
1 Introduction

It is anticipated that the questions below are a first round of questions. A second round of questions can be more focused based and cover just the options that have noticeable support. For example, if 10 companies prefer option A and 2 companies prefer option B, then the second round of questions will be about the details of option A.

The FS_UIA_ARC TR after SA2 #162 is TR 23.700-32 V0.3.0.

2 Collection of companies' views to be considered for conclusions

2.1 Key Issue #1

Feedback Form 1: Question KI#1.1: It has already been concluded that the User Identifier format is an NAI. Can the User Identifier be operator assigned, third party assigned or should both options be possible?

1 – Deutsche Telekom AG Both
2 – Ericsson LM Exposure APIs (perhaps CAPIF) from the entity managing the UIP, which is outside the 5GC
3 – Ericsson LM Both should be possible as per 22.101. When assigned by 3rd party, it can be assumed that 3rd party also controls the associated credentials.
4 – vivo Mobile Communication Co. both is ok
5 – InterDigital Both should be possible. However, even when it is 3rd party assigned, it should be managed by the operator. A use case for 3rd party assignment is where the user want wants to use his email address as the user identity.
6 – LG Electronics France According to SA1 requirement, 3rd party can provide User Identifier. Therefore, both options should be supported.

<p>7 – HUAWEI Technologies Japan K.K.</p> <p>Both options are possible, subject to the scenarios.</p>
<p>8 – China Mobile Com. Corporation</p> <p>Both options are okay</p>
<p>9 – Motorola Mobile Com Technology</p> <p>The user identifier is operator controlled. Both options, operator assigned and 3rd party assigned, are possible. The operator would approve any user identifier requested by a user. Note that as per requirement in clause 26a.2.1 in TS 22.101: <u>”User Identifier shall be independent of existing identifiers relating to subscription (e.g. IMSI, MSISDN, IMPI, IMPU, SUPI, GPSI).”</u></p>
<p>10 – Nokia Corporation</p> <p>We suggest that the User Identifier shall be defined by both, i.e. operator assigned or by third party. However, 5GS shall ensure that the User Identifier is unique across the PLMN.</p>
<p>11 – Qualcomm Incorporated</p> <p>Which party assigns the User Identifier is a deployment issue, not a standardization issue. In our view, the User Identifier should be assigned via AF. The AF can be provided either by third party or operator.</p>
<p>12 – Nubia Technology Co.</p> <p>ZTE: Both options are possible.</p>
<p>13 – NEC Europe Ltd</p> <p>Both options should be possible.</p>
<p>14 – Samsung Electronics Czech</p> <p>Both</p>
<p>15 – Apple Benelux B.V.</p> <p>Both options are possible. But when it is 3rd party assigned, there has to be some mechanism to ensure the uniqueness. This may lead to situation that an MNO entity is finally responsible for validating the assigned User Identifiers.</p>

<p>16 – Guangdong OPPO Mobile Telecom.</p> <p>User Identifier should be assigned by operator. Third party assigned identifier is possible, but the application layer approach is out of the scope of this study.</p>
<p>17 – CATT</p> <p>Both should be possible.</p>
<p>18 – Philips International B.V.</p> <p><apologies for the late input> Both</p>

Feedback Form 2: Question KI#1.2: Is the User Identity Profile managed by the operator, third party, or should both options be possible?

<p>1 – Deutsche Telekom AG</p> <p>Both</p>
<p>2 – Ericsson LM</p> <p>What is outside the operator domain is not to be standardized and thus what is left is that some information is needed in the operator domain (e.g. linkage) which can be called the UIP and that is managed by the operator.</p>
<p>3 – vivo Mobile Communication Co.</p> <p>both is ok, depends on the answer of 1.1</p>
<p>4 – InterDigital</p> <p>Operator managed is preferred.</p>
<p>5 – LG Electronics France</p> <p>According to SA1 requirement, 3GPP system should be able to update User Identity Profile based on input from 3rd party. Therefore, both options should be supported.</p>
<p>6 – HUAWEI Technologies Japan K.K.</p> <p>Both are possible. If the User ID is assigned by the operator, the User Identity Profile has to be managed by the operator. If the User ID is assigned by the third party, the User Identity Profile can be managed by the third party but need authorization by the operator, which implies that the operator has to manage it as well.</p>

7 – China Mobile Com. Corporation

Both options are ok. the third party needs to get authorization from the operator if the user ID is assigned by the third party.

8 – Motorola Mobile Com Technology

The user profile creation, information included and format should be under the operator control. Any third party that has SLA agreements with an operator could trigger user profile creation.

9 – Nokia Corporation

User Identity Profile can be managed by OAM and AF/NEF; hence operator and third party shall be allowed to manage User Identity Profile.

10 – Qualcomm Incorporated

Which party manages the User Identity is a deployment issue, not a standardization issue. In our view, the User Identity should be managed via AF. The AF can be provided either by third party or operator.

11 – Nubia Technology Co.

ZTE: Both are possible. The AF may use the NEF API to manage User Identity Profile

12 – NEC Europe Ltd

Both options should be possible.

13 – Samsung Electronics Czech

It is based on which entity has created the user profile.

E.g. in the case the User identifier is operator assigned, it should be managed by the operator, while 3rd party application services may just update it (e.g. provisioning specific QoS related to the 3rd party application service for a particular operator-assigned User identifier)

14 – Apple Benelux B.V.

Generally there has to be one entity responsible for management of user identity profiles in an operator domain. Management by AF through NEF API is not that straightforward. There are questions like how is the AF authorized to administer User Identity profiles for a particular subscriber, is there a user consent involved here? could there be multiple AFs responsible for an User Identity profile? Who is responsible for resolving conflicting requests from different AFs in management of one User Identity profile?

<p>15 – Guangdong OPPO Mobile Telecom.</p> <p>User Identity Profile should be managed by the operator only.</p>
<p>16 – CATT</p> <p>Both options are possible.</p>
<p>17 – Philips International B.V.</p> <p><apologies for the late input> Even when user identity is 3rd party assigned, the profile itself should be managed by the operator, with some possibilities to influence (e.g. QoS preferences) the profile using NEF/AF.</p>

Feedback Form 3: Question KI#1.3: Where is the User Identity Profile Stored?

<p>1 – Deutsche Telekom AG</p> <p>UDR</p>
<p>2 – Ericsson LM</p> <p>UIP is managed in application layer outside the 5GC, but still in the operator domain, i.e., within the 3GPP system (and stored in the application layer seen from 5GC).</p>
<p>3 – Deutsche Telekom AG</p> <p>Unified Data Repository should be the choice, the NFs that can manage the data should at least be NEF. The information of the Profile should be specified in 3GPP.</p>
<p>4 – vivo Mobile Communication Co.</p> <p>neutral for this.</p>
<p>5 – InterDigital</p> <p>The UDR.</p>
<p>6 – LG Electronics France</p> <p>In the UDM/UDR.</p>
<p>7 – HUAWEI Technologies Japan K.K.</p> <p>In the UDM/UDR.</p>

8 – China Mobile Com. Corporation

in the UDM/UDR

9 – Motorola Mobile Com Technology

The user profile is stored at the UDR. User profile information may be stored in multiple data sets in the UDR. For example, user profile for subscription data and a user profile for policy data.

10 – Nokia Corporation

UE Subscription is maintained at the UDM/UDR and for the results to be provided to the consumer NF by considering both the UE Subscription that the User Identifier is using and the User Identity Profile, it is more efficient to maintain the User Identity Profile at the UDM/UDR.

So, our view is that User Identity Profile is maintained at the UDM/UDR.

11 – Qualcomm Incorporated

The User Identity profile should be stored in an AF.

12 – Nubia Technology Co.

ZTE: UDM/UDR

13 – NEC Europe Ltd

UDR

14 – CableLabs

UDM/UDR seems good. We also like to mention that this information could be available to external AAA server when needed.

15 – Samsung Electronics Czech

UDM/UDR data is generally subscription-based (i.e. SUPI is INDEX/key to fetch the data), it can be better if some other entity (e.g. UIDF) is used to store only the User profile. The INDEX/key to fetch the user profile will be the user identifier, which the NF consumers like AMF and/or SMF use to fetch the user profile.

This can be either operator-controlled; or controlled by 3rd party and stored outside 5GC.

<p>16 – Apple Benelux B.V.</p> <p>A User Identity profile (here i am assuming that there is no subscription related data in the raw user identity profile) independent of any subscription information should not be stored in UDR. A user identity profile is meaningful within 5GC only when it is linked to a subscription. UDM/UDR should not be burdened with storage of User Identity profiles. Part of the user identity profile (identifiers, QoS etc) may get added to UDM/UDR when it is linked to a subscription.</p>
<p>17 – Guangdong OPPO Mobile Telecom.</p> <p>UDR</p>
<p>18 – CATT</p> <p>UDR</p>
<p>19 – Philips International B.V.</p> <p><apologies for the late input> UDM/UDR.</p>

Feedback Form 4: Question KI#1.4: There is an editor’s note in the conclusion that says that whether more than one User Identity can be in the User Identity Profile is FFS. Should it be possible for more than one User Identity to be in a User Identity Profile? If yes, then what is the use case?

<p>1 – Ericsson LM</p> <p>UIP:User=1:1, UIP:UID=1:N according to TS 22.101. Use case is unknown, we can live with UIP:UID=1:1.</p>
<p>2 – Deutsche Telekom AG</p> <p>Yes.</p>
<p>3 – vivo Mobile Communication Co.</p> <p>neutral for this. but the use case for the multiple user id in profile should be clear described.</p>
<p>4 – InterDigital</p> <p>We prefer to only support one user identity per User Identity Profile in this release. That being said, we see value in supporting multiple user identities per User Identity Profile. The use case is that a user is allowed to present different user identities depending on how the user is accessing the system. Ideally solutions should provide enough future proofness to allow such support in a future release.</p>

5 – LG Electronics France

It seems that there is no use case. If there is clear use case, it can be revisited.

6 – HUAWEI Technologies Japan K.K.

No support for Rel-19. Unclear what's the relationship of the user identities to share the same profile. They belong to a group or the same person? The requirement needs to be clarified before it can be considered for this release.

7 – China Mobile Com. Corporation

We prefer to only support one user identity per User Identity Profile in this release. Unclear what's the relationship of the user identities to share the same profile.

8 – Motorola Mobile Com Technology

Yes, multiple User Identifiers are possible if multiple User IDs policies can be supported by the same profile.

9 – Nokia Corporation

Have one User Identifier per User Identity Profile. If there are more than one identifier to be created, create them as two independent User Identity Profiles. This helps to keep the solution simple.

10 – Qualcomm Incorporated

The User Identity and User Identity Profile is managed by AF. How to define the user identity profile is out of SA2 scope.

11 – Nubia Technology Co.

ZTE: More UIDs in one Profile is preferred. Example, for one UE/SUPI, one UID for game and one UID for work. But can live with one User ID in one User Identity Profile in this release.

12 – Samsung Electronics Czech

For simplicity and to avoid complexity it is better to have one user identifier per user profile

13 – Apple Benelux B.V.

In our view there may be multiple user identity within a single user identity profile. For example, they may be associated with different application providers. Application providers may prefer to work with a user identifier that is unique in their domain (and can be user across networks to identify a user). They could be seen as an aliases to the user identifier in the User Identity profile.

14 – Guangdong OPPO Mobile Telecom.

Yes, it should be possible for more than one User Identity to be in a User Identity Profile. Furthermore, A User Identity Profile consolidates information associated with a user’s one or multiple User Identities, with each User Identity including information, such as User IDs, service preferences, QoS parameters, and possibly credentials.

One valid and practical use case could be as follow. A human user might have an identity as a regular consumer in the 5GS. And the same human user might have the other identity as a VIP gaming customer in the 5GS. In the User Identity Profile for this human user, it includes regular consumer user identity, e.g. best-effort data service with a User ID, as well as other relevant information belonging to this consumer user identity. While in this human user’s the other identity within this User Identity Profile, e.g. VIP gaming user identity, it could have a different User ID used to identity his/her gaming user identity, along with the information for an enhanced 5GS service, e.g. VPN services, low-latency, and guaranteed bit rate, etc.

15 – CATT

For simplicity, we prefer one User Identity in one User Identity Profile.

16 – Philips International B.V.

<apologies for the late input> In our view one user identity per user identity profile would keep things clear and simple. For different user identity another user identity profile could be created.

Feedback Form 5: Question KI#1.5: It has already been concluded that a User Identity Profile includes a list of linked subscriptions. What other information, or parameters, should be stored in the User Identity Profile?

1 – Ericsson LM

Regarding credentials, see answer to question KI#1.1, i.e. if the UID is controlled by the operator then credentials are part of the UIP

Parameters enabling QoS differentiation can be assumed as possible to store in the UIP, but it is reasonable to assume that the user itself does not work directly in setting 5GC QoS parameters but user friendly information is disclosed to the user and then the entity managing the UIP converts the user request into 5GC QoS parameters. Information related to Guidance for URSP e.g. DNN and S-NSSAI can be used to control specifics of a user identified by a UID.

More information/detailed requirements are required in order to determine additional parameters to enable additional service differentiation e.g. for SMS and IMS.

2 – Deutsche Telekom AG

User Preferences for services (Service cahin, IMS settings).

3 – vivo Mobile Communication Co.

from my side, the dedicated policy data (UE policy or PCC rule) can be added, this is aligned with the requirements for differentiation of service. other requirements need clarification.

4 – InterDigital

QoS Parameters associated with DNN/S-NSSAI combinations and the identity of the subscription (e.g., SUPI) the user is linked with and whether the user is currently active with that subscription.

5 – LG Electronics France

Specific service settings and parameters, i.e. QoS information needs to be stored in the User Identity Profile.

6 – HUAWEI Technologies Japan K.K.

DNN, S-NSSAI, QoS profile, Authentication mechanism and so on. Crossing subscription data between SUPI and User Identity will be authorized for the User Identity when the corresponding user accesses the network.

7 – Motorola Mobile Com Technology

The User Profile is identified by a Data Key and/or Data Sub Key combination in the UDR. The Data Keys can be the SUPI, GPSI and/or User ID.

Other parameters that can be stored in the user profile are:

- List of devices (i.e. PEI) authorised to use the user profile
- List of available slices/DNNs for a user,
- List of available services for a user (e.g. SMS, MBS, V2X, etc.)
- Policy Data (e.g. for a PDU Session, AM and/or UE related policy).

8 – Nokia Corporation

Each User identifier may have the following.

- Security profile (Authentication and Privacy details)
- Additional Service Identifiers like GPSI.
- Services (and its content like DNN, slices, SMS service, etc) that are allowed / disallowed.
- PCC Rules.

9 – Qualcomm Incorporated

The User Identity profile should be managed by AF, the definition is out of SA2 scope.

SA2 only need to take care what parameters are provided by AF for service differentiation based on the User Identity.

The authentication and credential should be coordinated with SA3. Before SA3 specify the mechanism for authentication of User Identity, SA2 can't assume that 5GC can support the authentication of User Identity.

10 – Nubia Technology Co.

ZTE: Qos profile, Service information, credential (optional)

11 – NEC Europe Ltd

List with one or more network slices that the user can use. This list may be a subset of the Allowed NSSAI for the UE, i.e. the Allowed NSSAI feature is not impacted however, different users of the UE may be allowed access to different slices meaning not all the network slices from the Allowed NSSAI would be available to each user of the UE.

12 – Samsung Electronics Czech

For the use case to expose the user identity verification/authentication results to 3rd party (as concluded in KI#3), storing only the linked subscription(s) is enough.

For the use case of providing service differentiation to different user identities, the User profile may further store information related to specific QoS settings, e.g. to block particular websites, QoS parameters for particular application services, etc.

13 – Apple Benelux B.V.

From SA2 perspective, the minimum required is information for deriving PCC rules to provide QoS differentiation per linked subscription. Other content (like credentials) may have to be added depending on SA3' s progress.

14 – Guangdong OPPO Mobile Telecom.

A UIP may include one or multiple User Identities. For each User Identity, the following elements should be stored in the User Identity Profile:

- User ID: the User ID is PLMN-unique, as the identifier of the User Identity. The User ID is also used for authentication and authorization to access 5G service.
- User Identity specific service settings and parameters
- QoS information
- Linked 5GS subscription identified by a SUPI.

15 – CATT

At least service parameters, and optionally credentials.

16 – Philips International B.V.

<apologies for the late input> The UIP should include:

- Authentication parameters, security credentials and privacy setting related to the user identity.
- List of devices authorised to use the user profile
- List of available slices/DNNs for the user,

- List of available services for the user
- Policy information specific to the user.

Feedback Form 6: Question KI#1.6: It has already been concluded that a User Identifier can be linked/unlinked with a subscription. What event(s), or request(s), trigger the User Identifier to be linked/unlinked?

1 – Ericsson LM

Via a management procedure triggered by User managing his/her UIP. (When User logs in to a UID, a linkage becomes active.)

2 – Deutsche Telekom AG

O&M procedure or request received via an NEF API

3 – vivo Mobile Communication Co.

neutral.

4 – InterDigital

Invocation of an NEF API should be used to link and unlink a user identifier with a subscription or OAM.

5 – LG Electronics France

Link/Unlink is triggered by the AF by using NEF service.

6 – HUAWEI Technologies Japan K.K.

First the linkage between the User IDs and SUPIs needs to be subscribed in the UDM/UDR before the user ID can be authorized to link with the specific SUPI. Then the trigger for the activation of the link can come from the UE request e.g. for activation during PDU Session establishment or the AF request via an NEF API.

7 – China Mobile Com. Corporation

Activation during PDU Session establishment or the AF request via an NEF API.

8 – Motorola Mobile Com Technology

In one option, the AF triggers linking/unlinking of user identifier to a subscription (i.e. when the AF sends a User Profile creation request that includes the linked user identifier(s) to a subscription). In another option the OAM can configure UDM/UDR to link a user identifier to a subscription.

<p>9 – Nokia Corporation</p> <p>This question is about the administrative aspects. The entire process of linking / unlinking needs to be carried out with the involvement of the UE Subscription and the User Identities (for example self-services), hence must be carried out through the OAM/ trusted AF (based on the security profile).</p>
<p>10 – Qualcomm Incorporated</p> <p>The linkage of user identity to a subscription is triggered via application layer and is managed by an AF.</p>
<p>11 – Nubia Technology Co.</p> <p>ZTE: AF request (i.e. via NEF API), or OAM configuration</p>
<p>12 – NEC Europe Ltd</p> <p>Linked by the operator or by the service provider via NEF</p>
<p>13 – Samsung Electronics Czech</p> <p>if the user profile already includes SUPI(s) (i.e. only through these SUPI(s) User identifier is allowed to access), then linking/unlinking is done whenever the User profile is created/updated/deleted.</p> <p>Otherwise, whenever a User identifier is (trying to) using a SUPI, linking and activation are done simultaneously (after successful authentication) and it can be done either via NAS (as described in Solution #7) or via NEF (as defined in Solution #23). In this case, only 1 SUPI can be linked to a User identifier at a particular time.</p>
<p>14 – Apple Benelux B.V.</p> <p>Linking/ unlinking with a subscription is done by OAM. We dont think a NEF API for this is required.</p>
<p>15 – Guangdong OPPO Mobile Telecom.</p> <p>User ID is linked/unlinked at the time of provisioning via OAM calling UDM API, alternatively via AF calling NEF API to trigger UDM to authorize the request and updating UIP to include/remove a SUPI.</p>
<p>16 – CATT</p> <p>At the provisioning phase, either via OAM or AF/NEF.</p>
<p>17 – Philips International B.V.</p> <p><apologies for the late input> Agree with Samsung</p>

Feedback Form 7: Question KI#1.7: In this release, when a user identifier is active with a subscription, should PCC Rules be adjusted?

<p>1 – Ericsson LM</p> <p>They may, via AF influencing 5GC e.g. AF request for QoS.</p>
<p>2 – Deutsche Telekom AG</p> <p>PCF should take into account information regarding the user (e.g. preferences) for decisions on PCC rules, i.e. answer is yes.</p>
<p>3 – vivo Mobile Communication Co.</p> <p>yes, adjust the QoS according to user ID</p>
<p>4 – InterDigital</p> <p>Yes. QoS Parameters should be part of the user profile and the adjustment should be based on these QoS Parameters.</p>
<p>5 – LG Electronics France</p> <p>Yes. PCF can retrieve User Identify Profile information from UDR to apply QoS setting for a user identifier.</p>
<p>6 – HUAWEI Technologies Japan K.K.</p> <p>Yes, the PCF can adjust the PCC rules taking the user ID profile into account.</p>
<p>7 – China Mobile Com. Corporation</p> <p>yes, adjust the QoS according to user ID</p>
<p>8 – Motorola Mobile Com Technology</p> <p>If a User profile for a user identifier includes specific policy data (e.g. PDU Session policy control data, AM or UE policy subscription data), the PCF applies the PCC rules related to policy data.</p>
<p>9 – Nokia Corporation</p> <p>We do not have a strong opinion of having this in this release or in future releases. However, at the initial release, the UE Subscription may want to limit QoS parameters for the allowed corresponding Applications. So, we need to factor in at least some capabilities to be part of the release.</p> <p>Further, since it is always one User Identifier active with a UE subscription at any given point of time, rules will be installed and not adjusted from UE (or different User Identifier) to the User Identifier.</p>

<p>10 – Qualcomm Incorporated</p> <p>The PCC rule may be changed based on the request of AF according to activation of user identify.</p>
<p>11 – Nubia Technology Co.</p> <p>ZTE: Yes. PCF can update the PCC rule (existing parameters) according to the User Identity Profile.</p>
<p>12 – NEC Europe Ltd</p> <p>Yes</p>
<p>13 – Samsung Electronics Czech</p> <p>Yes, A single user identifier can have multiple PDU sessions simultaneously and for each PDU session the PCC rules will be set (and changed) as per the service requirement</p>
<p>14 – Apple Benelux B.V.</p> <p>Information from user identity profile may be used by the PCF to generate PCC rules</p>
<p>15 – Guangdong OPPO Mobile Telecom.</p> <p>Yes, but it is capped at the current subscription.</p>
<p>16 – CATT</p> <p>Yes, QoS may be adjusted.</p>
<p>17 – Philips International B.V.</p> <p><apologies for the late input> Yes.</p>

Feedback Form 8: Question KI#1.8: When a user is active with a subscription, is information from the user profile used to determine how to influence QoS for the UE's PDU Session(s)?

<p>1 – Ericsson LM</p> <p>It may, via AF influencing 5GC e.g. AF request for QoS</p>
<p>2 – Deutsche Telekom AG</p> <p>Not sure how this question is different to previous. Answer to the question is yes.</p>

<p>3 – vivo Mobile Communication Co.</p> <p>yes. the same as question 1.7</p>
<p>4 – InterDigital</p> <p>Yes. QoS Parameters should be part of the user profile and the adjustment should be based on these QoS Parameters. For example, PCC Rules can be adjusted. The N4 Rules, QoS Rules, and QoS Profiles would then be adjusted based on the updated PCC Rules.</p>
<p>5 – LG Electronics France</p> <p>Yes. PCF can retrieve User Identify Profile information from UDR to apply QoS setting for a user identifier.</p>
<p>6 – HUAWEI Technologies Japan K.K.</p> <p>Yes, the UDM can provide the default QoS taking the user profile into account, and the PCF can adjust the PCC rules taking the user ID profile into account, considering it is the user id to be charged.</p>
<p>7 – China Mobile Com. Corporation</p> <p>Yes. PCF can retrieve User Identify Profile information from UDR to apply QoS setting for a user identifier.</p>
<p>8 – Motorola Mobile Com Technology</p> <p>Yes, if the user profile information is linked to specific PDU session policy control data. In our view the specific PDU session policy control data can be linked to a user identifier or user profile identifier.</p>
<p>9 – Nokia Corporation</p> <p>As described in KI#1.7, we believe that UE Subscription and the linked User Profile may want to limit QoS parameters for the allowed corresponding Applications.</p> <p>Since it is always one User Identifier active with a UE subscription at any given point of time, rules will be installed and not adjusted from UE (or different User Identifier) to the User Identifier.</p>
<p>10 – Qualcomm Incorporated</p> <p>The AF can request to influence QoS when a user is active.</p>
<p>11 – Nubia Technology Co.</p> <p>ZTE: Yes, see Answer to Q#1.7</p>
<p>12 – Samsung Electronics Czech</p> <p>Yes, if the AF influences QoS for the particular user identifier.</p>

<p>13 – Apple Benelux B.V.</p> <p>Yes, as in the answer for Q#1.7</p>
<p>14 – Guangdong OPPO Mobile Telecom.</p> <p>Yes, but it is capped at the current subscription.</p>
<p>15 – CATT</p> <p>Yes, User’s service parameters may influence the QoS.</p>
<p>16 – Philips International B.V.</p> <p><apologies for the late input> Yes, as in answer to Question KI#1.7</p>

Feedback Form 9: Question KI#1.9: In this release, when a user identifier is active with a subscription, should SMS over NAS be disabled or should it be possible to use SMS over NAS?

<p>1 – Ericsson LM</p> <p>MSISDN shall be used for SMS. If a UID is linked to an MSISDN the SMS service may be supported. Preferably, SMS for a UID may only be supported via SMSoIP</p>
<p>2 – Deutsche Telekom AG</p> <p>It should not be specific to the User but to the subscription, no impact to legacy service, i.e. it should be possible to use SMS over NAS. We (DT) in SA1 had only SMS over IMS in mind when requirements were created.</p>
<p>3 – vivo Mobile Communication Co.</p> <p>No, it is unclear why the user ID should have the association with the SMS/IMS service.</p>
<p>4 – InterDigital</p> <p>In this release, our preference is to disable the SMS service while the user is active with the subscription.</p>
<p>5 – LG Electronics France</p> <p>Since all services of the UE should be associated with a user identifier, either SMS over NAS should be supported for the user identifier or disabled while the user identifier is active.</p>

<p>6 – China Mobile Com. Corporation</p> <p>No. Don't take Voice and SMS-related services into consideration in this release.</p>
<p>7 – Motorola Mobile Com Technology</p> <p>Yes, the user profile may include information whether the SMS service is enabled or disabled for the User ID.</p>
<p>8 – Nokia Corporation</p> <p>There are solutions defined for SMS over NAS for the User Identifier and the UE Subscription based on the factors on who has the active registration with the network. As described in the solutions in the TR, SMS over NAS can be supported, and the User Identity Profile shall have additional service identifiers, like a corresponding GPSI of the User Identifier when the SMS service needs to be supported for the User Identifier. We do not see the reason for disabling and not supporting SMS services.</p>
<p>9 – Qualcomm Incorporated</p> <p>No. The security risk should be evaluated by SA3 before we start the related study in SA2.</p>
<p>10 – Nubia Technology Co.</p> <p>ZTE: neutral</p>
<p>11 – NEC Europe Ltd</p> <p>It should be available.</p>
<p>12 – Samsung Electronics Czech</p> <p>SMS service by definition is for a GPSI (either MSISDN-based or non-MSISDN-based), hence whether or not a user identifier is active on a UE or not, the SMS service should still be possible if allowed by the UE subscription.</p>
<p>13 – Apple Benelux B.V.</p> <p>In our view, a user identifier being active on a subscription should not interrupt any service that is available for that subscription. As an example , I may own my subscription with the MNO and may decide to activate /deactivate my user identifier based on the applications I am using. During this time, I dont expect that my legacy services available to my subscription is interrupted. It is another scenario when another user identifier (sort of guest user) active on my subscription. in this case, there may be a valid case for interrupting legacy services to my subscription.</p>
<p>14 – Guangdong OPPO Mobile Telecom.</p> <p>We think this feature could be deferred to next release. SMS over NAS is not specified in the scope of this study.</p>

15 – Philips International B.V.

<apologies for the late input> No strong opinion whether or not to defer SMS to a next release as long as it is solved in the end.

Feedback Form 10: Question KI#1.10: In this release, when a user identifier is active with a subscription, should it be possible to use the IMS service?

1 – Ericsson LM

If the User can log into IMS services, then yes. However, how a user can register to IMS using the UID and credentials needs to be solved by SA3

2 – Deutsche Telekom AG

Certainly yes (and ideally user profile information, e.g. preferences should be taken into account for his/her IMS services)

3 – vivo Mobile Communication Co.

whether the user id should have association with IMS service is FFS. negative for this.

4 – InterDigital

In this release, our preference is to disable the IMS service while the user is active with the subscription.

5 – LG Electronics France

Since all services of the UE should be associated with a user identifier, either IMS should be supported for the user identifier or disabled while the user identifier is active.

6 – China Mobile Com. Corporation

No. Don't take the IMS service into consideration in this release

7 – Motorola Mobile Com Technology

Yes, the user profile may include information whether the IMS service is enabled or disabled for the User ID, i.e. the IMS service may be disabled for a User ID (however enabled by default).

8 – Nokia Corporation

As described in KI#1.9. the User Identity Profile may have additional service identifiers like IMPU for the User Identities.

<p>9 – Qualcomm Incorporated</p> <p>No. The security risk should be evaluated by SA3 before we start the related study in SA2.</p>
<p>10 – Nubia Technology Co.</p> <p>ZTE: similar answer to Q#1.9</p>
<p>11 – Samsung Electronics Czech</p> <p>Similar to the answer in 1.9, IMS service should be allowed as usual as per the UE subscription</p>
<p>12 – Apple Benelux B.V.</p> <p>As described in our response for Q#1.9.</p>
<p>13 – Guangdong OPPO Mobile Telecom.</p> <p>Involving IMS service to a specific User Identifier might be complex which is beyond the TU of this release, which we think could be deferred to the next release.</p>
<p>14 – Philips International B.V.</p> <p><apologies for the late input> No strong opinion whether or not to defer IMS to a next release as long as it is solved in the end.</p>

Feedback Form 11: Question KI#1.11: How does a linked user become active with a subscription?

<p>1 – Ericsson LM</p> <p>When the User is authenticated and authorised towards the entity managing the UIP for the UID used. Then via PCF/NEF APIs the managing entity may request QoS and guide 5GC</p>
<p>2 – Deutsche Telekom AG</p> <p>During PDU Session establishment and IMS registration only.</p>
<p>3 – InterDigital</p> <p>The UE sends a NAS message (Registration, PDU Session Establishment, or PDU Session Modification) to the network and the NAS message includes an indication that a user wants to become active.</p>

<p>4 – LG Electronics France</p> <p>UE sends Registration Request with a user identifier to activate the user identifier.</p>
<p>5 – HUAWEI Technologies Japan K.K.</p> <p>After the user is authenticated during the PDU Session establishment, it becomes active.</p>
<p>6 – China Mobile Com. Corporation</p> <p>After the user is authenticated during the PDU session establishment/modification</p>
<p>7 – Motorola Mobile Com Technology</p> <p>Either the UE includes a user identifier (indicating an active user), or the AF indicates that a user with specific user identity is active.</p>
<p>8 – Nokia Corporation</p> <p>A single entity (UE Subscription or a User Identifier) is active at any given point of time. A User Identifier may use Data services, SMS services, etc. It would be inefficient with additional handling to have a User Identifier linked and be active in the network if we use the procedures like PDU Session procedures (multiple PDU Sessions), AF based (external control and need additional validations, implementation dependencies for the use case to be realized).</p> <p>Considering these, we prefer to have the Authentication and linking being done during the Registration procedure and rest of the services (NFs) are agnosticized of linking and authenticating.</p>
<p>9 – Qualcomm Incorporated</p> <p>It can be achieved via application layer interaction. We don't see the necessary and benefit of using NAS signaling.</p>
<p>10 – Nubia Technology Co.</p> <p>ZTE: UE send NAS message (e.g. Registration).</p>
<p>11 – NEC Europe Ltd</p> <p>With the Registration procedure (in a NAS message).</p>
<p>12 – Samsung Electronics Czech</p> <p>After successful authentication and authorization of the user identifier.</p>

13 – Apple Benelux B.V.

An active user identifier is included in the Registration procedure by the UE. This may trigger authentication and authorization . The user becomes active based on the result of these procedures.

14 – Guangdong OPPO Mobile Telecom.

Once the user is authenticated, the state of the user active/inactive/suspended should be determined by AMF or SMF.

15 – Philips International B.V.

<apologies for the late input> Agree with Apple.

Feedback Form 12: Question KI#1.12: Which principles can be selected or considered for key issue #1 conclusions? Also identify, if possible, which solution(s) the principles are taken from.

1 – Ericsson LM

- The UID may be assigned and managed by the MNO or by a 3rd party
- The UIP standardized in 3GPP is managed by the MNO
- The subscriber can manage the UIP associated to a subscription via a management interface provided by the MNO
- The UIP is stored in the HPLMN, in an MNO operated entity e.g. AF or new NF
- The UIP can include:
 - credentials for authentication if UID assigned by the MNO
 - QoS differentiation information (also mapping between user friendly parameters to 3GPP level parameters)
 - Information related to Guidance for URSP e.g. DNN and S-NSSAI to be used when User Link active
 - Service differentiation information e.g. to initiate parental control (standardize or not?), information for SMS and IMS services.
- No impacts to VPLMN (at roaming)
- Existing services towards the PCF are re-used e.g. for requesting QoS differentiation
- No impacts to UDM as UIP is enabling service differentiation on top of subscriptions.
- The MNO operated entity managing the UIP, e.g. AF or new NF, uses services towards the 5GC e.g. towards the PCF for QoS differentiation.
- MSISDN is used for SMS over NAS or IMPU for IMS

2 – InterDigital

The principles of Solution #3 are preferred. Solution #3 describes procedures where the user profile information can be provisioned and exposed via the NEF, users can be linked to subscriptions via the NEF, and the UE can provide the user identifier that needs to become active in the registration request. How the user is authenticated can be left to SA WG#3. We prefer that the UE can provide the user identifier that needs to become active in a Registration Update message, however, if it is decided that it is preferred to go with an approach where the user identifier that needs to become active is provided during PDU Session Establishment, then Solution #1 is our preference.

Solution #25 only focuses on the format of the user identifier, and we prefer this approach for formatting the user identifier (i.e. an NAI that can be operator assigned or assigned by a third party).

There are solutions that share the same principles as Solution #1 and there are solutions that share the same principles as Solution #3.

3 – LG Electronics France

User Identity Profile is Linked/Unlinked by the AF using NEF service. UE sends Registration Request with a user identifier to activate the user identifier. When the user identifier is activated, all PDU Sessions are released and re-established. During the PDU Session establishment, PCF retrieves user identity profile from UDR to apply user identifier specific QoS. Sol#3 can be taken as a baseline.

4 – Motorola Mobile Com Technology

Principle 1: Either UDM or AMF can store and maintain active user identifier. The UDM may send the active user ID to the AMF.

Principle 2: At a PDU session request UE determines active user and includes related user identifier. UE may determine the user identifier based on local user profile information provisioned by an operator controlled AF (as per Solution 1)

Principle 3: At PDU session est request (as per Solution 1),

- AMF includes the active user ID (based on user profile and identifies User Profile linked to user identity) in the request message to the SMF.
- SMF includes active user identifier to PCF.
- PCF retrieve user profile information from UDR and applies related applicable policies in the PDU session

Principle 4: During registration procedure, the PCF may create AM/UE Policies based on the user profile associated to an active user id.

5 – Qualcomm Incorporated

The user identity can be managed and authenticated via application layer in an AF. When a user identity is activated with a subscription, AF can trigger the service differentiation to 5GC.

The human user has to interact with a UI that is part of HLOS that is out of scope of 3GPP and therefore this is the only place where the human user can be authenticated. Stemming from that any further authentication with the 3GPP system is unnecessary since the "owner of UI" (e.g. HLOS) has to be trusted by the 5GS.

6 – Nubia Technology Co.

ZTE: For the provisioning/link/unlink, the solution#3 or #17 (quite similar) can be select. For UID activation procedure, it depends on the conclusion for Q#1.11. When a UID is active, how to notify the ongoing PDU session, or future PDU session, the solution#17 can be selected.

7 – Nokia Corporation

Following principles shall be selected/considered:

- User Identifier shall be a NAI, which is unique inside a PLMN(Solution #1, #10, #17, #18)

- User profile

 - o is stored in UDM/UDR

 - (Solution #1, #2, #3, #4, #5, #6, #8, #10, #14, #16, #17, #18, #20, #21, #23, #26)

 - o Security Credentials, Policies (QoS), Linked devices

 - (Solution #1, #4, #5, #7, #17, #18, #23)

- Linking and Unlinking of User profile with UE Subscription via

 - o NEF/AF

 - (Solution #1, #3, #10, #17, #18, #19, #23)

 - o OAM

 - (Solution #10, #17)

- Signaling of human User/device Flag during Registration to distinguish human User, device, and or UE registration

 - (Solution #10)

- User activation/deactivation of human User is performed during registration process and allows to provide

 - o Providing individual 3GPP identifiers for human Users to UE to offer 3GPP services like Voice, IMS, and SMS over NAS

 - (Solution #6, #10, #17)

 - o Policies for a human User to restrict a linked UE subscription

 - (Solution #1, #2, #3, #10, #17, #19, #20, #26)

8 – Guangdong OPPO Mobile Telecom.

The following solution principles for KI#1 are proposed:

- A UIP may include one or multiple User Identities [Sol#1, #2, #3, #4, and #5]
- Each User Identity should be associated with at least the following attributes:
 - User ID
 - User Identity specific service settings and parameters
 - QoS information
- UIP is stored in UDM/UDR [Sol#1, #2, #3, #4, and #5]
- The User Identity is identified by a PLMN-unique User Identifier, which can be further linked/unlinked with a 5GS subscription identified by a SUPI. The User ID could also be used for authentication and authorization to access 5G service. [Sol#1, #2, #3, #4, and #5]
- User ID association and traffic association could be supported by using enhanced session management procedures with User ID support. [Sol#1-3]
- User ID management should be implemented to support User ID status, activation, linking/unlinking, and access to specific services. [Sol#1-7]

9 – Philips International B.V.

<apologies for the late input> See answers to previous questions.

2.2 Key Issue #2

Feedback Form 13: Question KI#2.1: When the user is authenticated, authentication is performed between the UE and what entity?

1 – Deutsche Telekom AG

AAA-server

2 – Ericsson LM

Between the UE and the entity managing the UIP e.g. UIP server or an AAA-S associated to the entity managing the UIP.

<p>3 – InterDigital</p> <p>A AAA Server.</p>
<p>4 – LG Electronics France</p> <p>Either DN-AAA or UDM. If User Identity Profile is managed by operator, 5GC should be able to perform authentication. If User Identity Profile is managed by 3rd party, 5GC should be able to authenticate user identifier by interworking with 3rd party AAA.</p>
<p>5 – HUAWEI Technologies Japan K.K.</p> <p>Huawei: Either between UE and AAA Server when the User Identity is managed by third party or between UE and UDM/AUSF when the User Identity is managed by the operators..</p>
<p>6 – China Mobile Com. Corporation</p> <p>Operator internal AAA server or external third-party AAA.</p>
<p>7 – Motorola Mobile Com Technology</p> <p>Between UE and AAA server. How the UE receives credentials for authentication/authorisation to the AAA server is out of scope.</p>
<p>8 – Nokia Corporation</p> <p>SA2 shall define that the authentication is carried out for the User Identifier. So, it shall be UDM, AUSF, AAA Server, etc. Further details shall be defined at SA3.</p>
<p>9 – Qualcomm Incorporated</p> <p>Authentication is performed between the UE and AF.</p>
<p>10 – Nubia Technology Co.</p> <p>ZTE: UDM/AUSF, or UDM/NSSAAF/AAA-S</p>
<p>11 – NEC Europe Ltd</p> <p>AAA Server</p>
<p>12 – Samsung Electronics Czech</p> <p>The authentication can be performed between UE and AAA-S (or UIDF implementing AAA server) and the 5G-NFs will be transparently forwarding the data between these two entities.</p>

13 – Apple Benelux B.V. UE and AAA server
14 – Guangdong OPPO Mobile Telecom. Authentication should be performed between UE and AAA server, with the assistance of AMF.
15 – Philips International B.V. <apologies for the late input> Agree with LG and Huawei.

Feedback Form 14: Question KI#2.2: Should interaction between the UE and entity (i.e. the entity from the previous question) be via NAS or user plane?

1 – Deutsche Telekom AG user plane
2 – Ericsson LM Via User Plane during UIP management procedures, but also possible via EAP over NAS via secondary authentication if secondary authentication is used to activate a User Link.
3 – vivo Mobile Communication Co. neutral.
4 – InterDigital NAS, similar to Secondary Authorization / Authentication by a DN-AAA Server during PDU Session Establishment or similar to Network Slice Specific Authentication and Authorization by a AAA-S.
5 – LG Electronics France NAS signalling connection. Similar procedure like primary authentication or NSSAA can be used.
6 – China Mobile Com. Corporation NAS

7 – Motorola Mobile Com Technology

Optionally, the network operator may choose to authenticate a user ID provided by the UE using existing mechanism (e.g. Secondary authentication/authorisation during PDU session establishment).

8 – Nokia Corporation

We prefer that the Authentication of the User Identifier using the UE Subscription is done in the similar way as done for the UE Subscription. These are proven techniques, and we prefer to leverage the same instead of bringing in new additions to the architecture.

So, we strongly recommend using the NAS.

9 – Qualcomm Incorporated

Interaction via application layer in User Plane.

10 – Nubia Technology Co.

ZTE: via NAS

11 – NEC Europe Ltd

via NAS. Similar to Network Slice Specific Authentication and Authorization by a AAA-S.

12 – Samsung Electronics Czech

The user can be authenticated via NAS-MM or NAS-SM. Similar to UAV authentication where both (UUAA-MM & UUAA-SM) procedure is allowed. A similar mechanism can be kept here as well.

the authentication can be triggered either when UE sends the user identifier during the NAS procedure or 3rd party requests 5GC to trigger user identity authentication.

13 – Apple Benelux B.V.

NAS procedures

14 – Guangdong OPPO Mobile Telecom.

NAS

15 – Philips International B.V.

<apologies for the late input> NAS procedures.

Feedback Form 15: Question KI#2.3: What entity enforces the restriction that only one user shall be active with a UE's subscription at a given time?

1 – Deutsche Telekom AG

UDM seems to be the simplest choice to us, **especially as this artificial limitation was introduced to reduce the SID scope and therefore should not require extra efforts in SA2 and it should not hinder future extension to more than one active users simultaneously at a given time.** It would be even better to consider this limitation in a way that solutions should enable easy extension in future releases to allow more than one user in parallel.

2 – Ericsson LM

The entity managing the UIP, e.g. UIP server.

3 – InterDigital

The UDM. If a user is active with a subscription, the user identity of the active user should be stored in the UE's subscription.

4 – LG Electronics France

By the UDM.

5 – HUAWEI Technologies Japan K.K.

AMF or UDM.

6 – China Mobile Com. Corporation

UDM

7 – Motorola Mobile Com Technology

The UDM ensures one active user ID. UDM may take active user input from the UE (i.e. the UE ensures one active user ID at any time) or from the AF.

8 – Nokia Corporation

As described in the above KI, the UDM shall maintain the User Identity Profile and accordingly a UECM registration for the User Identity will ensure the state machine is maintained. So, without impacting additional nodes, it is required that UDM takes the control as currently done for the UE Subscription and enforces that only one User Identity is active with a UE Subscription.

So, the enforcement shall be at the UDM from the network point of view. Also, the UE too could enforce.

<p>9 – Qualcomm Incorporated</p> <p>AF and UE.</p>
<p>10 – Nubia Technology Co.</p> <p>ZTE: UDM</p>
<p>11 – Samsung Electronics Czech</p> <p>UDM can store whenever a user identifier becomes active on a SUPI. Any other entity (AMF -> for registration-based/SMF->for PDU SE-based) can then query the UDM to check if another user is active and then apply the restriction that only one user shall be active.</p>
<p>12 – Apple Benelux B.V.</p> <p>UDM - for each subscription data, it can maintain the state of active user identifier. There can be 0 or 1 active user identifier per subscription.</p>
<p>13 – Guangdong OPPO Mobile Telecom.</p> <p>AMF should enforce this restriction. UDM/UDR could store the information of the user's state, but it is not recommended to let UDM enforce the restriction.</p>
<p>14 – Philips International B.V.</p> <p><apologies for the late input> Agree with Samsung.</p>

Feedback Form 16: Question KI#2.4: Which principles can be selected or considered for key issue #2 conclusions? Also identify, if possible, which solution(s) the principles are taken from.

<p>1 – Ericsson LM</p> <ul style="list-style-type: none">- Admin that assigns the UID also provide means to authenticate the UID (AAA etc)- No impacts to VPLMN (at roaming)- No impacts to UDM as UIP is enabling service differentiation on top of subscription- No final conclusions on authentication can be done without SA3 input

2 – vivo Mobile Communication Co.

No or less impact to NAS layer, have only one authentication procedure of user id.

3 – InterDigital

The principles of solution #8 are preferred for establishing a framework for authenticating the UE. The details can be left to SA WG#3. In solution #8, the AMF triggers authentication. If it is decided that it is preferred to go with an approach where the user identifier is provided during PDU Session Establishment, then Solution #1 is our preference.

In terms of enforcing the restriction, we prefer the principles of Solution #17, specifically section 6.17.3.2.

There are solutions that share the same principles as Solution #8 and there are solutions that share the same principles as Solution #3.

4 – LG Electronics France

Authentication is performed with DN-AAA or UDM. The UDM forces the restriction that only one user shall be active with a UE's subscription at a given time.

5 – Motorola Mobile Com Technology

Optionally user id authorisation at PDU session establishment request as per Solution 1.

6 – Qualcomm Incorporated

The security risk and authentication mechanism of user identity need to be studied in SA3.

7 – NEC Europe Ltd

The principles of solution #8. In solution #8, the AMF triggers the user specific authentication.

8 – Nokia Corporation

Following principles shall be selected/considered:

- Authentication and Authorization of human Users via registration procedure

o Signalization of human User/device Flag during Registration to detect the human User case (Solution #10)

o Adaptation of current Registration procedure to support User identifier for human User by adding User identifier together with SUPI of UE in the signaling

(Solution #2, #4, #10, #14, #21, #22. #26)

o Privacy solution for User identifier via radio interface similar to SUCI/GUTI method (details shall be specified by SA3)

(Solution #10, #22)

o User activation/deactivation of human User is performed during registration process

(Solution #4, #10, #17, #3, #8, #9, #14, #21, #26)

- Support of services like SMS over NAS

(Solution #6, #10, #28)

- Authentication and Authorization to provide User profile and UE subscription related information to 5GS shall be performed in an Application Server which is out of scope in 3GPP SA2. Nevertheless, SA3 shall provide respective principles to protect the unauthorized manipulation of User profile and UE subscription information. This includes:

o linking/unlinking User profiles with UE subscriptions

(Solution #2, #10, #17, #18, #23)

o restricting UE subscriptions for a human User profile

(Solution #3, #10, #17, #19, #23)

o max number of human Users

(Solution #10)

- MNO shall be able to restrict max number of human User for a UE subscription

(Solution #10)

9 – Samsung Electronics Czech

Both AMF and SMF-based authentication procedure and enforcement of a single active user identifier on the system is recommended

10 – Guangdong OPPO Mobile Telecom.

AMF as authenticator to reuse EAP based authentication to authenticate User ID by AAA Server.

11 – Philips International B.V.

<apologies for the late input> Agree with LG.

2.3 Key Issue #3

Feedback Form 17: Question KI#3.1: How is user profile information and functionality exposed?

1 – Deutsche Telekom AG

via NEF APIs

<p>2 – Ericsson LM</p> <p>Exposure APIs (perhaps CAPIF) from the entity managing the UIP, which is outside the 5GC</p>
<p>3 – vivo Mobile Communication Co.</p> <p>netural.</p>
<p>4 – InterDigital</p> <p>Via NEF API.</p>
<p>5 – LG Electronics France</p> <p>By using NEF service.</p>
<p>6 – HUAWEI Technologies Japan K.K.</p> <p>via NEF APIs</p>
<p>7 – China Mobile Com. Corporation</p> <p>via NEF APIs</p>
<p>8 – Nokia Corporation</p> <p>We should leverage the existing exposure architecture. NEF shall be able to extend the services (API) that shall be used by the AF and then the NEF could fetch the information from 5GC NFs like UDM, NWDAF and provide response to the NEF/AF.</p>
<p>9 – Qualcomm Incorporated</p> <p>The user profile is managed by AF, and can be exposed to 5GC via Naf.</p>
<p>10 – Nubia Technology Co.</p> <p>ZTE: NEF API</p>
<p>11 – Samsung Electronics Czech</p> <p>using NEF APIs</p>
<p>12 – Guangdong OPPO Mobile Telecom.</p> <p>Existing NEF API with extra parameters</p>

13 – Philips International B.V.

<apologies for the input> NEF

Feedback Form 18: Question KI#3.2: What user profile information can be exposed? For each piece of information, please describe a use case.

1 – Ericsson LM

Capabilities to manage e.g. create, update and remove a UIP. For other, we need use cases to know which information that can be of interest

2 – InterDigital

In addition to what has already been concluded...

It should be possible to expose, to an authorized AF, the subscriptions that are linked to a user identifier. The use case is so that the AF can check which subscriptions the user is already linked to (i.e. before requesting that a subscription and user identifier be linked).

It should be possible to expose, to an authorized AF, the user identifiers that are linked to a subscription. The use case is so that the AF can check which subscriptions the user is already linked to (i.e. before requesting that a subscription and user identifier be linked).

It should be possible to expose, to an authorized AF, what user identifier is active with a subscription. The use case is that AF could use the user identifier to adjust settings, or services, in the N6-LAN (e.g. parental controls).

3 – LG Electronics France

Authentication/Authorization result. This can be used by application to check validity of user.

4 – HUAWEI Technologies Japan K.K.

Authentication result of the user ID, to bring new revenue to operators to provide authentication exposure as a service.

5 – Nokia Corporation

Any information that is exposed shall consider privacy aspects (of the User Identifier and the corresponding UE Subscription) defined by SA3. Following information can be considered as part of the exposure:

- Current state of the User Identifier

- Linked UE Subscriptions
- Current registration status and the corresponding UE Subscription
- PCC Rules
- Services and the associated identifiers
- Last N authentication results
- Last N authorization results

6 – Nubia Technology Co.

ZTE: UID Provisioning, the AF can create/update the user identity profile. UID and subscription Link/unlink, UID activation result

7 – Samsung Electronics Czech

Whether a User identifier is active or not (based on whether 5GC can/could successfully authenticate a user identity associated with that user identifier) for the use case as currently described in the interim conclusions (i.e. operator's authentication exposure service).

8 – Apple Benelux B.V.

Through a NEF API, 5GC should only expose whether a user identifier is active with a subscription or not. NEF APIs should not enable possibility for an AF to provide one user identifier and request all related information from 5GC (The user identity exposure feature should not be used as a method for "phishing information" from the operator)

9 – Guangdong OPPO Mobile Telecom.

Authentication result along with User ID, in the case of Single Sign-on where the User ID and its authentication results could be used to enable the user to securely access other applications and services.

10 – Philips International B.V.

<apologies for the late input> Agree with Nokia

Feedback Form 19: Question KI#3.3: Which principles can be selected or considered for key issue #3 conclusions? Also identify, if possible, which solution(s) the principles are taken from.

1 – Ericsson LM

- Any exposure must be use case driven
- Exposure APIs (perhaps CAPIF) from the entity managing the UIP, which is outside the 5GC

2 – InterDigital

Solution #15 for verifying whether a user is linked to a subscription.

Solution #16 for exposing information from the profile, specifically section 6.16.3.1. We see value in exposing historical results as described in 6.16.3.2 but prefer not to expose historical results in this release.

3 – LG Electronics France

Authentication/Authorization result can be exposed by using NEF service.

4 – Nubia Technology Co.

ZTE: see answer to Q#3.2. For the privacy check, the principle in the solution#29 can be considered. SA2 also needs to cooperate with SA3 in this regard.

5 – Nokia Corporation

Solutions 10, 15, 16, 29 to be considered. And the following principles shall be agreed:

- All exposure adheres to privacy profile and in co-ordination with SA3.
- Exposure of User Identities and information shall be based on privacy profile.
- Exposure of authentication and authorization results (with some historical data).
- Provisioning of User Identity Profile (and corresponding User Identifier), linking and unlinking of User Identifier with the UE Subscription shall be possible.

6 – Samsung Electronics Czech

Clarify the currently agreed conclusion that verification results may be obtained based on the user identity authentication performed by the 5GC for the specific user identifier.

Taken from Solution#11 and partly from solution#15

7 – Apple Benelux B.V.

Verification result of whether a user identifier is active with a subscription.

8 – Guangdong OPPO Mobile Telecom.

To use existing Nnef_EventExposure service operation to expose authentication results along with User ID.

9 – Philips International B.V.

<apologies for the late input> Agree with Nokia

2.4 Key Issue #4

Feedback Form 20: Question KI#4.1: Is it necessary for the 5GC to be able to identify traffic from each individual non-3GPP device (i.e. in scenarios where differentiation for charging is desired)?

1 – CableLabs

The question seems misleading with “(i.e., in scenarios where differentiation for charging is desired)”. Based on the agreed KI#4 “The objective of this key issue is how an identifier is used by the network to control the traffic to/from UE or 5G-RG when the traffic is associated with the non-3GPP devices”, and solutions, we believe it is necessary for the 5GS (e.g., 5GC and/or 5G-RG) to identify traffic from each individual non-3GPP device primarily for QoS provisioning. However, whether this will be used for different charging or not is a separate question, so we propose to change the question as

- *“Is it necessary for the 5GSC to be able to identify traffic from each individual non-3GPP device (i.e. in scenarios where differentiation for charging is desired)?”*.

Minimum, we should replace “i.e.” to “e.g.” as charging is an example to utilize identified traffic/device.

2 – CableLabs

If the question is whether to support additional charging based on identification of individual devices (e.g., parental control or speed boosting), we believe that’s beneficial though we have not discussed charging aspects in details. Note that 5G-RG is considered as trusted (e.g., operator controlled) and charging/QoS provisioning is done at the 5G-RG though traffic is coming from non-3GPP devices behind the 5G-RG. When we discuss authentication/authorization, this aspect should be considered in our view.

3 – Ericsson LM

For IP PDU sessions, it is only needed for 5GC to identify traffic based on either port ranges or IPv6 prefixes. How UE/5G-RG maps a device (or even devices) to this port range/IPv6 prefix is out of SA2 scope. For Ethernet PDU sessions, individual devices can be identified via MAC address.

In general, this is only needed in case of QoS differentiation and information to charging output (we don’t see charging differentiation for a subscription, but which “device” did what can be needed in the billing information)

4 – vivo Mobile Communication Co.

yes. The network can arrange the device id. And both the device id and the IP address that arranged by the UE to identify the device behind the UE.

5 – InterDigital

Yes

6 – LG Electronics France

Based on operator’s policy, if charging differentiation is required, it should be supported.

7 – Charter Communications

YES, it is necessary for the 5GC to be able to identify traffic from each individual non-3GPP device.

HOWEVER, the primary motivation of such identification is for us (as an operator) NOT to charge individual non-3gpp devices behind an 5G-RG but to be able to perform policy control for each non-3GPP device. As discussed during the formulation of the SID, examples use cases are as follows:

- provide a higher or lower priority treatment for an individual non-3GPP device based on the request of the 5G-RG subscriber/admin.
- allow parental control type services (e.g., limit access to internet for an individual non-3GPP device) based on the request of the 5G-RG subscriber/admin.

In our humble opinion, the text in parenthesis is misleading as it uses “i.e.”. The corresponding Key Issue in the TR has the following text, which uses “e.g.”.

“whether and how the 5GC identifies individual non-3GPP devices connecting behind a UE or 5G-RG. (e.g. in order to charge the individual non-3GPP devices),”

In addition, the operator only charges the 5G-RG subscriber but not the individual non-3GPP devices connecting behind the 5G-RG.

8 – HUAWEI Technologies Japan K.K.

Yes, this is the objective of the study for KI#4.

9 – China Mobile Com. Corporation

Yes

10 – Motorola Mobile Com Technology

Yes the solutions agreed in the TR already support identifying traffic from each non-3GPP device.

11 – Nokia Corporation

Why is this specific question of charging is considered? This is not in the scope of this study or talked about.

The use case defined in the study requires that 5GS needs to identify the traffic and implement PCC Rules for the traffic that is identified with certain identity configured for the UE Subscription.

5GS could additionally optionally include the information of the identifier that it identified for traffic flows in the current communication with the CHF.

<p>12 – Qualcomm Incorporated</p> <p>No.</p> <p>5GC can provide service differentiation for the device traffic based on URSP or AF request, but no need to identify the device ID.</p> <p>The use cases mentioned in the SID e.g. parental control, service differentiation in the form of different QoS levels warrant that the 5GS provides a small handful of PDU sessions with different policies each e.g. parental control Vs not, gold/silver/bronze QoS etc and the non 3GPP device traffic maps to one of these PDU sessions.</p>
<p>13 – NEC Europe Ltd</p> <p>Yes</p>
<p>14 – Nubia Technology Co.</p> <p>ZTE: Yes. If the Qos/policies for different non-3gpp devices are different</p>
<p>15 – Samsung Electronics Czech</p> <p>Yes</p>
<p>16 – Apple Benelux B.V.</p> <p>We agree with Ericsson that 5GC may only need to identify traffic based on either port ranges or IP6 prefixes.</p>
<p>17 – Guangdong OPPO Mobile Telecom.</p> <p>Yes</p>
<p>18 – Philips International B.V.</p> <p><apologies for the late input> Agree with Charter</p>

Feedback Form 21: Question KI#4.2: Is it necessary to specify a procedure to facilitate authentication via the 5GC of the user identifier associated with each individual non-3GPP device(s) connecting behind the UE or 5G-RG (i.e. to enable service differentiation and charging)?

<p>1 – CableLabs</p> <p>In our view, whether/how to authenticate/authorize a non-3GPP device is up to SA3. SA2 work may assume proper authorization of applying policy for a non-3GPP has occurred. For example, a non-3GPP device may be authenticated locally by 5G-RG or may be authenticated via EAP-based mechanism. Policy provisioning on 5G-RG by 5GC for non-3GPP devices should be SA2 focus in our view.</p>
--

2 – Ericsson LM

No, it is up to the implementation of UE/5G-RG to make sure that the Device behind it is authenticated,. Authentication of the device behind the UE/RG would be applicable in case the charged party is to be changed but our view is that this is not required nor needed. However, the UE/5G-RG needs to be authenticated for this service, this by means of secondary authentication or direct authentication to an application server outside of 5GC.

3 – vivo Mobile Communication Co.

it seems that identify the device is enough, no other obvious benefit to further authentication. needs more clarification for this and open for this

4 – InterDigital

Yes. This is needed for charging in scenarios where the non-3GPP device is provisioned with credentials and a user identifier.

5 – InterDigital

Yes. This is needed for charging in scenarios where the non-3GPP device is provisioned with credentials and a user identifier.

6 – LG Electronics France

Can be supported optionally. Not mandatory.

7 – Charter Communications

NO, it is NOT necessary to specify a procedure to facilitate authentication via the 5GC of the individual non-3GPP device(s) connecting behind the 5G-RG to enable service differentiation and charging. In other words, the non-3GPP devices connecting behind 5G-RG can be authenticated via existing commonly deployed authentication methods by WLAN-AP/5G-RG that may not involve 5GC.

Authentication of non-3GPP devices by the 5GC does NOT need to be a prerequisite for service differentiation (and/or charging) for non-3GPP devices behind 5G-RG.

8 – HUAWEI Technologies Japan K.K.

The authentication is not for the non-3GPP device, but for the user id associated with the non-3GPP device which identify the user or the subscriber of the non-3GPP device. And whether to authenticate the non-3GPP device or not is optional for operator to decide. May not be needed for all non-3GPP devices, but 3GPP needs to provide the mechanism to facilitate it.

<p>9 – China Mobile Com. Corporation</p> <p>Yes. This is needed for charging in scenarios where the non-3GPP device is provisioned with credentials and a user identifier.</p>
<p>10 – Motorola Mobile Com Technology</p> <p>We can use the existing procedure to authenticate the device ID/user ID, i.e. using secondary authentication/authorisation during PDU session establishment/modification</p>
<p>11 – Nokia Corporation</p> <p>Authentication of non-3GPP devices is not in the scope of the study. However, any authentication of the non-3GPP devices shall be taken care by the UE or 5G-RG in similar ways that a UE or 5G-RG authenticates the tethering connections. These mechanisms are well defined by the UE or 5G-RG already.</p> <p>Hence there is no need to bring in additional authentication here, but just identify the traffic flows and implement the policies defined for the identity that is representing a specific traffic.</p>
<p>12 – Qualcomm Incorporated</p> <p>No.</p>
<p>13 – NEC Europe Ltd</p> <p>No, it is up to the implementation of UE/5G-RG to make sure that the Device behind it is authenticated.</p>
<p>14 – Nubia Technology Co.</p> <p>Not mandatory. It depends on whether the 5GC identifies the non-3gpp device via authentication procedure.</p>
<p>15 – Samsung Electronics Czech</p> <p>Yes</p>
<p>16 – Apple Benelux B.V.</p> <p>No</p>
<p>17 – Guangdong OPPO Mobile Telecom.</p> <p>No, there are solutions that does not need to specify such an authentication. The user identifier associated with each individual non-3GPP device connecting behind the UE or 5G-RG could be assigned by the 5GS operator.</p>
<p>18 – Philips International B.V.</p> <p><apologies for the late input> Agree with Cablelabs.</p>

Feedback Form 22: Question KI#4.3: Is it necessary to specify a procedure where the UE or 5G-RG binds/associates the user identifier to a non-3GPP device without requiring authentication via the 5GC of the non-3GPP device (i.e. to enable service differentiation without charging)?

1 – CableLabs

This question seems mis-leading in a few aspects:

- It ties association/binding to service differentiation without charging: association/binding at the 5G-RG can be used for service differentiation and potentially for charging purpose. Not sure why "*i.e. to enable service differentiation without charging*" is mentioned in the question.
- It seems limiting solutions of identification/binding at UE/5G-RG: different solutions may consider association by 5GC and/or 5G-RG
- As mentioned earlier, we believe authentication aspects should be left to SA3.

Thus, we like to rephrase as follows:

- *Is it necessary to specify a procedure where 5GS(5GC and/or UE or 5G-RG) enables ~~that the UE or 5G-RG to binds/associates the user identifier to a non-3GPP device without requiring authentication via the 5GC of the non-3GPP device~~(i.e. to enable service differentiation without charging)?*

Based on the revised question, we see this is necessary. A non-3GPP may be authenticated by AAA via 5GC or may be locally authenticated. But 5GC and/or 5G-RG should be able to identify the non-3GPP device and bind the non-3GPP device with the UE or 5G-RG. Note that charging and policy provisioning are for 5G-RG not for individual non-3GPP device. For example, parental control is managed in the 5G-RG not in a non-3GPP device. In that sense, as long as, proper mechanism to authenticate/authorize services on 5G-RG is in-place, mapping between policies and non-3GPP devices can be done by 5G-RG and/or 5GC.

2 – InterDigital

Yes. This use case is a scenario where there is an RG in the home and the homeowner wants to allow non-3GPP device(s) in the home to connect. The homeowner has control over the RG and can identify which user identifiers are associated with each non-3GPP device. The non-3GPP device would likely use a PSK to connect to the RG. Since the homeowner has control over the RG and the non-3GPP devices, the PSK based authentication and authorization between the non-3GPP device an RG is sufficient.

3 – LG Electronics France

Yes.

4 – Charter Communications

We have similar view as CableLabs. Depending on the solution, the binding/association of one or more user identifier(s) of a non-3GPP device can be at the 5G-RG and/or at the 5GS.

In our view, the text in parenthesis seems misleading because it implies the authentication of an individual non-3GPP device behind an 5G-RG via/by the 5GC is required for charging. Please also see relevant aspects in our replies to Questions KI#4.1 and #4.2.

5 – Nokia Corporation

Why is this specific question of charging is considered?

The use case defined in the study requires that 5GS needs to identify the traffic and implement PCC Rules for the traffic that is identified with certain identity configured for the UE Subscription.

So, it is not required to additionally define authentication mechanisms. 5GS could also include the information of the identifier that it identified for traffic flows in the current communication with the CHF.

6 – Qualcomm Incorporated

No.

7 – NEC Europe Ltd

No, it is up to the implementation of UE/5G-RG

8 – Samsung Electronics Czech

Need to define the scenario,

if the device identification is only specific to a particular UE/5G-RG then authentication with 5GC may not be required (still a local authentication may be needed), because in this case, the subscriber of UE/5G-RG itself has requested (in prior) specific QoS for the particular device.

if the device identifiers are identifiable across subscriptions, (that is same device profile can be used when a particular device Identifier accesses via different UEs/5G-RGs) then the authentication with 5GC is required.

9 – Guangdong OPPO Mobile Telecom.

Yes, it is necessary to support this scenario.

10 – Philips International B.V.

<apologies for the late input> Agree with CableLabs.

Feedback Form 23: Question KI#4.4: In this release, should the operator be able to optionally restrict the number of simultaneously active User Identifiers per UE or 5G-RG?

<p>1 – CableLabs</p> <p>We are neutral but consider this as a low priority.</p>
<p>2 – Ericsson LM</p> <p>The number of different service differentiations can be enabled by the operator, e.g. by allowing a maximum number of IPv6 Prefixes, IPv4 port ranges or MAC addresses via configuration</p>
<p>3 – InterDigital</p> <p>Yes, but we would also be ok with concluding that it is not possible to support this restriction in this release.</p>
<p>4 – vivo Mobile Communication Co.</p> <p>we can do it by the IP address arrangement allocation by network to limit the device.</p>
<p>5 – LG Electronics France</p> <p>No strong view.</p>
<p>6 – Charter Communications</p> <p>It is considered a low priority feature/capability.</p> <p>The ambition of the key issue should be to identify non-3GPP devices connecting behind the 5G-RG to be able to provide differentiated service by the 5G-RG subscriber when (s)he would like to.</p>
<p>7 – HUAWEI Technologies Japan K.K.</p> <p>Yes, needs to be enforced at least by the network, e.g. by the AMF.</p>
<p>8 – China Mobile Com. Corporation</p> <p>Yes, needs to be enforced at least by the network</p>
<p>9 – Motorola Mobile Com Technology</p> <p>Low priority for Lenovo</p>

<p>10 – Nokia Corporation</p> <p>We do not see a strong need for restrictions. Even if it is applied, the condition that should be enforced is of the number of identifiable non-3GPP devices and the action should be defined by the operator policies and not restrict alone as an action.</p>
<p>11 – Qualcomm Incorporated</p> <p>No.</p> <p>The use case and requirement are not clear.</p>
<p>12 – NEC Europe Ltd</p> <p>Yes</p>
<p>13 – Nubia Technology Co.</p> <p>ZTE: low priority</p>
<p>14 – Samsung Electronics Czech</p> <p>Yes</p>
<p>15 – Apple Benelux B.V.</p> <p>No , dont see the requirement for this</p>
<p>16 – Guangdong OPPO Mobile Telecom.</p> <p>Yes</p>

Feedback Form 24: Question KI#4.5: When the operator restricts the number of simultaneously active User Identifiers per UE or 5G-RG, should it be possible for the UE or 5G-RG to send traffic from non-3GPP devices that are not associated with a user identifier?

<p>1 – CableLabs</p> <p>Yes (e.g., via Rel-18 NAUN3 feature) if restriction is supported. One of feature of Rel-18 WWC is to support NAUN3 device. If a non-3GPP device is not identified and is not supported by KI#4 solution due to restriction or capability, we believe traffic from such device can be supported via Rel-18 NAUN3 feature.</p>
<p>2 – Ericsson LM</p> <p>Yes, some default treatment should be possible</p>

3 – InterDigital

Yes. It is already possible today for a non-3GPP device to send and receive data via an RG without a user identity.

4 – vivo Mobile Communication Co.

yes

5 – LG Electronics France

Yes. Restriction should be applied only to non-3GPP devices associated with user identifier.

6 – Charter Communications

YES, it is necessary for the 5GC to be able to identify traffic from each individual non-3GPP device.

HOWEVER, the primary motivation of such identification is for us (as an operator) NOT to charge individual non-3gpp devices behind an 5G-RG but to be able to perform policy control for each non-3GPP device. As discussed during the formulation of the SID, examples use cases are as follows:

- provide a higher or lower priority treatment for an individual non-3GPP device based on the request of the 5G-RG subscriber/admin.
- allow parental control type services (e.g., limit access to internet for an individual non-3GPP device) based on the request of the 5G-RG subscriber/admin.

In our humble opinion, the text in parenthesis is misleading as it uses “i.e.”. The corresponding Key Issue in the TR has the following text, which uses “e.g.”.

“whether and how the 5GC identifies individual non-3GPP devices connecting behind a UE or 5G-RG. (e.g. in order to charge the individual non-3GPP devices),”

In addition, the operator only charges the 5G-RG subscriber but not the individual non-3GPP devices connecting behind the 5G-RG.

7 – Charter Communications

Please ignore our previous comment as it was intended as a reply for KI#4.1.

Here is our reply for the this question:

YES.

The ambition of the key issue should be to identify non-3GPP devices connecting behind the 5G-RG to be able to provide differentiated service by the 5G-RG subscriber when (s)he would like to.

8 – HUAWEI Technologies Japan K.K.

Yes, possible to send traffic from non-3GPP devices that are not associated with a user identifier, for those non-3GPP devices not to be controlled or be provided differentiated services by the operators, similar as right now, and no need to describe?

9 – China Mobile Com. Corporation Yes.
10 – Motorola Mobile Com Technology Yes
11 – Nokia Corporation As above in 4.4. Yes.
12 – Qualcomm Incorporated Yes, that’s already been supported in the existing UE.
13 – NEC Europe Ltd Yes, for backward compatibility.
14 – Nubia Technology Co. ZTE: Yes
15 – Samsung Electronics Czech Yes
16 – Guangdong OPPO Mobile Telecom. In our view, this is a business decision of the operator. And it depends on the motivation why the operator wants to restrict the number of simultaneously active User Identifiers per UE/5G-RG. When the restriction is enabled on UE/5G-RG, it should not allow non-3GPP devices that are not associated with a User Identifier to send traffic. Certainly, if the operator wants to allow UE/5G-RG to send traffic from non-3GPP devices that are not associated with a user identifier, they could choose not to enable the restriction.

Feedback Form 25: Question KI#4.6: Can the traffic from the non-3GPP devices share the same PDU Session? If no, is a different DNN/S-NSSAI combination used for each PDU Session?

<p>1 – CableLabs</p> <p>We support non-3GPP devices share a PDU session e.g., based on different QoS flows. We are open for separate PDU, however, scalability aspects should be considered (e..g, not favor creating separate/individual PDU session per each non-3GPP device).</p>
<p>2 – InterDigital</p> <p>Yes, traffic from different non-3GPP devices should be able to share a PDU Session. We should not require that the 5G-RG establish a separate PDU Session for each non-3GPP device.</p>
<p>3 – vivo Mobile Communication Co.</p> <p>yes, it is the same as in PIN, and share a PDU session may have benefit.</p>
<p>4 – LG Electronics France</p> <p>Yes. Operator should be able to control DNN, S-NSSAI of PDU Session used for each non-3GPP devices that is associated with a user identifier.</p>
<p>5 – Charter Communications</p> <p>YES</p>
<p>6 – HUAWEI Technologies Japan K.K.</p> <p>Yes, but the standard should allow the UE/5G-RG to create different PDU Sessions for some of the non-3GPP devices, though not all devices need that. Different DNN/Slice can be applied but not flexible and not realistic in per non-3GPP device granularity, better to extend URSP to support it. Devices that do not need to be recognized can share the same PDU Session, by reusing Rel-18 mechanism.</p>
<p>7 – Motorola Mobile Com Technology</p> <p>We cannot assume that the same PDU session will be always shared. 5G/RG can establish different PDU session (e.g. different DNN or slices) based on configuration information provisioned at 5G/RG.</p>
<p>8 – Nokia Corporation</p> <p>Both options should be possible to support different deployment options of the consumer markets and the enterprise communities.</p>
<p>9 – Qualcomm Incorporated</p> <p>No, it's hard to share PDU session when service differentiation is required.</p> <p>Yes, different DNN/S-NSSAI combination used for each PDU Session is the most feasible and simple approach.</p>
<p>10 – NEC Europe Ltd</p> <p>Yes</p>

11 – Nubia Technology Co.

ZTE: both options are possible

12 – Samsung Electronics Czech

The non-3GPP devices can share the same PDU session, only when the traffic is intended for the same DNN/S-NSSAI. If traffic is intended for different DNN/S-NSSAI then a new PDU session needs to be triggered by UE/5G-RG

13 – Guangdong OPPO Mobile Telecom.

Yes, as long as the required QoS for the non-3GPP device can be met by this PDU session. E.g. both of the two devices require only best-effort services.

14 – Philips International B.V.

<apologies for the late input> Agree with Huawei, Motorola and Samsung

Feedback Form 26: Question KI#4.7: Which principles can be selected or considered for key issue #4 conclusions? Also identify, if possible, which solution(s) the principles are taken from.

1 – CableLabs

We like to list some requirements:

- No impact on non-3GPP device (e.g., support legacy non-3GPP device) and non-3GPP access between non-3GPP device & RG (e.g., legacy WLAN)
- Backward compatibility/coexistence/fallback to Rel-18 features (e.g., coexistence with NAUN3 devices or fallback to NAUN3 in case restriction happens or Rel-19 feature cannot be applicable)
- No mandate of authentication of non-3GPP device by external or 5G system (i.e., should work with non-3GPP devices supporting only local authentication e.g., PSK)
- Device profile information (or device information) including QoS profile should be available in either/both on 5GC UDM as well as external AAA server when needed.
- NAT scenario of RG should be supported/considered
- Scalability should be supported/considered (solution should not restrict a number of supported devices due to its feature e.g., dedicated PDU session per device)

2 – Ericsson LM

- IPv6 prefixes, IPv4 port ranges, mac addresses are defined to be used for each device behind UE/5G-RG this is used to detect its traffic for differentiated QoS provisioning and for billing information
- The UE/5G-RG provides Pv6 prefixes, IPv4 port ranges, mac addresses which is the information that is triggering the QoS differentiation
- No impacts to VPLMN (at roaming)
- Existing services towards the PCF are re-used

3 – InterDigital

For the case where the case where UE or 5G-RG binds/associates the user identifier to a non-3GPP device without requiring authentication via the 5GC of the non-3GPP device, we think that the principles of section 6.34.3.3 are good. For the case where authentication via the 5GC of the user identifier is required, we think that the procedure of 6.34.3.3 needs to be enhanced. For example, it can be enhanced so that the NAS SM Request of step 4 can trigger an EAP authentication of the non-3GPP device (e.g. a procedure similar to Secondary Authorization / Authentication by a DN-AAA Server during PDU Session Establishment).

4 – vivo Mobile Communication Co.

introduce both device id and IP address identification of device behind the UE.

5 – LG Electronics France

Network provides policy to the UE that is used to identify non-3GPP devices. The UE determines PDU Session parameters for the identified non-3GPP device using the received policy and informs detected non-3GPP device identifier + assigned address information to the SMF. SMF informs PCF of received information to apply non-3GPP device specific QoS by retrieving Device Identity Profile from UDR. Sol#34 can be taken as baseline with addition of non-3GPP device authentication procedure.

6 – Charter Communications

Key principles from our perspective are as follows:

- No impact to the way that diverse types of non-3GPP devices (e.g., IoT devices, laptops, TVs, gaming, etc.) behind an RG/WLAN-AP currently are authenticated and gain connectivity. Otherwise, it will be a huge operational burden that cannot be deployed.
- Solutions proposing separate PDU session for each non-3GPP device is not realistic/preferred.
- RG subscriber (homeowner) is in full control of devices connected behind the RG, for example by viewing the devices connected behind the RG, by updating end-to-end QoS for each non-3GPP device. This can be done via a portal connected to 5GC via PCF and AF/NEF APIs as per the key issue description.
- 5GS enablement of identification and service differentiation for non-3GPP devices connecting behind the RG is the focus of the KI. Charging of individual non-3GPP devices is not necessary.

7 – Motorola Mobile Com Technology

The following are the key principles

- During association between the non-3GPP device and 5G-RG, non-3GPP device includes a user identifier that is used to identify the device
- 5G-RG (based on user profile information stored locally) includes user identifier in PDU session request. Network authenticates user ID and provisions policies according to a user profile associated to this user id

8 – Nokia Corporation

Solution 31, 32 can be considered. And the following principles shall be agreed:

- 5GS needs to identify the traffic and implement PCC Rules for the traffic that is identified with certain identity configured for the UE Subscription.
- Solutions should not have authentication of non-3GPP devices as a mandatory condition, for traffic identification corresponding to a non-3GPP device.

9 – Qualcomm Incorporated

The non-3GPP device identity and profile are stored in Device Authorization Server (DAS).

The authentication/authorization of non-3GPP device may happen only via the application layer interworking with Device Authorization Server (DAS). The impacts to the PDU sessions establishment procedure are not expected. The interaction between UE and DAS are out of scope of 3GPP.

The DAS may trigger the delivery of URSP rules to the associated UE/RG for the route selection of the traffic to/from the non-3GPP device.

The PIN ID specified in Traffic Descriptor of URSP can be used to indicate the DNN/S-NSSAI and other RSD parameters that the device is allowed to use.

The AF/DAS can request QoS via NEF/PCF with corresponding traffic filter for the service flow of the device.

Qualcomm solution S2-2404816 is our preference but was not handled in SA2 #162.

10 – NEC Europe Ltd

Principles in solution 33 for the restriction of the number of simultaneously active non-3gppdevice requirement.

11 – Guangdong OPPO Mobile Telecom.

The Device Identifier should be provided by the network, rather than sending by non-3GPP device itself.

5G-RG/UE determines the association of a non-3GPP device to a PDU session based on URSP evaluation.

3 Round 1 Summary from Rapporteur

3.1 Key Issue #1 – Round 1 Summary

Question KI#1.1 asked “It has already been concluded that the User Identifier format is an NAI. Can the User Identifier be operator assigned, third party assigned or should both options be possible?”

17 Companies responded. All companies indicated that both are possible. A few companies qualified their answer with comments (e.g. who assigns the identifier does not need to be identified).

Proposal: Proceed under the assumption that the User Identifier can be operator assigned or third party assigned.

Question KI#1.2 asked “Is the User Identity Profile managed by the operator, third party, or should both options be possible?”

11 companies seemed to be clear that both options should be possible. 3 companies seemed to be clear that the User Identity Profile should be operator managed.

Proposal: Proceed under the assumption that the User Identity Profile can be managed by an operator or by a third party.

Question KI#1.3 asked “Where is the User Identity Profile Stored?”

18 Companies responded. 14 companies indicated that the User Identity Profile should be stored in the UDR. 2 Companies indicated that the User Identity Profile should be stored outside of the 5GC (i.e. UIP or an AF). 1 company was neutral. Another company indicated that it should not be stored in the UDR.

Proposal: Proceed under the assumption that the User Identity Profile is stored in the UDR.

Question KI#1.4 asked “There is an editor’s note in the conclusion that says that whether more than one User Identity can be in the User Identity Profile is FFS. Should it be possible for more than one User Identity to be in a User Identity Profile? If yes, then what is the use case?”

16 companies responded. 8 companies expressed a preference that there should only one user identity in the User Identity Profile. 6 companies expressed a preference that it should be possible for more than one user identity to be in the User Identity Profile. 2 companies were neutral or indicated that the question is out of scope.

Some of the companies that indicated a preference for only one user identity per User Identity Profile also indicated that they were open to listening to use cases, but generally prefer to keep things simple.

Proposal: Tentatively agree that only one user identity can be included in the user identity profile but allow companies to continue to discuss this. Discussions should focus on the use case and what complexities, if any, arise from allowing multiple user identities to be included in the user profile. Note that some responses to this question described supporting use cases, companies are encouraged to review these use cases and see if they are convinced.

Question KI#1.5 asked “It has already been concluded that a User Identity Profile includes a list of linked subscriptions. What other information, or parameters, should be stored in the User Identity Profile?”

16 companies responded.

12 companies respond that there should be QoS Information in the User Identity Profile.

At least 7 companies indicated that DNN/S-NSSAI combinations should be stored in the User Identity Profile.

At least 9 companies indicate that the User Identity Profile should include service information or service settings. Some companies specifically mentioned example of what service settings might be (e.g. SMS, MBS, V2X, and IMS were mentioned).

Proposals:

1. Proceed under the assumption that the User Identity Profile includes QoS Information.
2. Proceed under the assumption that the User Identity Profile includes DNN/S-NSSAI's that the user is allowed to access.
3. In round 2, ask more detailed question about what other service information should be included.

Question KI#1.6 asked "It has already been concluded that a User Identifier can be linked/unlinked with a subscription. What event(s), or request(s), trigger the User Identifier to be linked/unlinked?"

17 companies responded.

11 companies responded that the linking/unlinking can be triggered via NEF APIs.

8 companies responded that the linking/unlinking can be triggered via OAM.

2 companies indicated that linking/unlinking can happen whenever the user profile is created, updated, or deleted. However, how the user profile is created, updated, or deleted was not indicated.

2 companies indicated that linking/unlinking should happen in the application layer.

2 companies indicated that linking/unlinking can be triggered via NAS.

1 company was neutral.

1 company indicated that linking/unlinking should be via OAM but not via NEF APIs.

Proposals:

1. Proceed under the assumption that a trusted AF can use an NEF API to request that a user identifier be linked/unlinked with a subscription.
2. Proceed under the assumption that OAM procedures can be used to link/unlink a user identifier with a subscription.

Question KI#1.7 asked "In this release, when a user identifier is active with a subscription, should PCC Rules be adjusted?"

17 companies responded.

At least 16 responses seem to indicate that PCC rules should be adjusted.

2 responses indicate that the adjustment would be triggered by an AF request to change QoS.

9 responses seem to imply that the PCF obtains information from the user identity profile and uses that information to adjust PCC Rules.

Proposals:

1. Proceed under the assumption that PCC Rules are adjusted/updated when a user becomes active with a subscription.
2. In round two, ask more detailed questions about how the PCC Rules are updated (e.g. based on an AF request or based on the PCF reading from the user profile).

Question KI#1.8 asked “When a user is active with a subscription, is information from the user profile used to determine how to influence QoS for the UE’s PDU Session(s)?”

16 companies responded and responses were generally the same as question 1.7.

It seems that this question was interpreted as being the same as the last question. I apologize ☐. In round two I will ask a more detailed question. My intention with this question was to clarify if the PCF receives information from the user profile to adjust PCC Rules, or if PCC Rules are adjusted via an AF request.

Question KI#1.9 asked “In this release, when a user identifier is active with a subscription, should SMS over NAS be disabled or should it be possible to use SMS over NAS?”

16 companies responded.

9 companies seem to indicate that it is ok to use SMS when the user is active with the subscription.

At least one company suggests that SMS can be disabled when the user is active with the subscription.

At least two companies suggest that whether SMS is disabled can be based on configuration (e.g. information in the user profile).

Proposals:

1. Proceed under the assumption that SMS can be used when a user identifier is active with a subscription.
2. In round two, ask more detailed questions about how the SMS service is impacted, if at all, when a user identifier is active with a subscription (e.g. is the service adjusted for the user?).

Question KI#1.10 asked “In this release, when a user identifier is active with a subscription, should it be possible to use the IMS service?”

14 companies responded.

9 companies seem to indicate that it is ok to use IMS when the user is active with the subscription.

At least one company suggests that IMS can be disabled when the user is active with the subscription.

At least two companies suggest that whether IMS is disabled can be based on configuration (e.g. information in the user profile).

Proposals:

1. Proceed under the assumption that IMS can be used when a user identifier is active with a subscription.
2. In round two, ask more detailed questions about how the IMS service is impacted, if at all, when a user identifier is active with a subscription (e.g. is the service adjusted for the user?).

Question KI#1.11 asked “How does a linked user become active with a subscription?”

15 companies responded.

12 companies indicated that the user identifier is provided in NAS signalling. 3 of these companies expressed a clear preference for the user identifier being provided during PDU Session Establishment. 4 of these companies expressed a preference for the user identifier being provided during registration.

2 companies indicated that an application layer procedure may be used.

Proposals:

1. Proceed under the assumption that a linked user becomes active with a subscription by providing a user identifier in a NAS message.
2. In round two, ask more detailed questions about what NAS message should be used to provide the user identifier.

Question KI#1.12 asked “Which principles can be selected or considered for key issue #1 conclusions? Also identify, if possible, which solution(s) the principles are taken from.”

9 companies responded. The answers were very detailed and consistent with answers to earlier questions.

3.2 Key Issue #2 – Round 1 Summary

Question KI#2.1 asked “When the user is authenticated, authentication is performed between the UE and what entity?”

15 companies responded.

10 companies indicated AAA Server.

3 companies indicated AAA Server or UDM/AUSF

Two companies indicated application layer signalling with an AF, UIP Server, or AAA Server.

Proposals:

1. Proceed under the assumption that authentication is performed between the UE and a AAA Server.

Question KI#2.2 asked “Should interaction between the UE and entity (i.e. the entity from the previous question) be via NAS or user plane?”

15 companies responded.

11 companies indicated NAS. Multiple companies recommended using procedures that are similar to existing NAS-MM and/or NAS-SM procedures.

3 companies indicated user plane.

1 company indicated that they are neutral.

Proposals:

1. Proceed under the assumption that communication between the UE and AAA-S is via NAS.

Question KI#2.3 asked “What entity enforces the restriction that only one user shall be active with a UE’s subscription at a given time?”

14 companies responded.

10 companies indicated UDM. One of the 10 companies was also open to using the AMF.

2 companies indicated an AF (e.g. UIP or AF).

1 company indicated AMF.

Proposals:

1. Proceed under the assumption that the UDM enforces the restriction that only one user shall be active with a UE’s subscription at a given time.

Question KI#2.4 asked “Which principles can be selected or considered for key issue #2 conclusions? Also identify, if possible, which solution(s) the principles are taken from.”

12 companies responded. The answers were very detailed and consistent with answers to earlier questions.

3.3 Key Issue #3 – Round 1 Summary

Question KI#3.1 asked “How is user profile information and functionality exposed?”

<https://nwm-trial.etsi.org/#/documents/8871>

13 companies responded.

10 companies indicated NEF APIs.

2 Companies indicated APIs outside of the 5GC (e.g. CAPIF or Naf).

1 company indicated that they are neutral.

Proposals:

1. Proceed under the assumption that NEF APIs are used to expose user profile information.

Question KI#3.2 asked “What user profile information can be exposed? For each piece of information, please describe a use case. “

10 companies responded.

6 companies indicated that it should be possible to expose whether a user is active with a subscription.

5 companies indicated that authentication results should be exposed.

4 companies indicated that what subscriptions a user is linked to should be exposed.

Proposals:

1. In round 2, ask for company opinions on exposing authentication results, whether a user is active, and linked subscriptions.

Question KI#3.3 asked “Which principles can be selected or considered for key issue #3 conclusions? Also identify, if possible, which solution(s) the principles are taken from.”

9 companies responded. The answers were very detailed and consistent with answers to earlier questions.

3.4 Key Issue #4 – Round 1 Summary

Question KI#4.1 asked “Is it necessary for the 5GC to be able to identify traffic from each individual non-3GPP device (i.e. in scenarios where differentiation for charging is desired)?”

17 companies responded.

12 companies were clear that it is necessary for the 5GC to be able to identify traffic from each individual non-3GPP device.

1 company responded no.

There was some discussion about the need to discuss charging. As rapporteur, I would like to point out that the SID says:

- “The reason for utilizing operator user-specific identities in the 3GPP network is to allow the operator to charge and provide service differentiation based on the user identifier.”
- “Support for associating an identifier with traffic of a UE may enable charging and service differentiation by an RG’s home network operator for users whose non-3GPP device(s) connect to the 5GC via the RG.”
- “NOTE: Charging is in the remit of SA WG5.”.

Although charging is in the remit of SA5, in SA2 we need to be sure that the necessary information is available to be sent to a CHF. If we are going to charge a non-3GPP device, then the identity of the non-3GPP seems to be the minimum information that is needed.

Proposals:

1. Proceed under the assumption that “The 5GC needs to be able to identify traffic from each individual non-3GPP device.”
2. In round 2, ask if the individual devices will be identifier by user identifier or IP Address/MAC Address.

Question KI#4.2 asked “Is it necessary to specify a procedure to facilitate authentication via the 5GC of the user identifier associated with each individual non-3GPP device(s) connecting behind the UE or 5G-RG (i.e. to enable service differentiation and charging)?”

18 companies responded.

8 companies responded yes.

6 companies responded no.

2 companies responded that it can be left to SA3.

Proposals:

1. Proceed under the assumption that “Whether and how to authenticate/authorize a non-3GPP device is a SA WG3 decision.”

Question KI#4.3 asked “Is it necessary to specify a procedure where the UE or 5G-RG binds/associates the user identifier to a non-3GPP device without requiring authentication via the 5GC of the non-3GPP device (i.e. to enable service differentiation without charging)?”

10 companies responded.

6 companies responded yes.

2 companies responded no.

It is not clear that everyone has a common understanding of the question.

Proposals:

1. In round 2, ask, “Is it necessary to specify a procedure where the user identifier is bound to a non-3GPP device? If yes, who does the binding (e.g. the 5GC or 5G-RG/UE)? If yes, who is aware of the binding (e.g. the 5GC, 5G-RG/UE, or both?)”

Question KI#4.4 asked “In this release, should the operator be able to optionally restrict the number of simultaneously active User Identifiers per UE or 5G-RG?”

16 companies responded.

14 companies responded yes. However, 7 of those companies indicated that this feature is low priority.

2 companies responded no.

Proposals:

1. Proceed under the assumption that the operator is able to optionally restrict the number of simultaneously active User Identifiers per UE or 5G-RG. However, in terms of prioritizing meeting time, this will be low priority.

Question KI#4.5 asked “When the operator restricts the number of simultaneously active User Identifiers per UE or 5G-RG, should it be possible for the UE or 5G-RG to send traffic from non-3GPP devices that are not associated with a user identifier?”

15 companies responded.

All companies seem to be agreed that it is possible for the UE or 5G-RG to send traffic from non-3GPP devices that are not associated with a user identifier.

Proposals:

1. Proceed under the assumption that it is possible for the UE or 5G-RG to send traffic from non-3GPP devices that are not associated with a user identifier.

Question KI#4.6 asked “Can the traffic from the non-3GPP devices share the same PDU Session? If no, is a different DNN/S-NSSAI combination used for each PDU Session?”

14 companies responded.

13 companies seem to be agree that sharing a PDU Session should be possible.

Sending traffic to different PDU Sessions is already supported in the existing system and it is assumed that this will continue to be supported. At least 9 companies also indicated that using separate PDU Session should be possible.

1 company commented that it is hard to share a PDU Session when service differentiation is required and they prefer different DNN/S-NSSAI combinations.

Proposals:

1. Proceed under the assumption that, when their traffic is going to the same DNN/S-NSSAI combination, traffic from the non-3GPP devices share the same PDU Session.

Question KI#4.7 asked “Which principles can be selected or considered for key issue #4 conclusions? Also identify, if possible, which solution(s) the principles are taken from.”

11 companies responded. Responses were fairly diverse and consistent with other replies to the key issue #4 questions.

4 Round 2

4.1 Key Issue #1 – Round 2 Questions

4.1.1 User Identity Profile Management

Based on the round 1 discussion, it is proposed that that FS_UIA_ARC Key Issue #1 work proceeds under the following assumptions:

- The User Identifier can be operator assigned or third party assigned.
- The User Identity Profile can be managed by an operator or by a third party.
- The User Identity Profile is stored in the UDR.

Feedback Form 27: Question KI#1.13: Can NEF API's be used by a trusted AF (i.e. operator owned or 3rd party owned) to manage the User Identity Profile?

1 – Qualcomm Incorporated

Not sure about the question.

If the AF is in the trusted domain, NEF is not needed. AF can send request to NF directly via SBI.

Furthermore we don't agree with the assumptions stated above, for the fundamental reason that the activation/de-activation of the user profile in the device requires some UI interaction and security e.g. password, biometrics etc that can only be enabled by HLOS e.g. “switch user” in locked device menu. Considering that the part of the device is out of scope of 3GPP (“Terminal Equipment”) we don't see how the operator can assign and manage the User Identity Profile.

2 – NEC Europe Ltd Yes
3 – vivo Mobile Communication Co. it seems possible to handle this way.
4 – Guangdong OPPO Mobile Telecom. Yes, it should be possible.
5 – LG Electronics France Yes.
6 – Nokia Corporation Yes, a trusted AF can use the NEF APIs also. However, a third party owned is not a trusted AF. NEF shall be able to control the information and functions that could be exposed to untrusted AF.
7 – HUAWEI Technologies Japan K.K. Yes
8 – Deutsche Telekom AG yes
9 – Beijing Xiaomi Software Tech yes
10 – Motorola Mobile Com Technology Yes
11 – CATT Yes.
12 – InterDigital Yes
13 – Siemens AG The case Trusted AF owned by a third party is not clear, as in 3GPP third party refers to MNO for which the third party's AF is untrusted.

<p>14 – Samsung Electronics Czech</p> <p>Question seems unclear, if AF is in trusted domain, then NEF may not be required. Thus Both Trusted AF and Untrusted AF can be possible. In case Untrusted AF, NEF will authorize before accepting the request. This is as per the existing existing procedures</p>
<p>15 – Ericsson LM</p> <p>No, the UIP is stored in an AF and thus no need for NEF APIs to manage the UIP</p>
<p>16 – Apple Benelux B.V.</p> <p>If the scenario is about User Identity profile stored in UDRs, then such management by an AF may be required. But here it is critical to define that there should be only one AF per MNO that is authorised to do it.</p>
<p>17 – Nubia Technology Co.</p> <p>ZTE: Yes. In the parameter provisioning procedure in 23.502 clause , all the NF (trusted/un-trusted) use the NEF API</p>

Feedback Form 28: Question KI#1.14: Does managing a user profile include creating, modifying, and deleting a user profile?

<p>1 – Qualcomm Incorporated</p> <p>No. See above QC comments.</p>
<p>2 – NEC Europe Ltd</p> <p>Yes</p>
<p>3 – Beijing Xiaomi Software Tech</p> <p>yes</p>
<p>4 – Guangdong OPPO Mobile Telecom.</p> <p>Managing a user profile should include CRUD operations, i.e. create, read, update and delete.</p>
<p>5 – LG Electronics France</p> <p>Yes.</p>

<p>6 – Nokia Corporation</p> <p>Yes. A trusted AF can create User Identity Profile.</p> <p>All the mapped AFs (based on the properties set for the User Identity Profile and consent captured of the linked UE Subscription) can carry out modifying (changes and linking/unlinking) and deletion of the user identity profile.</p>
<p>7 – Nokia Corporation</p> <p>Yes. A trusted AF can create User Identity Profile.</p> <p>All the mapped AFs (based on the properties set for the User Identity Profile and consent captured of the linked UE Subscription) can carry out modifying (changes and linking/unlinking) and deletion of the user identity profile.</p>
<p>8 – CATT</p> <p>Yes.</p>
<p>9 – HUAWEI Technologies Japan K.K.</p> <p>Yes</p>
<p>10 – Deutsche Telekom AG</p> <p>yes</p>
<p>11 – Beijing Xiaomi Software Tech</p> <p>yes</p>
<p>12 – Motorola Mobile Com Technology</p> <p>Yes, all 3 procedures are possible.</p>
<p>13 – InterDigital</p> <p>Yes</p>
<p>14 – Samsung Electronics Czech</p> <p>Yes</p>
<p>15 – Ericsson LM</p> <p>Yes, but see answer to question 27</p>
<p>16 – Apple Benelux B.V.</p> <p>Yes, we may also want to include reading from a user profile as part of this management service</p>

17 – Nubia Technology Co.

ZTE: Yes. It may also contain Query/Subscribe(for Event notification)

Feedback Form 29: Question KI#1.15: In the operator managed scenario, can OAM procedure be used to manage the User Identity Profile?

1 – Qualcomm Incorporated

No.

See above QC comments.

2 – NEC Europe Ltd

Yes

3 – Guangdong OPPO Mobile Telecom.

Yes

4 – LG Electronics France

Whether OAM procedure can be used is not in the scope of SA2.

5 – Nokia Corporation

Yes

6 – CATT

Not sure. Need confirmation from SA5.

7 – HUAWEI Technologies Japan K.K.

Yes

8 – Deutsche Telekom AG

yes

9 – Beijing Xiaomi Software Tech

need confirmation with SA5

10 – Motorola Mobile Com Technology Yes, but it is left to the implementation and network deployment, i.e. out of scope of SA2.
11 – InterDigital Yes, SA2 can conclude this and ask SA5 to do any necessary work.
12 – Samsung Electronics Czech Yes
13 – Ericsson LM An E2E solution that works need to be described before making such conclusion, but if there is an operator managed UIP then ok.
14 – Apple Benelux B.V. Yes, that is possible
15 – Nubia Technology Co. ZTE: Yes, this option is possible.

4.1.2 User Identity Profile Contents

Based on the round 1 discussion, it is proposed that that FS_UIA_ARC Key Issue #1 work proceeds under the following assumptions:

- The User Identity Profile includes QoS Information.
- The User Identity Profile includes DNN/S-NSSAI's that the user is allowed to access.

The following question are about what else might be stored in the User Identity Profile and these questions are based on the round 1 questions.

Feedback Form 30: Question KI#1.16: Is the QoS Information in the User Identity Profile stored per DNN/S-NSSAI?

1 – Qualcomm Incorporated No, a default set of QoS information can be applied for all DNN/S-NSSAI.
--

2 – NEC Europe Ltd Yes
3 – vivo Mobile Communication Co. doesn't know the question clearly, QoS setting can be different according to user id, of course that the user ID can be limit used in DNN+s-NSSAI, but this is the limitation of user id in DNN, not the QoS limitation in DNN. We have already have the QoS related to DNN+S-NSSAI.
4 – Guangdong OPPO Mobile Telecom. No. The QoS information in the UIP should be stored per User ID (or User Identity which is identified by User ID).
5 – LG Electronics France Yes.
6 – Nokia Corporation Not required.
7 – CATT Needs further discussion.
8 – HUAWEI Technologies Japan K.K. Yes
9 – Deutsche Telekom AG No
10 – Beijing Xiaomi Software Tech no, user preferred Policy information can include the information (DNN/S-NSSAI) . but QoS information per DNN/S-NSSAI, makes things more complicated
11 – Motorola Mobile Com Technology The QoS information can be per UE level (UE-AMBR) , per PDU session level (per DNN/S-NSSAI combination)
12 – InterDigital Yes, similar to the "5GS Subscribed QoS profile" in TS 23.502, clause 5.2.3.3.1.

13 – Siemens AG It's not necessary to restrict QoS information to be stored per DNN/S-NSSAI in the User Identity Profile.
14 – Samsung Electronics Czech Yes, Also if the particular QoS information about DNN/S-NSSAI is not stored in the UIP, normal QoS as per UE's subscription will be used. Additionally it should not be mandatory for UIP to have DNN & S-NSSAI because UE should be allowed to use any DNN and S-NSSAI part of the subscription.
15 – Ericsson LM Depends on the E2E solution
16 – Apple Benelux B.V. No. Not sure if user identifiers need to have visibility over slices?
17 – Nubia Technology Co. ZTE: Yes, it can be (optional). It also can be applied to all or some DNNs/S-NSSAIs

Feedback Form 31: Question KI#1.17: Is the QoS Information QoS Flow level QoS parameter values (5QI and ARP)?

1 – Qualcomm Incorporated Yes.
2 – vivo Mobile Communication Co. yes
3 – China Mobile Com. Corporation yes
4 – Guangdong OPPO Mobile Telecom. Yes
5 – LG Electronics France Yes.
6 – Nokia Corporation Yes. An MNO shall have a limited set of templates for QoS information that can be chosen when the User Identity Profile is created or modified.

7 – CATT Needs further discussion. Other QoS parameters (e.g. GFBR, MFBR) may also be contained in the QoS information for the User Identity Profile.
8 – HUAWEI Technologies Japan K.K. Yes
9 – Deutsche Telekom AG yes
10 – Beijing Xiaomi Software Tech possible, but need further discussion
11 – Motorola Mobile Com Technology The QoS information may include one or more policies defined for PDU Session related policy information in Table 6.4-1 of 3GPP TS 23.503. For example, it may include: Authorised Session-MBR, Authorised Default 5QI/ARP
12 – InterDigital yes
13 – Samsung Electronics Czech Yes
14 – Ericsson LM Ok, but we don't see the need to restrict to only these as all QoS parameters can be updated using existing NEF/PCF services from an AF
15 – Apple Benelux B.V. yes
16 – Nubia Technology Co. ZTE: Possible

Feedback Form 32: Question KI#1.18: Can information about IMS settings be stored in the User Identity Profile?

1 – Qualcomm Incorporated

No.

In this release, we prefer no impact to IMS from User Identity.

2 – vivo Mobile Communication Co.

no, we prefer that no impact to IMS because the requirement is not clear and time limit in R19.

3 – China Mobile Com. Corporation

No.

4 – Guangdong OPPO Mobile Telecom.

Yes, per the definitions of User Identity and UIP.

5 – LG Electronics France

In order to support IMS based on MSISDN associated with User Identifier, UE need to have credentials for the MSISDN of User Identifier. However, there is no solution that enables IMS service when a User Identifier is activated. Therefore, IMS service based on UE subscription should be disabled.

6 – Nokia Corporation

We do not expect to bring in any new changes for the IMS configurations/settings.

Additional IMPUs based on the implementations can be configured in the HSS imsServiceProfile for the Subscription.

Any relation between multiple UE Subscriptions to an IMPU of a User Identity or the corresponding service configurations and flows, if required needs to be studied in future releases.

7 – CATT

No. To support IMS setting per user identity, probably enhancements to (/interactions with) IMS subsystem are needed, which is not in the scope of Rel-19.

8 – HUAWEI Technologies Japan K.K.

It is not clear what IMS settings are under the discussion. If this is about supporting IMS service for the User Identity, we would propose to defer the discussion to next release, due to time restriction, i.e. no support of IMS service for the User Identity in this release.

9 – Deutsche Telekom AG yes, it should not be excluded to realize some of the stage 1 requirements in Rel19
10 – Beijing Xiaomi Software Tech not preferred, only impact on the PDU session that is used for IMS service.
11 – Motorola Mobile Com Technology Propose to work on this topic in a future release
12 – InterDigital We also prefer to work on this in a future release.
13 – Samsung Electronics Czech No
14 – Ericsson LM Cannot progress work without a complete description. However, with an appropriate IMPU used for IMS registration then an IMS service Profile is selected
15 – Apple Benelux B.V. No
16 – Nubia Technology Co. ZTE: No, because it is unclear what is the “information about IMS settings”. (The simple way may be, in the User ID profile, there is a setting about whether the User ID is “allowed”, or “not allowed” to use the IMS service corresponding to the subscription)

Feedback Form 33: Question KI#1.19: Can information about SMS settings be stored in the User Identity Profile?

1 – Qualcomm Incorporated No. In this release, we prefer no impact to SMS from User Identity.
2 – vivo Mobile Communication Co. no, we prefer that no impact to SMS because the requirement is not clear and time limit in R19.
3 – China Mobile Com. Corporation No, the same rule as IMS

<p>4 – Guangdong OPPO Mobile Telecom.</p> <p>Yes, per the definitions of User Identity and UIP.</p>
<p>5 – LG Electronics France</p> <p>Yes. User Identity Profile stores whether SMS service is allowed and MSISDN associated with the User Identifier.</p>
<p>6 – Nokia Corporation</p> <p>As part of the User Identity Profile, additional GPSI can be attached to the User Identifier.</p>
<p>7 – CATT</p> <p>No. The requirement of provisioning SMS per user is unclear.</p>
<p>8 – HUAWEI Technologies Japan K.K.</p> <p>- See the answer to the question in KI#1.18 for IMS.</p>
<p>9 – Deutsche Telekom AG</p> <p>Yes, that might be the limited IMS impact (as we know that SA1 had only SMS over IMS in mind at the time of creating the requirements)</p>
<p>10 – Beijing Xiaomi Software Tech</p> <p>no, prefer SMS/IMS not in this release</p>
<p>11 – Motorola Mobile Com Technology</p> <p>Propose to work on this topic in a future release</p>
<p>12 – InterDigital</p> <p>We also prefer to work on this in a future release.</p>
<p>13 – Samsung Electronics Czech</p> <p>No</p>
<p>14 – Ericsson LM</p> <p>Cannot progress work without a complete description, and we need to discuss what are these SMS settings as such. However, it is not a good idea to disable SMS as such.</p>

15 – Apple Benelux B.V.

No

16 – Nubia Technology Co.

ZTE: No, because it is unclear what is the “information about SMS settings”. (Another way could be, in the User ID profile, there is a setting about whether the User ID is “allowed”, or “not allowed” to use the SMS service corresponding to the subscription.)

Feedback Form 34: Question KI#1.20: Can information about service chain settings be stored in the User Identity Profile?

1 – Qualcomm Incorporated

No. Service chain can be triggered by AF influence.

2 – vivo Mobile Communication Co.

No such requirements, prefer not.

3 – China Mobile Com. Corporation

No such requirements, prefer not.

4 – Guangdong OPPO Mobile Telecom.

This does not seem to be in the scope.

5 – LG Electronics France

No.

6 – Nokia Corporation

No additional settings shall be required. However, the services that are allowed for a User Identifier access shall be made available in the User Identity Profile.

7 – CATT

Maybe, similar to “AF traffic influence request information for service function chaining” in the Application Data in UDR.

8 – HUAWEI Technologies Japan K.K. See the answer to the question in KI#1.18 for IMS.
9 – Deutsche Telekom AG Yes, the changes needed for that seem to be limited.
10 – Beijing Xiaomi Software Tech No such requirements, prefer not.
11 – Motorola Mobile Com Technology Yes
12 – InterDigital We think that this can be achieved in Rel-19.
13 – Samsung Electronics Czech No
14 – Ericsson LM yes, but as UIP is in the AF, the AF can influence the service chain using the existing NEF/PCF services
15 – Apple Benelux B.V. No
16 – Nubia Technology Co. ZTE: No, in this release. There is no solution on this issue in the TR phase

Feedback Form 35: Question KI#1.21: Can information about other services (e.g. MBS, V2X) be stored in the User Identity Profile?

1 – Qualcomm Incorporated No.
2 – NEC Europe Ltd Yes. The User Profile may contain services allowed/allowed/restricted per User.

<p>3 – vivo Mobile Communication Co.</p> <p>No, prefer only linked to URSP is enough.</p>
<p>4 – China Mobile Com. Corporation</p> <p>No</p>
<p>5 – Guangdong OPPO Mobile Telecom.</p> <p>We do not think this is in the scope either. A response of yes or no will both open lots of possibilities which we can not complete in this release.</p>
<p>6 – LG Electronics France</p> <p>Yes.</p>
<p>7 – Nokia Corporation</p> <p>No additional settings shall be required. However, the services that are allowed for a User Identifier access shall be made available in the User Identity Profile.</p>
<p>8 – Nokia Corporation</p> <p>It is not required. We do not have such capability check even for the UEs.</p> <p>But such an information can be provisioned into the User Identity Profile, if a valid use case is brought in and shall be of less priority.</p>
<p>9 – CATT</p> <p>Maybe, similar to what are indicated in the subscription data in UDR.</p>
<p>10 – HUAWEI Technologies Japan K.K.</p> <p>See the answer to the question in KI#1.18 for IMS.</p>
<p>11 – Deutsche Telekom AG</p> <p>Yes for what is required by SA1, no for the rest (e.g. V2X, MBS).</p>
<p>12 – Beijing Xiaomi Software Tech</p> <p>prefer not</p>
<p>13 – Motorola Mobile Com Technology</p> <p>Yes, but only support whether the service is disabled for a user. The User profile may also include information whether there is a user consent for LCS services</p>

14 – InterDigital We prefer not in this release
15 – Samsung Electronics Czech No
16 – Ericsson LM cannot progress work without a complete description
17 – Apple Benelux B.V. No
18 – Nubia Technology Co. ZTE: No, in this release

Feedback Form 36: Question KI#1.22: Can the PEI's of devices that the user is allowed to use be stored in the User Identity Profile?

1 – Qualcomm Incorporated No.
2 – vivo Mobile Communication Co. No,
3 – China Mobile Com. Corporation No
4 – Guangdong OPPO Mobile Telecom. No
5 – LG Electronics France Yes.
6 – Nokia Corporation It is not required. We do not have such capability check even for the UEs. But such an information can be provisioned into the User Identity Profile, if a valid use case is brought in and shall be of less priority.

7 – CATT No.
8 – HUAWEI Technologies Japan K.K. Open. The PEI can be retrieved from the UDM for the SUPI linked with the User Identity, so it may not need to be stored in the User Identity Profile.
9 – Deutsche Telekom AG Maybe something that can be looked at in a later release...
10 – Beijing Xiaomi Software Tech yes,
11 – Motorola Mobile Com Technology yes usefull for Key Issue 4 solutions
12 – InterDigital We do not think that this is needed
13 – Samsung Electronics Czech No, (atleast clearly not for the Human User case)
14 – Ericsson LM what is the use case?
15 – Apple Benelux B.V. No. In our understanding, there is no requirement associated with this.
16 – Nubia Technology Co. ZTE: No

Feedback Form 37: Question KI#1.23: Can user specific AMF policies be stored in the User Identity Profile?

1 – Qualcomm Incorporated No.

<p>2 – vivo Mobile Communication Co.</p> <p>No. SM policy and UE policy are enough and seen have value</p>
<p>3 – China Mobile Com. Corporation</p> <p>No</p>
<p>4 – Guangdong OPPO Mobile Telecom.</p> <p>No, we do not see the need to store user specific AMF policies in the UIP based on architecture requirements.</p>
<p>5 – LG Electronics France</p> <p>No.</p>
<p>6 – Nokia Corporation</p> <p>The subset parameters of the linked UE Subscription can be attached to the User Identity Profile and the same may be used for policy decisions during the AM policy association / modification.</p>
<p>7 – HUAWEI Technologies Japan K.K.</p> <p>No, first not clear what the AMF policies are in the context, secondly policy is not part of User Identity Profile.</p>
<p>8 – CATT</p> <p>No.</p>
<p>9 – Deutsche Telekom AG</p> <p>No.</p>
<p>10 – Beijing Xiaomi Software Tech</p> <p>no</p>
<p>11 – Motorola Mobile Com Technology</p> <p>Yes (e.g. UE-AMBR)</p>
<p>12 – InterDigital</p> <p>We prefer not in this release.</p>
<p>13 – Samsung Electronics Czech</p> <p>More clarification on what kind of AM policies are being referred.</p>

<p>14 – Ericsson LM</p> <p>for what usage and where are the requirements? Existing NEF/PCF service can be used to update AM policies by a trusted AF.</p>
<p>15 – Apple Benelux B.V.</p> <p>As Ericsson’s comments indicate, not clear what is the use case?</p>
<p>16 – Nubia Technology Co.</p> <p>ZTE: No</p>

Feedback Form 38: Question KI#1.24: Can user credentials be stored in the User Identity Profile?

<p>1 – Qualcomm Incorporated</p> <p>No.</p>
<p>2 – NEC Europe Ltd</p> <p>Yes. The User Profile may contain an attribute indicating whether user specific authentication is required. The User Profile may also contain the the AAA Server address and potentially the authentication algorithm/credentials.</p>
<p>3 – Guangdong OPPO Mobile Telecom.</p> <p>This should be in the remit of SA3.</p>
<p>4 – LG Electronics France</p> <p>If authentication is done by DN-AAA, no need to store credentials in the User Identity Profile.</p>
<p>5 – LG Electronics France</p> <p>If authentication is done by DN-AAA, no need to store credentials in the User Identity Profile.</p>
<p>6 – Nokia Corporation</p> <p>We expect that the entity that is Authorizing the User Identifier shall store the user credentials. If AUSF/UDM is authenticating, then it shall (in the ARPF and is defined by SA3), else if it is the AAA Server then the AUSF through the NSSAAF shall receive the authentication results from the AAA Server.</p>

<p>7 – HUAWEI Technologies Japan K.K.</p> <p>Yes, similar as what’s defined for SUPI.</p>
<p>8 – CATT</p> <p>Yes.</p>
<p>9 – Beijing Xiaomi Software Tech</p> <p>yes</p>
<p>10 – Motorola Mobile Com Technology</p> <p>If the question is whether the user profile include authorisation credentials in the user profile then the answer is no.</p> <p>If the question is the whether the user profile includes configuration information on where user credential provided by the UE are authenticated (e.g. AAA server address) then the answer is yes.</p>
<p>11 – InterDigital</p> <p>Yes, SA2 can suggest this to SA3</p>
<p>12 – Samsung Electronics Czech</p> <p>Maybe</p>
<p>13 – Ericsson LM</p> <p>seems more SA3 issue, but if we later conclude authentication is between UE and AAA-S why are the credentials stored in the UIP?</p>
<p>14 – Apple Benelux B.V.</p> <p>This has to come from SA3 work conclusions</p>
<p>15 – Nubia Technology Co.</p> <p>ZTE: Yes. It can (optional) and SA3 input is needed</p>

4.1.3 User Identity Influence on QoS

Based on the round 1 discussion, it is proposed that that FS_UIA_ARC Key Issue #1 work proceeds under the following assumptions:

- PCC Rules are adjusted/updated when a user a becomes active with a subscription.

Feedback Form 39: Question KI#1.25: Are the PCC Rules updated based on information that the PCF receives from the User Identity Profile?

<p>1 – Qualcomm Incorporated</p> <p>No.</p> <p>The AF, is responsible to request appropriate QoS when the corresponding User Identity Profile is enabled.</p>
<p>2 – NEC Europe Ltd</p> <p>Yes</p>
<p>3 – vivo Mobile Communication Co.</p> <p>yes</p>
<p>4 – China Mobile Com. Corporation</p> <p>Yes</p>
<p>5 – Guangdong OPPO Mobile Telecom.</p> <p>Yes, it should be possible.</p>
<p>6 – LG Electronics France</p> <p>Yes.</p>
<p>7 – Nokia Corporation</p> <p>The PCF considers the subset of rules that are provisioned to the User Identifier of a specific linked UE Subscription and PCF shall consider the PCC rules that are derived from the combination of UE Subscription and User Identity Profile.</p>
<p>8 – HUAWEI Technologies Japan K.K.</p> <p>Yes</p>
<p>9 – CATT</p> <p>Yes</p>
<p>10 – Deutsche Telekom AG</p> <p>PCC Rules are adjusted/updated when a user a becomes active with a subscription considering additionally User Profile Information.</p>

11 – Beijing Xiaomi Software Tech yes
12 – Motorola Mobile Com Technology Yes
13 – InterDigital yes
14 – Samsung Electronics Czech yes
15 – Ericsson LM No, PCF does not receive info from UIP as such. Unclear question, but AF can use existing PCF services or NEF services with, new info e.g. UID to be sent to CHF by SMF, to influence PCF in creating PCC rules
16 – Apple Benelux B.V. Yes
17 – Nubia Technology Co. ZTE: Yes

Feedback Form 40: Question KI#1.26: Are the PCC Rules updated based on invocation of existing PCF/NEF API (e.g., Npcf_PolicyAuthorization_Create)?

1 – Qualcomm Incorporated Possibly yes. Depending on authorization.
2 – Guangdong OPPO Mobile Telecom. Yes, it could be, but not necessarily the Npcf_PolicyAuthorization_Create service operation.
3 – LG Electronics France Yes. PCF can take into account both User Identity Profile and AF input to update PCC Rules.
4 – Nokia Corporation Yes.

<p>We do not expect change in the architecture.</p>
<p>5 – HUAWEI Technologies Japan K.K.</p> <p>The PCC rule can be updated either by OAM or by the request from AF with authorization by the PCF/operator. For both cases, the request is per user id, not based on the IP description.</p>
<p>6 – CATT</p> <p>Yes</p>
<p>7 – Deutsche Telekom AG</p> <p>Yes.</p> <p>We do not expect change in the architecture.</p>
<p>8 – Motorola Mobile Com Technology</p> <p>The user profile information is provided once and stored in the UDR (e.g. the user profile may reference a specific PDU session related policy). The PCF retrieves the user profile associated with the identified user and applies the QoS policy.</p>
<p>9 – InterDigital</p> <p>Yes, in the sense that it is already possible for an AF to use the API to configure QoS for a flow. However, it should not be relied on for adjusting QoS when a user becomes active. The QoS should be based on the contents of the user profile. An authorized AF is always allowed to request changes.</p>
<p>10 – Samsung Electronics Czech</p> <p>Yes</p>
<p>11 – Ericsson LM</p> <p>Yes</p>
<p>12 – Apple Benelux B.V.</p> <p>Yes</p>
<p>13 – Nubia Technology Co.</p> <p>ZTE: Yes, depend on the existing PCF/NEF/UDR API. Npcf_PolicyAuthorization is one of them.</p>

4.1.4 Linking

Based on the round 1 discussion, it is proposed that that FS_UIA_ARC Key Issue #1 work proceeds under the following assumptions:

- A trusted AF can use an NEF API to request that a user identifier be linked/unlinked with a subscription.
- OAM procedures can be used to link/unlink a user identifier with a subscription.

Feedback Form 41: Question KI#1.27: For each user identity, is there only one, or more than one, AF that is authorized to request that the user be linked to a subscription?

1 – Qualcomm Incorporated

We disagree with the assumptions. The linking/unlinking of the user identity profile can only happen in HLOS because this is where the UI that the user interacts with. In this respect the AF only knows which user identity profile is in use.

2 – Guangdong OPPO Mobile Telecom.

We think for each user identity, there should be *only one* AF that is authorized to request that the user be linked to a subscription.

3 – LG Electronics France

Only one AF for each user identity.

4 – Nokia Corporation

The User Identity Profile may have the AFs that can manage the User Identity Profile (for example, linked to different UE Subscriptions); Accordingly, the corresponding AF shall be able to

- Link - Any trusted AF
- Unlinking - Corresponding linked AF
- Manage (Update / delete of User Identity Profile Information) – The AF that created the User / OAM

5 – HUAWEI Technologies Japan K.K.

It is unclear what's the use case for the AF to request link between a user and a SUPI, even for the one AF case?

6 – CATT

More than one AF.

7 – CATT

Sorry, please ignore my previous answer. Only one AF.

8 – Beijing Xiaomi Software Tech it depends on the authorization, one or more authroized AF can make such request
9 – Motorola Mobile Com Technology Only one AF managed by the operator.
10 – InterDigital Only one seems sufficient and we do not see a need to make it more complicated than that.
11 – Samsung Electronics Czech Yes, only 1 AF should control; If linking is performed by the AF, then linking and activation should be one-step process
12 – Ericsson LM The AF managing the UIP stored in the AF is authorized to update User Links, i.e. there is only one AF
13 – Apple Benelux B.V. only one AF
14 – Nubia Technology Co. ZTE: For each user identity, one AF is better/simpler

Feedback Form 42: Question KI#1.28: For each subscription, is there only one, or more than one, AF that is authorized to request that a user be linked to the subscription?

1 – Qualcomm Incorporated Yes.
2 – Guangdong OPPO Mobile Telecom. Wt think, for each subscription, there should be only one AF that is authorized to request that a user be linked to the subscription.
3 – LG Electronics France Only one AF for each user identity.

<p>4 – Nokia Corporation</p> <p>A UE Subscription may consent the AFs that can manage the linking process. So, only those AFs that are allowed based on the consent shall be allowed to link a User Identity Profile to the UE Subscription. (For eg the UE subscription may want the subscription should be able to be linked by Corporate AF, but not by any of the other AFs).</p>
<p>5 – HUAWEI Technologies Japan K.K.</p> <p>Same answer as for Question KI#1.27</p>
<p>6 – CATT</p> <p>More than one AF.</p>
<p>7 – Beijing Xiaomi Software Tech</p> <p>only the owner AF of the user identity profile. for each subscription, more owner AFs can link to one subscription</p>
<p>8 – Motorola Mobile Com Technology</p> <p>only one AF managed by the operator</p>
<p>9 – InterDigital</p> <p>Only one seems sufficient and we do not see a need to make it more complicated than that.</p>
<p>10 – Ericsson LM</p> <p>Would be good to get the use case for using more than one AF, and why does it matter whether more than one AF is able to create User Links?</p>
<p>11 – Apple Benelux B.V.</p> <p>Restricting to only one AF is preferred</p>
<p>12 – Nubia Technology Co.</p> <p>ZTE: It can be more than one. In this release, can live with only one</p>

4.1.5 Activation

Based on the round 1 discussion, it is proposed that that FS_UIA_ARC Key Issue #1 work proceeds under the following assumptions:

- A linked user becomes active with a subscription by providing a user identifier in a NAS message.

Feedback Form 43: Question KI#1.29: Is the user identifier provided in an NAS-MM (e.g. registration) or a NAS-SM (e.g. PDU Session Establishment)? Which NAS message(s)?

<p>1 – Qualcomm Incorporated</p> <p>We prefer NAS is not impacted for indication of User identifier.</p> <p>NAS-SM (e.g. PDU Session Establishment), if NAS has to be used.</p>
<p>2 – NEC Europe Ltd</p> <p>NAS-MM. Registration Request.</p>
<p>3 – vivo Mobile Communication Co.</p> <p>We prefer not impact the NAS procedure. And if have to use, prefer session related. And, this must be optional feature supported by UE, not madatory. I am not ok to have this madatory feature.</p>
<p>4 – China Mobile Com. Corporation</p> <p>NAS-SM</p>
<p>5 – Guangdong OPPO Mobile Telecom.</p> <p>NAS-SM.</p>
<p>6 – LG Electronics France</p> <p>NAS-MM message.</p>
<p>7 – Nokia Corporation</p> <p>A single entity (UE Subscription or a User Identifier) is active after successful registration of SUPI and User identifier.</p> <p>A User Identifier may use Data services, SMS services, etc (as discussed in the discussions of NWM round 1 too). It would be inefficient with additional handling to have a User Identifier linked and be active in the network if we use the procedures like PDU Session procedures (multiple PDU Sessions and additional checks).</p> <p>Considering these, we prefer to have the Authentication and linking being done during the Registration procedure (NAS-MM) and rest of the services (NFs) are agnosticized of linking and authenticating.</p>
<p>8 – HUAWEI Technologies Japan K.K.</p> <p>Our preference is PDU session establishment, but open for other procedures.</p>

9 – CATT

Whether and what NAS message(s) are used need further discussion. NAS-SM messages seem not appropriate.

10 – Beijing Xiaomi Software Tech

we prefer NAS-MM procedure

11 – Motorola Mobile Com Technology

Our preference is to have the user id provided in NAS-SM. Each PDU session established by the UE includes a user id that is used by the corresponding SMF to retrieve the user profile. When the user changes the UE includes in a PDU session modification request the user id of the new user. The AMF can release any established PDU session that the new user is not allowed to use (e.g. DNN or S-NSSAI not allowed for new user)

12 – Deutsche Telekom AG

We prefer NAS is not impacted for indication of User identifier.
NAS-SM (e.g. PDU Session Establishment), if NAS has to be used.

13 – InterDigital

We prefer NAS-MM. This seems to make more sense the user is supposed to be associated with all of the UE's PDU Sessions.

14 – Samsung Electronics Czech

We think that both can be possible based on different use cases.

15 – Ericsson LM

Prefer UP to be used, but if NAS then NAS-SM with PDU Session Establishment using ePCO or EAP Response/Identity message

16 – Apple Benelux B.V.

Prefer NAS-MM procedure

17 – Nubia Technology Co.

ZTE: NAS-MM is better, e.g. Registration message or new NAS message. For the NAS-SM, it needs to clarify: 1) how to handle the existing PDU session; 2) whether the activation is encapsulated in the SM container, or both in the SM container and new IE out of SM container.

4.1.6 SMS

Based on the round 1 discussion, it is proposed that that FS_UIA_ARC Key Issue #1 work proceeds under the following assumptions:

- SMS can be used when a user identifier is active with a subscription.

Feedback Form 44: Question KI#1.30: When a user is active with a subscription, does delivery of the SMS service continue based only on information from the subscription? In other words, when the user becomes active, are SMS messages still delivered to the MSISDN in the subscription?

<p>1 – Qualcomm Incorporated</p> <p>Yes. SMS is based on UE subscription, no impact from activation of user identity.</p>
<p>2 – vivo Mobile Communication Co.</p> <p>current MSISDN procedure is not impact, prefer no impact to SMS after introducing user id.</p>
<p>3 – China Mobile Com. Corporation</p> <p>Yes. SMS is based on UE subscription</p>
<p>4 – Guangdong OPPO Mobile Telecom.</p> <p>We think this needs to be further studies in the next release, rather in Rel-19. There is no requirements in the SID about the delivery of the SMS service for the specific user.</p>
<p>5 – LG Electronics France</p> <p>A user can get SMS service by using MSISDN stored in the User Identity Profile, i.e., SMS service of UE subscription is disabled and SMS service of the active user is enabled.</p>
<p>6 – Nokia Corporation</p> <p>SMS shall be allowed to the GPSI that is associated with the User Identifier that is currently active. SMS shall not be delivered to the GPSI/MSISDN belonging to the UE Subscription as the UE is being used by User Identifier.</p>
<p>7 – HUAWEI Technologies Japan K.K.</p> <p>Open for discussion. Our preference is to prohibit the SMS service for the MSISDN corresponding to the SUPI for this release.</p>

8 – CATT Yes.
9 – Beijing Xiaomi Software Tech yes, new feature should not override the existing feature.
10 – Motorola Mobile Com Technology Yes
11 – Deutsche Telekom AG Yes, there is no stage 1 requirement to "override" the existing feature. Such service related question should be addressed to SA1 not SA2.
12 – InterDigital yes
13 – Samsung Electronics Czech Yes, still delivered to the MSISDN in the subscription
14 – Ericsson LM Yes, but they are not delivered to the UE in case "another" user is active associated to the SUPI. We tried to ask SA1 at the last meeting and we will again propose to ask SA1.
15 – Apple Benelux B.V. Yes
16 – Nubia Technology Co. ZTE: Yes. (also can see the answer to Q#1.19. It depends on whether the setting in the UIP is set to "allowed" or "not allowed" for SMS service.)

Feedback Form 45: Question KI#1.31: When a user is active with a subscription, does activation of the user impact the SMS service? If yes, then in what way is the SMS service impacted? Is an MSISDN that is associated with the User Identity Profile used instead?

1 – Qualcomm Incorporated No.
2 – vivo Mobile Communication Co.

No
3 – China Mobile Com. Corporation No
4 – Guangdong OPPO Mobile Telecom. No
5 – LG Electronics France A user can get SMS service by using MSISDN stored in the User Identity Profile, i.e., SMS service of UE subscription is disabled and SMS service of the active user is enabled.
6 – Nokia Corporation Yes. As described in answer to KI#1.30, SMS shall be allowed to the GPSI that is associated with the User Identifier that is currently active. SMS shall not be delivered to the GPSI/MSISDN belonging to the UE Subscription as the UE is being used by User Identifier.
7 – HUAWEI Technologies Japan K.K. Same answer as to Question KI#1.30
8 – CATT No.
9 – Beijing Xiaomi Software Tech no seems
10 – Motorola Mobile Com Technology The SMS service should not be impacted. Propose to leave this to the next release
11 – InterDigital No
12 – Samsung Electronics Czech No impact.
13 – Ericsson LM If UIP is associated to an IMS subscription and SMSoIP is subscribed, then yes. For SMS over NAS, not supported. However, in general need an E2E solution to be described.

14 – Apple Benelux B.V. No
15 – Deutsche Telekom AG Yes for SMSoIMS, no for SMS over NAS.
16 – Nubia Technology Co. ZTE: No impact is preferred.

4.1.7 IMS

Based on the round 1 discussion, it is proposed that that FS_UIA_ARC Key Issue #1 work proceed under the following assumptions:

- IMS can be used when a user identifier is active with a subscription.

Feedback Form 46: Question KI#1.32: When a user is active with a subscription, does delivery of the IMS service continue based only information from the subscription?

1 – Qualcomm Incorporated Yes.
2 – vivo Mobile Communication Co. Yes
3 – China Mobile Com. Corporation Yes
4 – Guangdong OPPO Mobile Telecom. We think this needs to be further studies in the next release, rather in Rel-19. There is no requirements in the SID about the delivery of the IMS service for the specific user.
5 – LG Electronics France In order to support IMS based on MSISDN associated with User Identifier, UE need to have credentials for the MSISDN of User Identifier. However, there is no solution that enables IMS service when a User Identifier is activated. Therefore, IMS service based on UE subscription should be disabled.

6 – Nokia Corporation Yes. Also refer to answer to KI#1.18
7 – HUAWEI Technologies Japan K.K. Same answer as to Question KI#1.30, KI#1.31, i.e. to prohibit IMS service for this release.
8 – CATT Yes.
9 – Motorola Mobile Com Technology Yes
10 – Deutsche Telekom AG yes
11 – InterDigital yes
12 – Samsung Electronics Czech Yes
13 – Ericsson LM No, but need to discuss the scenario e.g. if owner let other user use the UE then IMS services to the owner of the UE subscription probably need to be disabled.
14 – Apple Benelux B.V. Yes
15 – Nubia Technology Co. ZTE: Yes. (also can see the answer to Q#1.18. It depends on whether the setting in the UIP is set to “allowed” or “not allowed” for IMS service.)

Feedback Form 47: Question KI#1.33: When a user is active with a subscription, does activation of the user impact the IMS service? If yes, then in what way is the IMS service impacted? Is an IMPU that is associated with the User Identity Profile used instead?

1 – Qualcomm Incorporated No.
2 – vivo Mobile Communication Co. No
3 – China Mobile Com. Corporation No
4 – Guangdong OPPO Mobile Telecom. No
5 – LG Electronics France In order to support IMS based on MSISDN associated with User Identifier, UE need to have credentials for the MSISDN of User Identifier. However, there is no solution that enables IMS service when a User Identifier is activated. Therefore, IMS service based on UE subscription should be disabled.
6 – Nokia Corporation It is strongly recommended to not to impact IMS in the current release. In regard to the same, we could leave at deployment option that indicates that IMPU can be configured based on the User Identifier. Also refer to our answer to KI#1.18
7 – HUAWEI Technologies Japan K.K. Same answer as to Question KI#1.32
8 – CATT No.
9 – Motorola Mobile Com Technology Propose to study in a future release
10 – InterDigital No
11 – Samsung Electronics Czech No impact
12 – Ericsson LM We should not impact IMS. IMPU tied to the user is registered with the IMPI tied to the IMS subscription and associated with the UID should work.

13 – Apple Benelux B.V. No impact
14 – Nubia Technology Co. ZTE: No impact is preferred.

4.2 Key Issue #2 – Round 2 Questions

Based on the round 1 discussion, it is proposed that that FS_UIA_ARC Key Issue #2 work proceeds under the following assumptions:

- Authentication is performed between the UE and a AAA Server.
- Communication between the UE and AAA-S is via NAS.
- The UDM enforces the restriction that only one user shall be active with a UE’s subscription at a given time.

Feedback Form 48: Question KI#2.5: Is communication between the UE and AAA Server via NAS-MM or NAS-SM signaling?

1 – Qualcomm Incorporated We disagree with the assumptions. There is no need in our view for authentication between the UE (modem) and AAA Server in the form of secondary authentication. The reason is that the control of credentials that are associated with the user identity profile can only reside in HLOS, since it is only there that interaction with the user can happen. As long as the operator trusts the HLOS to perform authentication and user identity “tag” e.g. NAI can be provided to the network in NAS-SM (PCO). If the operator cannot trust the HLOS none of this can work because there are no means for the operator to interact directly with the user.
2 – NEC Europe Ltd NAS-MM. Similar to network slice specific authentication.
3 – LG Electronics France NAS-MM message.
4 – Nokia Corporation Re-use the principles described in 23.501 sections 5.30.2.9.2 and 23.502 sections 4.2.2.2.4. (Based on MM)

<p>5 – HUAWEI Technologies Japan K.K.</p> <p>Our preference is NAS-SM. But open with NAS-MM.</p>
<p>6 – CATT</p> <p>The messages to use between the UE and AAA Server are to be decided by SA3.</p>
<p>7 – Beijing Xiaomi Software Tech</p> <p>NAS-MM preferred</p>
<p>8 – Motorola Mobile Com Technology</p> <p>NAS-SM: Each PDU session is authenticated based on the user id and credentials provided by the UE</p>
<p>9 – Guangdong OPPO Mobile Telecom.</p> <p>NAS-MM</p>
<p>10 – InterDigital</p> <p>NAS-MM is preferred since the UE is supposed to be associated with all PDU Sessions</p>
<p>11 – Samsung Electronics Czech</p> <p>As indicated in 1.29, UE should be able to provide User Identifier and /or credentials in both NAS-MM and NAS-SM messages.</p> <p>Also, the option of HLOS performing local authentication (as indicated by QC), and UE just providing some sort of "user ID tag"/"successful authentication" can also be an alternate option in case operator wants to support this method, and the Operator can trust the HLOS authentication mechanism. Some pre-configuration (OTT based) might be needed between the operator and the UE.</p>
<p>12 – Ericsson LM</p> <p>UP, but if NAS is used then NAS-SM</p>
<p>13 – Deutsche Telekom AG</p> <p>UP, but if NAS is used then NAS-SM</p>
<p>14 – Nubia Technology Co.</p> <p>ZTE: NAS-MM. (also see the answer to Q#1.29)</p>

Feedback Form 49: Question KI#2.6: How is the AAA Server selected?

<p>1 – Qualcomm Incorporated</p> <p>No need for AAA Server.</p>
<p>2 – NEC Europe Ltd</p> <p>The AAA Server retrieved from the User Profile.</p>
<p>3 – LG Electronics France</p> <p>Based on information in User Identifier (NAI format).</p>
<p>4 – Nokia Corporation</p> <p>Re-use the principles described in 23.501 sections 5.30.2.9.2 and 23.502 sections 4.2.2.2.4. (Based on MM). The Authentication Server details are stored in the profile.</p>
<p>5 – HUAWEI Technologies Japan K.K.</p> <p>Based on User ID or DNN/S-NSSAI if the AAA server is deployed by the third party, or subject to operators' deployment if the User ID is allocated by the operator.</p>
<p>6 – CATT</p> <p>To be decided by SA3.</p>
<p>7 – Motorola Mobile Com Technology</p> <p>Using existing procedure where the SMF identifies the AAA server based on information provided by the UE in the SM PDU DN request container in the PDU session request. AAA server needs to be reachable by each SMF to enable authentication</p>
<p>8 – Deutsche Telekom AG</p> <p>Based on information in User Identifier (NAI format).</p>
<p>9 – Guangdong OPPO Mobile Telecom.</p> <p>AAA server is selected by AMF. The AMF performs the role of the EAP Authenticator and communicate with the AAA-S.</p>
<p>10 – InterDigital</p> <p>Based on the user identifier.</p>

11 – Samsung Electronics Czech

AAA server address can be stored in User profile, or can come from UE (based on realm part of user identifier).

12 – Ericsson LM

For UP there is no need for 3GPP to specify. If NAS-SM, then based on User ID and configuration

13 – Nubia Technology Co.

ZTE: Similar with Credential holder case in the SNPN. UDM/AUSF select the AAA server according to the User ID, or information in the User ID profile.

Feedback Form 50: Question KI#2.7: When, or in what procedure(s), does the UDM enforce the restriction that only one user shall be active with a UE's subscription at a given time?

1 – Qualcomm Incorporated

No need.

2 – LG Electronics France

During the activation of User Identifier (during Registration procedure), UDM enforce the restriction.

3 – Guangdong OPPO Mobile Telecom.

We still do not think the question is accurate. UDM/UDR may store User ID state, or perform active user restriction check, but we do not think we should specify UDM to enforce the restriction. It should be AMF or SMF, based on the information from UDM/UDR to enforce the restriction that only one user shall be active with a UE's subscription at a given time.

4 – Nokia Corporation

The UDM is responsible to activate a human User with a UE subscription during the Registration procedure (see answer to KI#1.29). Therefore, we propose that the UDM also enforces the restriction that only one human User shall be active with a UE subscription during the Registration procedure.

5 – CATT

After the user identifier/user profile is active with a subscription.

<p>6 – Beijing Xiaomi Software Tech</p> <p>during the linkage operation in registration procedure, after authentication/authorization of the User identity, the linkage information is stored in UDM, so UDM can make there is only one linkage.</p>
<p>7 – Motorola Mobile Com Technology</p> <p>After successfull authentication the SMF provides authenticated active user ID to the UDM. We also support AF providing active user information via NEF to the UDM</p>
<p>8 – Deutsche Telekom AG</p> <p>After the user identifier/user pofile is active with a subscription (PDU Session Establishment).</p>
<p>9 – InterDigital</p> <p>During activation of the user (e.g. in a registration procedure).</p>
<p>10 – Samsung Electronics Czech</p> <p>UDM can't enforce the restriction. It just stores the result of active user identifier. Assuming both NAS-MM and NAS-SM is allowed to authenticate the user identifier, then whenever a new user identifier is coming, AMF and/or SMF fetch the profile from UDM and after finding that already one user is active, AMF and/or SMF will reject it instead of proceeding with authentication of this new user identifier.</p>
<p>11 – Ericsson LM</p> <p>UDM is not suitable for such restriction</p>
<p>12 – Apple Benelux B.V.</p> <p>UDM, based on the User identifier activation (During registration procedure) .</p>
<p>13 – Nubia Technology Co.</p> <p>ZTE: UDM, during the User ID activation</p>

4.3 Key Issue #3 – Round 2 Questions

Based on the round 1 discussion, it is proposed that that FS_UIA_ARC Key Issue #3 work proceeds under the following assumptions:

- NEF APIs are used to expose user profile information.

Feedback Form 51: Question KI#3.4: Should it be possible to expose authentication results, via an NEF API?

1 – Qualcomm Incorporated We disagree with the assumption. No need for APIs.
2 – NEC Europe Ltd No
3 – China Mobile Com. Corporation No
4 – LG Electronics France Yes.
5 – Guangdong OPPO Mobile Telecom. Yes
6 – Nokia Corporation Yes, the exposure shall be through the NEF APIs.
7 – HUAWEI Technologies Japan K.K. Yes
8 – CATT Yes
9 – Beijing Xiaomi Software Tech yes
10 – InterDigital yes
11 – Samsung Electronics Czech Yes, if a 3rd party requests for User authentication by providing a particular "User ID" , network can trigger user authentication and return to the 3rd party if User ID was successfully authenticated, i.e. the Authentication result (success/failure).

<p>12 – Ericsson LM</p> <p>No, a use case need to be provided. Also, an AF does not expose via NEF.</p>
<p>13 – Apple Benelux B.V.</p> <p>We have some difficulty in agreeing with the assumption.</p> <p>Authentication results , as explained by Samsung above, is a different scenario that requires more discussion (whether an (or any) AF is allowed to trigger 5GC authentication of a user identifier). In general authentication result is not to be exposed through NEF API to any AF. If there is consensus on User Identity profile management through NEF API, then such management API may provide authentication result to the AF that is authorized to manage user identity profiles in that MNO. But again, that is more appropriate as services of management API and not as a general exposure API.</p>
<p>14 – Deutsche Telekom AG</p> <p>No</p>
<p>15 – Nubia Technology Co.</p> <p>ZTE: Yes</p>

Feedback Form 52: Question KI#3.5: Should it be possible to expose, to an authorized AF, whether a user is active, via an NEF API?

<p>1 – Qualcomm Incorporated</p> <p>No.</p>
<p>2 – NEC Europe Ltd</p> <p>No</p>
<p>3 – China Mobile Com. Corporation</p> <p>No</p>
<p>4 – LG Electronics France</p> <p>No need to expose whether a user is active. According to architecture assumption, a User Identifier is active when the User Identifier has been authenticated and authorized to use a linked subscription. Therefore, exposing authentication results is sufficient.</p>
<p>5 – Guangdong OPPO Mobile Telecom.</p> <p>No</p>

6 – Nokia Corporation Yes. The security profile associated with the User Identity Profile and the consent provided by the UE Subscription shall control what can be exposed and it shall be discussed with SA3.
7 – HUAWEI Technologies Japan K.K. Yes
8 – CATT Yes
9 – Beijing Xiaomi Software Tech it seems depend on whehter the authorized AF is the owner AF of the User Identity profile. if yes, then there is no need, beacuse the owner AF already has such active information. if not, why other AF needs such active information? need further clairifcation
10 – InterDigital yes
11 – Samsung Electronics Czech As per the Samsung’s answer above, 3rd party can similarly check or monitor if the User is active.
12 – Ericsson LM No, Need a valid use case
13 – Deutsche Telekom AG No
14 – Nubia Technology Co. ZTE: Yes

Feedback Form 53: Question KI#3.6: Should it be possible to expose, to an authorized AF, the identities of the subscriptions that are linked to a user identity, via an NEF API?

1 – Qualcomm Incorporated No.
2 – NEC Europe Ltd No

3 – China Mobile Com. Corporation No
4 – LG Electronics France No.
5 – Guangdong OPPO Mobile Telecom. No
6 – Nokia Corporation Yes, based on the consent profile of the UE Subscription (of which AF can fetch such information). This needs to be discussed along with SA3.
7 – HUAWEI Technologies Japan K.K. Open for discussion. So far it is unclear what's the use case for the AF to be aware of the SUPI, or it is meant for GPSI?
8 – CATT GPSI can be exposed.
9 – Beijing Xiaomi Software Tech need further clarification what specific identities of the subscription, for example, SUPI/SUCI is not allowed. GPSI may be ok
10 – InterDigital yes
11 – Samsung Electronics Czech No
12 – Ericsson LM No, Need a valid use case
13 – Apple Benelux B.V. No. Not as an exposure API. It maybe part of management APIs to the AF that is managing the user identity profiles, if such a functionality is agreed.
14 – Deutsche Telekom AG No

15 – Nubia Technology Co.

ZTE: Yes

Feedback Form 54: Question KI#3.7: If an AF is authorized to create a user profile, can the same AF read all or only partial information from the user profile?

1 – Qualcomm Incorporated

No.

2 – NEC Europe Ltd

No

3 – LG Electronics France

No. Why the same AF need to read provisioned information? AF should maintain the information to update User Identity Profile to detect change and send update request to 5GC.

4 – Guangdong OPPO Mobile Telecom.

No.

5 – Nokia Corporation

The User Identity Profile may have the AFs (the one created or the one allocated to manage based on OAM, etc) that can manage the User Identity Profile; so only those should be able to read. This needs to be aligned with SA3.

6 – HUAWEI Technologies Japan K.K.

Open for discussion, may be decided after the content of the user profile is stable.

7 – CATT

Information exposed to the AF can be only partial of the user profile.

8 – Beijing Xiaomi Software Tech

all the information in the User profile, after authorization.

9 – InterDigital

yes.

10 – Samsung Electronics Czech

Question is not clear. If an AF has created the user profile then that means it has all the information of the content of the user profile. Is there any extra information present in the user profile that the AF does not know and who has provisioned those extra content without the knowledge of the AF.

11 – Ericsson LM

From our perspective the UIP is stored in the AF creating the UIP i.e. there is no need for a separate "read"

12 – Apple Benelux B.V.

Not required as part of any exposure service. It could be part of a management service

13 – Nubia Technology Co.

ZTE: This Q has dependency with Q#1.27. If only one AF can manage (e.g. Link) the UIP, it can read all the information from the UIP.

4.4 Key Issue #4 – Round 2 Questions

Based on the round 1 discussion, it is proposed that that FS_UIA_ARC Key Issue #4 work proceed under the following assumptions:

- The 5GC needs to be able to identify traffic from each individual non-3GPP device.
- Whether and how to authenticate/authorize a non-3GPP device is a SA WG3 decision.
- The operator is able to optionally restrict the number of simultaneously active User Identifiers per UE or 5G-RG. However, in terms of prioritizing meeting time, this will be low priority.
- It is possible for the UE or 5G-RG to send traffic from non-3GPP devices that are not associated with a user identifier (i.e. legacy cases).
- When their traffic is going to the same DNN/S-NSSAI combination, traffic from the non-3GPP devices share the same PDU Session

Feedback Form 55: Question KI#4.8: Does the 5GC identify the traffic from the individual non-3GPP devices by a user identifier or an IP Address/MAC Address when obtaining service requirements (e.g. QoS)?

1 – Qualcomm Incorporated

We disagree with the assumptions, the conclusions should focus on the levels of differentiation that are needed and not on identifying individual devices.

IP Address can't work in case of NAT. MAC address can't work for IP type PDU Session, can't work for Random MAC address, and depends on the frame handling mode in UE/RG.

2 – NEC Europe Ltd

User Identifier

3 – vivo Mobile Communication Co.

firstly, current mechanism to identify the traffic is based on IP address + port, how to UPF to detect the traffic according to user ID? is that mean that to add any information in packet? I didn't know how to realize that and how to UE to add such packet header.

I prefer to use existing IP address, port number, or maybe MAC address to identify the traffic, user id can be used to identify the device by UE/5GRG, not identify traffic.

4 – China Mobile Com. Corporation

User Identifier

5 – LG Electronics France

The 5GC should be able to support different charging and QoS for each non-3GPP device. Therefore, 5GC should be able to identify traffic of individual non-3GPP devices. To support different QoS, 5GC should be able to identify non-3GPP device traffic based on address (e.g. IP address/MAC address). To support different charging, the detected non-3GPP traffic using address information should be also associated with non-3GPP device identifier.

6 – Guangdong OPPO Mobile Telecom.

The 5GC needs to be able to identify traffic from each individual non-3GPP device by a user identifier.

7 – Nokia Corporation

Firstly, we should support use cases to consider both single PDU Session and individual PDU Session per User Identifier. For both the cases, the solutions in the TR provide details on how of both the options (Single and multiple). In case of individual PDU Session, 5GC shall just rely on the sub keys of SUPI and DNN/S-NSSAI from the UDR for implementing policies. For a single PDU Session, 5GC may use the User Identifier or the IP Address/MAC Address.

When a new device is detected and an IP is used by the UE/5G-RG, the same shall be reported to the SMF as part of the PDU Session Modification procedures **along with the corresponding user identifier** (and similar for the release of the corresponding IP / non-3gpp device).

8 – HUAWEI Technologies Japan K.K.

By the User Identifier. The IP address/MAC address may be provided as well.

<p>9 – CATT</p> <p>It should be based on User Identifier as an IP address may be shared by several non-3GPP Devices.</p>
<p>10 – Beijing Xiaomi Software Tech</p> <p>prefer device identifier</p>
<p>11 – Motorola Mobile Com Technology</p> <p>Prefer user identifier</p>
<p>12 – Deutsche Telekom AG</p> <p>User Identifier</p>
<p>13 – Siemens AG</p> <p>For non-IP devices, can identify non-3GPP devices by MAC address, or user identifier.</p>
<p>14 – InterDigital</p> <p>User Identifier</p>
<p>15 – Samsung Electronics Czech</p> <p>The question seems ambiguous, if multiple devices (that have different User Identifiers) are sharing a PDU Session, then 5GC has to know the IP Address/MAC address of the devices in order to correlate each of them to a (possibly different) User profile (which is indexed by User ID) and then only it can provide service differentiation to different Non-3GPP devices within a PDU Session.</p>
<p>16 – Ericsson LM</p> <p>IP address, but depends on procedure as in "management" procedure the DEVICE identifier can be used</p>
<p>17 – Charter Communications</p> <p>Both options can be considered for conclusions phase. Depending on factors like the capabilities of the non-3GPP device, PDU session type, etc., the 5GC/5GS may use one or both for identification of traffic to/from an individual device.</p> <p>For example:</p> <ul style="list-style-type: none">- for a device that does not use MAC randomization, MAC address (IP address+port) can be used as a non-3GPP device identifier for Ethernet type (IP type) PDU session.- for a device that uses MAC randomization, a user identifier can be used by the 5GC.
<p>18 – CableLabs</p> <p>User identifier, but the IP address/MAC address could be provided as well.</p>

19 – Nubia Technology Co.

ZTE: by an IP Address/MAC Address.

Feedback Form 56: Question KI#4.9: Is it necessary to specify a procedure where the user identifier is bound to a non-3GPP device? If yes, who does the binding (e.g. the 5GC or 5G-RG/UE)? If yes, who is aware of the binding (e.g. the 5GC, 5G-RG/UE, or both)?

1 – Qualcomm Incorporated

No. User identifier and non-3GPP devices are different thing, no benefit to bind them together.

2 – vivo Mobile Communication Co.

UE binding may have benefit, because it is not nessasary to always let the 5GC to know the device is binded and this will cause NAS message strom.

3 – LG Electronics France

Yes. Binding should be supported. 5G-RG/UE binds device identifier and non-3GPP device based on policy received from the 5GC. The 5G-RG/UE also notifies the device identifier to the 5GC, which is used by the 5GC to support different charging and QoS.

4 – Guangdong OPPO Mobile Telecom.

It is necessary to bind the Device Identifier (we assume the user identifier here refers to non-3GPP Device Identifier) to a non-3GPP device. The binding process should be an interaction between the non-3GPP device and UE/5G-RG. Therefore, it is not necessary to specify a procedure in the scope of 3GPP.

5 – Nokia Corporation

The main requirement is to be able to identify the traffic and implement corresponding policies. Any such binding (which is also discussed during the round 1), shall be done only by the UE/5G-RG.

6 – HUAWEI Technologies Japan K.K.

The linkage of the User Identifier with the non-3GPP device (e.g. the MAC address) can be provisioned in the UDM/UDR. The UE/5G-RG is also aware of the linkage, either by receiving the information from the 5GC or AF or by pre-configuration.

7 – CATT

No, it is out of SA2 scope.

<p>8 – Beijing Xiaomi Software Tech</p> <p>here user identifier is device identifier right? whether device identifier of non-3GPP device can reuse user identifier need further discussion</p>
<p>9 – Motorola Mobile Com Technology</p> <p>Both are feasible. It is simpler that the 5G-RG/UE has user profile information to bind a device to a user identifier.</p>
<p>10 – Siemens AG</p> <p>The UE/5G-RG does the binding but is not necessary to define the procedure, which 5GC is not aware.</p>
<p>11 – InterDigital</p> <p>Both options should be possible. At least the 5GC should be aware of the binding.</p>
<p>12 – Samsung Electronics Czech</p> <p>More discussion required.</p>
<p>13 – Ericsson LM</p> <p>UE/5G-RG knows the binding and the entity handling the management requests e.g. AF/server. We are open to specify procedures but the for KI#4 we are using device identifiers, if needed.</p>
<p>14 – Charter Communications</p> <p>If user identifier is used, each user identifier needs to be bound to a non-3GPP device. Binding can be done by the 5G-RG/UE or by the 5GC that can be further discussed.</p> <p>For 5G-RG deployments, 5GS signalling load implications must be taken into consideration during evaluation phase if binding of a user identifier to a non-3GPP device requires dedicated signalling flow (like PDU session modification/establishment) between a 5G-RG and 5GC.</p>
<p>15 – Charter Communications</p> <p>If user identifier is used, each user identifier needs to be bound to a non-3GPP device. Binding can be done by the 5G-RG/UE or by the 5GC that can be further discussed.</p> <p>For 5G-RG deployments, 5GS signalling load implications must be taken into consideration during evaluation phase if binding of a user identifier to a non-3GPP device requires dedicated signalling flow (like PDU session modification/establishment) between a 5G-RG and 5GC.</p>
<p>16 – CableLabs</p> <p>Binding can be done either by the 5G-RG/UE or by the 5GC. And both 5G-RG/UE and 5GC would be aware of the binding.</p>

17 – Nubia Technology Co.

ZTE: The binding is by 5G-RG/UE. And the procedure about the binding is out of 3GPP scope.

5 Summary from Rapporteur

5.1 Key Issue #1 – Round 2 Summary

5.1.1 User Identity Profile Management

Based on the round 1 discussion, it is proposed that that FS_UIA_ARC Key Issue #1 work proceeds under the following assumptions:

- The User Identifier can be operator assigned or third party assigned.
- The User Identity Profile can be managed by an operator or by a third party.
- The User Identity Profile is stored in the UDR.

Question KI#1.13 asked “Can NEF API’s be used by a trusted AF (i.e. operator owned or 3rd party owned) to manage the User Identity Profile?”

17 Companies responded.

14 companies answered yes.

2 companies commented that the question was not clear.

1 company answered no.

Proposal: Proceed under the assumption that the NEF API’s be used by a trusted AF (i.e. operator owned or 3rd party owned) to manage the User Identity Profile.

Question KI#1.14 asked “Does managing a user profile include creating, modifying, and deleting a user profile?”

16 Companies responded.

15 companies answered yes.

1 company answered no.

Proposal: Proceed under the assumption that managing a user profile includes creating, modifying, and deleting a user profile.

Question KI#1.15 asked “In the operator managed scenario, can OAM procedure be used to manage the User Identity Profile?”

15 Companies responded.

10 companies answered yes. Some of these “yes” answers indicated that the details should be left to SA5.

3 companies answered that it is an SA5 decision.

1 company answered No.

Proposal: Proceed under the assumption that OAM procedures be used to manage the User Identity Profile, however, the details are left to SA WG#5.

5.1.2 User Identity Profile Contents

Based on the round 1 discussion, it is proposed that that FS_UIA_ARC Key Issue #1 work proceeds under the following assumptions:

- The User Identity Profile includes QoS Information.
- The User Identity Profile includes DNN/S-NSSAI’s that the user is allowed to access.

The following question are about what else might be stored in the User Identity Profile and these questions are based on the round 1 questions.

Question KI#1.16 asked “Is the QoS Information in the User Identity Profile stored per DNN/S-NSSAI?”

17 Companies responded.

7 companies answered yes.

7 companies answered no.

3 companies indicated the question was not clear or required further discussion.

Proposal: Proceed under assumption that the QoS Information in the User Identity Profile can stored per DNN/S-NSSAI, but it does not need to be stored per DNN/S-NSSAI.

Question KI#1.17 asked “Is the QoS Information QoS Flow level QoS parameter values (5QI and ARP)?”

16 Companies responded.

14 companies answered yes.

2 indicated the need for further discussion, but even these answers were interpreted to mean that these parameters are ok but other parameters need to be considered.

Proposal: Proceed under assumption that the QoS Information in the User Identity Profile can include QoS parameter values (5QI and ARP).

Question KI#1.18 asked “Can information about IMS settings be stored in the User Identity Profile?”

16 Companies responded.

13 companies answered no.

3 companies answered yes.

Proposal: Proceed under assumption that information about IMS settings cannot be stored in the User Identity Profile.

Question KI#1.19 asked “Can information about SMS settings be stored in the User Identity Profile?”

16 Companies responded.

11 companies answered no.

5 companies answered yes.

Proposal: Proceed under assumption that information about SMS settings cannot be stored in the User Identity Profile.

Question KI#1.20 asked “Can information about service chain settings be stored in the User Identity Profile?”

16 Companies responded.

11 companies answered no.

5 companies answered yes.

Proposal: Proceed under assumption that information about service chain settings cannot be stored in the User Identity Profile.

Question KI#1.21 asked “Can information about other services (e.g. MBS, V2X) be stored in the User Identity Profile?”

17 Companies responded.

12 companies answered no.

5 companies answered yes.

Proposal: Proceed under assumption that information about other services (e.g. MBS, V2X) cannot be stored

in the User Identity Profile.

Question KI#1.22 asked “Can the PEI’s of devices that the user is allowed to use be stored in the User Identity Profile?”

16 Companies responded.

11 companies answered no.

2 companies were open to discussing the use case

3 companies answered yes.

Proposal: Proceed under assumption the PEI’s of devices that the user is allowed to use are not stored in the User Identity Profile.

Question KI#1.23 asked “Can user specific AMF policies be stored in the User Identity Profile? ”

16 Companies responded.

11 companies answered no.

2 companies question the use case and/or require clarification

3 companies answered yes.

Proposal: Proceed under assumption that user specific AM policies are not stored in the User Identity Profile.

Question KI#1.24 asked “Can user credentials be stored in the User Identity Profile?”

14 Companies responded.

5 companies answered yes.

3 companies answered no.

4 companies responded that it should be left to SA3.

2 companies answered that credentials should in the entity that does the authentication.

NOTE: Many answers seem to imply that credentials should in the entity that does the authentication.

Proposal: Proceed under assumption that SA WG3 will decide where user credentials are stored.

5.1.3 User Identity Influence on QoS

Based on the round 1 discussion, it is proposed that that FS_UIA_ARC Key Issue #1 work proceeds under the following assumptions:

- PCC Rules are adjusted/updated when a user becomes active with a subscription.

Question KI#1.25 asked “Are the PCC Rules updated based on information that the PCF receives from the User Identity Profile?”

17 Companies responded.

15 companies answered yes.

2 companies answered no.

Proposal: Proceed under assumption that PCC Rules are updated based on information that the PCF receives from the User Identity Profile.

Question KI#1.26 asked “Are the PCC Rules updated based on invocation of existing PCF/NEF API (e.g., Npcf_PolicyAuthorization_Create)?”

13 Companies responded.

12 companies answered yes.

Proposal: Proceed under assumption that PCC Rules can be updated based on invocation of existing PCF/NEF API (e.g., Npcf_PolicyAuthorization_Create).

5.1.4 Linking

Based on the round 1 discussion, it is proposed that that FS_UIA_ARC Key Issue #1 work proceeds under the following assumptions:

- A trusted AF can use an NEF API to request that a user identifier be linked/unlinked with a subscription.
- OAM procedures can be used to link/unlink a user identifier with a subscription.

Question KI#1.27 asked “For each user identity, is there only one, or more than one, AF that is authorized to request that the user be linked to a subscription?”

13 Companies responded.

9 companies answered, “only one”.

2 companies answered, “more than one”.

2 companies questioned the user case and/or the premise of the question.

Proposal: Proceed under assumption that, for each user identity, is there only one AF that is authorized to request that the user be linked to a subscription.

Question KI#1.28 asked “For each subscription, is there only one, or more than one, AF that is authorized to request that a user be linked to the subscription?”

12 Companies responded.

7 companies answered, “only one”.

3 companies answered, “more than one”.

2 companies questioned the user case and/or the premise of the question.

Proposal: Proceed under assumption that, for each subscription, there is only one AF that is authorized to request that a user be linked to the subscription.

5.1.5 Activation

Based on the round 1 discussion, it is proposed that that FS_UIA_ARC Key Issue #1 work proceeds under the following assumptions:

- A linked user becomes active with a subscription by providing a user identifier in a NAS message.

Question KI#1.29 asked “Is the user identifier provided in an NAS-MM (e.g. registration) or a NAS-SM (e.g. PDU Session Establishment)? Which NAS message(s)?”

17 Companies responded.

7 companies answered, “NAS-MM”.

4 companies answered, “NAS-SM”.

4 companies prefer no NAS impact, 3 of the 4 prefer NAS-SM if there is impact.

1 company indicated that both NAS-MM and NAS-SM may need to be supported.

1 company prefers more discussion but comments that NAS-SM seems not appropriate.

Proposal: Discuss this more between now and SA2 #163.

5.1.6 SMS

Based on the round 1 discussion, it is proposed that that FS_UIA_ARC Key Issue #1 work proceeds under the following assumptions:

SMS can be used when a user identifier is active with a subscription.

Question KI#1.30 asked “When a user is active with a subscription, does delivery of the SMS service continue based only on information from the subscription? In other words, when the user becomes active, are SMS messages still delivered to the MSISDN in the subscription?”

16 Companies responded.

12 companies answered Yes.

4 companies answered No.

Proposal: Proceed under assumption that, when a user is active with a subscription, delivery of the SMS service continues based only on information from the subscription.

Question KI#1.31 asked “When a user is active with a subscription, does activation of the user impact the SMS service? If yes, then in what way is the SMS service impacted? Is an MSISDN that is associated with the User Identity Profile used instead?”

16 Companies responded.

12 companies answered No.

4 companies answered Yes.

Proposal: Proceed under assumption that, when a user is active with a subscription, the SMS service is not impacted.

5.1.7 IMS

Based on the round 1 discussion, it is proposed that that FS_UIA_ARC Key Issue #1 work proceed under the following assumptions:

- IMS can be used when a user identifier is active with a subscription.

Question KI#1.32 asked “When a user is active with a subscription, does delivery of the IMS service continue based only information from the subscription?”

15 Companies responded.

12 companies answered Yes.

3 companies answered No.

Proposal: Proceed under assumption that, when a user is active with a subscription, delivery of the IMS service continues based only information from the subscription.

Question KI#1.33 asked “When a user is active with a subscription, does activation of the user impact the IMS service? If yes, then in what way is the IMS service impacted? Is an IMPU that is associated with the User Identity Profile used instead?”

14 Companies responded.

13 companies answered No.

1 companies answered Yes.

Proposal: Proceed under assumption that, when a user is active with a subscription, activation of the user does not impact the IMS service.

5.2 Key Issue #2 – Round 2 Summary

Based on the round 1 discussion, it is proposed that that FS_UIA_ARC Key Issue #2 work proceeds under the following assumptions:

- Authentication is performed between the UE and a AAA Server.
- Communication between the UE and AAA-S is via NAS.
- The UDM enforces the restriction that only one user shall be active with a UE’s subscription at a given time.

Question KI#2.5 asked “Is communication between the UE and AAA Server via NAS-MM or NAS-SM signaling?”

14 Companies responded.

7 companies answered, “NAS-MM”.

4 companies answered, “NAS-SM”.

1 company says to defer to SA WG#3.

1 company says both.

1 company says neither

Proposal: Discuss this more between now and SA2 #163.

Question KI#2.6 asked “How is the AAA Server selected?”

13 Companies responded.

10 companies replied that the AAA Server is selected based on the user identifier (e.g. realm part of the NAI) and/or information from the user profile.

1 company replies that there is no need for a AAA Server.

1 company replies that it should be left for SA3.

1 company replies that the AMF performs the selection.

Proposal: Proceed under the assumption that the AAA Server is selected based on the user identifier or based on information that is retrieved from the user profile.

Question KI#2.7 asked “When, or in what procedure(s), does the UDM enforce the restriction that only one user shall be active with a UE’s subscription at a given time?”

13 Companies responded.

11 companies replied that the restriction is enforced during the activation procedure.

1 company replies that there the UDM is not suitable.

1 company replies that there is no need for such a restriction.

NOTE: A few companies made the clarification that it is not the UDM that enforces the restriction, but it is the AMF or SMF that enforces the restriction based on information from the UDM. I think that this is a good distinction, and this is how I am assuming that everyone read the question. I should have made the question clearer.

Proposal: Proceed under the restriction is enforced during the activation procedure based on information from the UDM.

5.3 Key Issue #3 – Round 2 Summary

Based on the round 1 discussion, it is proposed that that FS_UIA_ARC Key Issue #3 work proceeds under the following assumptions:

- NEF APIs are used to expose user profile information.

Question KI#3.4 asked “Should it be possible to expose authentication results, via an NEF API?”

15 Companies responded.

9 companies responded yes.

6 companies responded no.

Proposal: Discuss this more between now and SA2 #163.

Question KI#3.5 asked “Should it be possible to expose, to an authorized AF, whether a user is active, via an NEF API?”

14 Companies responded.

7 companies responded no.

6 companies responded yes.

1 companies requires further discussion.

Proposal: Discuss this more between now and SA2 #163.

Question KI#3.6 asked “Should it be possible to expose, to an authorized AF, the identities of the subscriptions that are linked to a user identity, via an NEF API?”

15 Companies responded.

9 companies responded no.

5 companies responded yes.

1 company is open to discussing.

Proposal: Discuss this more between now and SA2 #163.

Question KI#3.7 asked “If an AF is authorized to create a user profile, can the same AF read all or only partial information from the user profile?”

13 Companies responded.

5 companies responded no.

5 companies responded that some information can be read.

3 companies questioned the use case.

Proposal: Discuss this more between now and SA2 #163.

5.4 Key Issue #4 – Round 2 Summary

Based on the round 1 discussion, it is proposed that that FS_UIA_ARC Key Issue #4 work proceed under the following assumptions:

- The 5GC needs to be able to identify traffic from each individual non-3GPP device.
- Whether and how to authenticate/authorize a non-3GPP device is a SA WG3 decision.
- The operator is able to optionally restrict the number of simultaneously active User Identifiers per UE or 5G-RG. However, in terms of prioritizing meeting time, this will be low priority.
- It is possible for the UE or 5G-RG to send traffic from non-3GPP devices that are not associated with a user identifier (i.e. legacy cases).
- When their traffic is going to the same DNN/S-NSSAI combination, traffic from the non-3GPP devices share the same PDU Session

Question KI#4.8 asked “Does the 5GC identify the traffic from the individual non-3GPP devices by a user identifier or an IP Address/MAC Address when obtaining service requirements (e.g. QoS)?”

19 Companies responded.

12 companies indicated user identifier.

2 companies commented that the question needs clarification.

3 companies indicated IP Address

1 company indicated both.

1 company disagreed with the assumptions behind the question.

Proposal: Proceed under the assumption that the 5GC knows the User ID that is associated with the IP Address/MAC address of the devices and the User ID can be used to index the User Profile.

Question KI#4.9 asked “Is it necessary to specify a procedure where the user identifier is bound to a non-3GPP device? If yes, who does the binding (e.g. the 5GC or 5G-RG/UE)? If yes, who is aware of the binding (e.g. the 5GC, 5G-RG/UE, or both)?”

17 Companies responded.

12 companies indicated binding is needed. At least 7 companies indicated that both the 5G-RG/UE and 5GC should be aware of the binding. 4 companies indicated that only the 5G-RG/UE needs to know the binding.

2 companies indicated binding is not needed.

3 companies indicated binding requires further discussion.

Proposal: Proceed under the assumption that the user identifier will be bound to a non-3GPP device. The details of how the binding is done needs to be discussed more between now and SA2 #163.