? |  |
| (1f): What is the format of the user identifier (e.g. NAI)? |  |
| (1g): At SA #162, what Key Issue #1 solution principles are agreeable for an interim / partial conclusion? |  |

**Key Issue #2**

|  |  |
| --- | --- |
| (2a): What network function(s) or entities can trigger authentication of the user (e.g. AMF, SMF)? |  |
| (2b): User Identity Authentication takes place between the UE and what entity (e.g. AAA Server)? |  |
| (2c): To what degree does SA2 specify the authentication procedure (e.g. SA2 says that it takes place via control plane/EAP or over the user plane and SA3 defines the rest, etc.)? |  |
| (2d): Once a user is authenticated, what NF(s) need to enforce any restrictions on the user? What are restrictions based on (e.g. information in the user profile)? |  |
| (2e): At SA #162, what Key Issue #2 solution principles are agreeable for an interim / partial conclusion? |  |

**Key Issue #3**

|  |  |
| --- | --- |
| (3a): How is user profile information and functionality exposed (e.g. NEF APIs)? |  |
| (3b): What user profile information can be exposed (e.g. linked subscription identifiers)? |  |
| (3c): What user profile functionality can be exposed (e.g. the ability to check if a user is actively using a subscription)? |  |
| (3d): At SA #162, what Key Issue #3 solution principles are agreeable for an interim / partial conclusion? |  |