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

# 1 Overall description

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

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

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

**Key Issue #1**

|  |  |
| --- | --- |
| Key area | Company Input |
| (1a): Where is the user profile stored? (e.g. UDM/UDR, in a different NF, outside of the 5GC) | Nokia: Our analysis (by also considering the SID study and Architectural Assumption/Requirements, and the study is to bring User Identities under the 5GC) indicates to use UDM/UDR which already maintains the UE subscription. Our understanding is that bringing in a new NF or treating the same externally would not only loose flexibility but bring in additional interfaces and complexities.  [LGE] Stored in the UDR/UDM.  [InterDigital] Stored in the UDR/UDM.  [Lenovo] Our preference is that the user profile is available at the UDM/UDR (more specifically in the UDR) either pre-configured or created/updated by an Application Function.  [ZTE] Stored in the UDR/UDM.  [Ericsson] User Profile stored (and managed) outside existing 5GC NFs within the HPLMN trust domain and mapped to 5GC internal identities e.g. IMPU, SUPI, GPSI or user address, or using 5GC exposure interface for enabling service differentiation.  [OPPO] UDM/UDR is a valid choice.  [CATT] Stored in the UDR/UDM.  [Deutsche Telekom] Stored in the UDR.  [Samsung] Prefer other NF, since the databases in UDM and UDR are indexed by SUPI.  Other option is that we have a logically separate database in UDR (one is the subscription data indexed by SUPIs/GPSIs and other is User Profile Data indexed by only User Identifiers) and the User-Ids may optionally be stored in the UE subscription, if the network wants to ensure that only certain user Ids can use a UE.  [HW] Stored in the UDR/UDM.  [vivo] Store in trusted AF may better.  [NEC] UDR/UDM  [Xiaomi] UDM/UDR, but need to further clarify which parameters stored in UDM, which are in UDR. |
| (1a) Rapporteur Summary: | 13 Companies Replied.  10 Companies indicated a preference for storing the User Profile in the UDR/UDM.  1 Company prefers an NF other than the UDM/UDR  2 Companies indicated a preference for storing the User Profile outside of existing 5GC NFs but within the HPLMN trust domain. |
| (1b): How are user identities linked with a subscription? (e.g. based on a request received via an NEF API) | Nokia: The User profile which belongs to a human User Identifier as well as the UE subscription that belongs to a USIM/UE is provisioned by the PLMN via OAM/NEF. OAM/NEF should be used for linking and unlinking a human User Identifier with the UE Subscription.  [LGE] Based on AF request using NEF service.  [InterDigital] Based on AF request using NEF service.  [Lenovo] We see that the association of a user identity to a subscription to be based on request from AF, where the AF gets aware of the association via app-layer mechanisms  [ZTE] AF request or OAM (similar with subscription provisioning).  [Ericsson] via "management" interface to server outside 5GC e.g. via a portal, see 1a  [OPPO] by using UDM API, OAM, or NEF API  [CATT] Based on AF request using NEF service, or provisioned by operator via OAM.  [Deutsche Telekom] via NEF service or OAM service.  [Samsung] For the scenarios when User Identities are managed by an entity outside 5GC (and that outside entity is not aware of the UE’s Identifier) linking can be done triggered by UE via NAS and verified by that entity (acting as AF) via NEF APIs. Otherwise Operator configuration can be used,  [HW] based on the operator configuration (e.g. the User id is allocated by operator and subscribed the static link with specific UE) or AF request via NEF  [vivo] By management interface, just like the user request a new SIM card in the offline shop.  [Xiaomi] based on the request from AF via NEF |
| (1b) Rapporteur Summary: | 12 Companies Replied.  9 Companies indicated that linking can be based on an NEF API.  9 Companies indicated that linking can be based on an OAM.  1 Company indicated that linking can be triggered via NAS  NOTE 1: I counted “AF Request” to be via an “NEF API”  NOTE 2: I counted “Management Interface” and “Operator Configuration” as OAM. |
| (1c): When does the UE provide the user identity to the 5GC in order to become “active”? (e.g. in a Registration Procedure, in a PDU Session Establishment Procedure) | Nokia: The study indicates that only one i.e., be it a User or a UE, shall use the UE at any point of time, which clearly indicates and guides that the active registration shall be valid with any of the following:   * UE + User X or * UE   Hence, we strongly consider having the User details being fetched, authenticated, and authorized during the Registration procedure.  [LGE] During the Registration procedure.  [InterDigital] Tentatively, during the Registration procedure. The reason we say tentative is that we should consider what is concluded in key issue #4 and we should also consider that, in a future release, we may want to support multiple users per UE (i.e. identifying applications that run on a UE). It may be that the PDU Session based approaches give us a better foundation for expanding the feature in a future release.  [Lenovo] We need to clarify first what does it mean that a user identity becomes "active" in the 3GPP network. One option is to state that the user ID becomes active when the UE includes User ID information in a registration or PDU session request. However, other options could also be considered.  The main objectives of the work is to identify traffic belonging to a user and our preference is the user id to be included in a PDU session signalling  [ZTE] During the Registration procedure, or a new NAS message (e.g. User activation). Because only one active User for one UE at given time, using PDU session establishment will cause additional complexity, i.e. how to notify other PDU sessions.  [Ericsson] Leading question (i.e. question is implying some specific solution), as there is no need for the UE to provide the UID to the 5GC itself, the UE/user makes link active via management interface and then the 5GC is provided with information required for service differentiation.  [OPPO] According to Note 2 in clause 4.1 Architecture Assumption, a user is considered active if the associated user identifier has been authenticated and authorized to use a linked subscription to access the 5GS. This clearly indicates that to become “active”, the UE provides the user identity/user identifier during authentication and authorization process.  [CATT] We are not sure if it is necessary for a UE to provide user identity to the 5GC. We understand the study mainly aims to offer service differentiation for different users which can be achieved by AF (instead of UE) providing user identity to 5GC. So for this study we don’t expect impacts on either Registration or PDU session establishment procedure.  [Deutsche Telekom] Primarily, during PDU Session Establishment, there may be other cases. No extra effort for limiting to single active user for a UE should be done.  [Samsung] It will depend on what kind of impacts would happen to UE or its services once a User Identifier becomes active.  [HW] We support to use the PDU session procedure. Especially one User id does not mean only one credential to authenticate this User id, so during the PDU session, more varied credential can be authenticated based on service security level requirement.  In other words, we think the authentication of the User id is for the service (as mentioned in the SID, the user id is defined to identify the traffic. The access authorization should be based on the UE credential (i.e. the UE is legal to access the network firstly) and based on the link between the UE and the User id (i.e. this user id is allowed to access via this UE or not, which can be performed during the PDU session procedure). So we don't think it is necessary to impact the registration procedure to check whether the User id is correct or not.  [vivo] Unclear why UE to reports the user ID. The UE may let the trusted AF to know the user ID active or not, just like the user log in the computer or server by password. And the 5GC may be notified by the management interface and know the status of the user ID.  [NEC] in the Registration Request.  [Xiaomi], based on the restriction only one user linked to a UE subscription in a given time, we think registration procedure is better. By considering the future cases, we can extend registration procedure to enable multiple users, e.g., include multiple user IDs in the registrations; PDU session procedure is also a possible option |
| (1c) Rapporteur Summary: | 13 Companies Replied.  5 Companies indicated that the UE provides the user identity during Registration.  3 Companies indicated that the UE provides the user identity during PDU Session Establishment.  3 Companies indicated that the UE does not need to provide the user identity directly to the 5GC, but instead provides the user identity to an AF/Management Interface.  1 Company Indicated that the UE provides the user identity during the authentication and authorization process. |
| (1d): How are user specific policies considered when configuring QoS for a PDU Session? | Nokia: AMF as part of the PDU Session Create shall also include the User Identity to the SMF. SMF also includes the User Identity information to the PCF. The PCF shall fetch the policies corresponding to the UE + User Identity information from the UDR.  [LGE] User Identity Profile contains user specific QoS information and it is used by the PCF to generate PCC rule.  [InterDigital] User Identity Profile contains user specific QoS information and it is used by the SMF to generate QoS Rules, QoS Profiles, and N4 Rules. OR it is used by the PCF to generate PCC Rules. SMF and PCF should be considered.  [Lenovo] In our view, the user profile may contain PDU session related policy information. This aligns with the assumption that the user profile is stored in the UDR.  [ZTE] If the User Profile contains the user specific Qos setting or Service information, the PCF can use this to generate the PCC rule.  [Ericsson] Either entity storing UIP adapts and re-uses existing exposure interface for QoS, or the existing user profile for an account (related to human using the UE) is used e.g. SUPI.  [OPPO] When configuring QoS for a PDU Session, related to user specific policies, the SMF performs user identity specific policies association/modification with the PCF.  [CATT] The user specific QoS settings contained in User Identity Profile can be used by PCF to derive PCC rule  [Deutsche Telekom] If the User Profile contains the user specific QoS setting or Service information, the PCF can use this to generate the PCC rule..  .  [Samsung]  [HW] User specific QoS could take higher priority than the QoS defined in UE subscription data, or this can be decided based on the operator policy. In brief, we cannot accept to specify that the UE QoS shall take higher priority than User QoS. Otherwise, there is no need to define the user specific QoS at all.  [vivo] Configure the 5QI to certain user ID during the SM policy association.  [Xiaomi] during the PDU session establishment, PCF fetches the policy/QoS information stored in UDR to generate PCC rule for SMF. |
| (1d) Rapporteur Summary: | 12 Companies Replied.  9 Companies indicated that the PCF considers the user specific policies when generating PCC Rules.  2 Companies indicated that the SMF considers the user specific policies when generating QoS Rules, QoS Profiles, and N4 Rules.  1 Company indicated that existing service exposure mechanisms can be used to adapt QoS.  NOTE 1: InterDigital and Lenovo replies were interpreted to mean SMF or PCF.  NOTE 2: I understood vivo’s reply to mean that the PCF can consider the user ID. |
| (1e): Whether and how is the user identity considered in services that exist outside of a PDU Session (i.e. SMS)? | Nokia: As discussed in the SA2#161, our suggestion is to use the alias identities to the User Identity, for e.g. GPSI for the User Identity shall be used for SMS. This shall ensure that there is no impact to various other nodes and specifications.  [LGE] According to SID there is a NOTE saying that "it is assumed that the user identifier is associated with all of services that the UE access during the time that the user identifier and UE are associated". Therefore, SMS also should be associated with user identifier.  [InterDigital] We agree that the user identifier should be “associated with” the SMS service.  [Lenovo] The main objectives of the work is to identify traffic belonging to a user (i.e. PDU session related signalling). However, we are open to discuss how user identity is used to verify the services allowed for a user.  [ZTE]  [Ericsson] Service requirements are unclear, but the SMS/IMS services should use existing identifiers i.e. MSISDN and IMPU.  [OPPO] the same view as Nokia. The User Identity Profile includes additional user identifiers or user identifier alias, in addition to the primary user identifier.  [CATT] It is not clear to us for what purpose user identity is considered for SMS service.  [Deutsche Telekom] UID shall be taken into for all services.  [Samsung] Services like SMS (whether with MSISDN or MSISDN less) are bind to a specific subscription (i.e. a specific SUPI/GPSI) and not to a user identity (User ID and User profile are entirely different from a UE subscription), so would not prefer to change the behaviour of those services.  [HW] Open for discussion.  [vivo] needs more clarification, prefer to focus the overall procedure of user ID, and then focus whether the SMS service is limited to some of the user IDs. And also needs to clarify why we selects SMS service as the specific service for user ID, but not other services in network.  [Xiaomi] during the PDU session procedure, we are clear why and how to use the user identifier, but for SMS case, more clarification and justification are needed. Any enhancement for the SMS service? |
| (1e) Rapporteur Summary: | 11 Companies Replied.  4 companies indicated that the user identifier somehow impacts access to the SMS service.  2 companies indicated that it is unclear why the user identifier would impact access to the SMS service.  1 company indicates that the user identifier should not impact access to other services such as SMS  3 companies indicated that they are open to discuss how user identity is used to verify the services allowed for a user.  1 company abstained. |
| (1f): What is the format of the user identifier (e.g. NAI)? | Nokia: Yes, NAI is the way forward. MNO may use any of the following examples for the User Identifier:  - Name.MCCMNC.RoutingID@domain.com, or alternatively  - string.routingID@domain.com. or  - Name@domain.com, where domain is built out of the MCC/MNC of the MNO and the RoutingID i.e. domain may be RIDxx.MNCyy.MCCzz.  [LGE] NAI format which is unique within a PLMN.  [InterDigital] NAI and unique within a PLMN. We agree with the example above from Nokia.  [ZTE] NAI is preferred.  [Ericsson] NAI is OK  [OPPO] NAI is ok. But it could be email address or some number. We propose to defer the format of the user identifier discussion in the future study, or maybe leave it for stage 3.    [CATT] NAI format should be used.  [Deutsche Telekom] NAI, UIDs defined outside of 3GPP should be useable as well as a 3GPP defined UID should exist.  [Samsung] To be decided by CT4. Just need to ensure this may not be similar to 3GPP identifier i.e. mcc/mnc should not be tagged to user id.  [HW] NAI is ok  [vivo] NAI is ok.  [Xiaomi] NAI is ok. Better to leave to stage 3 |
| (1f) Rapporteur Summary: | 10 Companies Replied.  9 companies seem to agree that NAI format can be used for the user identity. 2 of the 10 companies also suggests to leave the discussion to stage-3. |
| (1g): At SA #162, what Key Issue #1 solution principles are agreeable for an interim / partial conclusion? | Nokia: A User profile for a human User Identifier is created and maintained in the UDM/UDR and when the deployments support multiple UDMs there could be a possibility that the UDM for the UE and the UDM for the human User could be different.  NEF/OAM shall be used by the PLMN for provisioning and management of User Identities and linking of User Profiles with the UE Subscription.  [InterDigital] We think that the following principle would be a good for interim / partial conclusions:   * The User Profile is stored in the UDM/UDR. * Linking is based on the AF invoking an NEF Service. * QoS Information from the User Profile is considered by the SMF when generating QoS Rules/QoS Profiles, and N4 Rules OR QoS Information from the User Profile is considered by the PCF when generating PCC Rules. * The format of the user identifier is an NAI. * The user identifier is associated with the UE’s use of the SMS service. * Tentatively, during the Registration procedure, we need to also consider the KI#4 conclusion.   [Lenovo] User Profile information is available in AM subscription, SM subscription data and Policy control subscription data and includes one or more of the following:  - A User Profile Reference ID that uniquely identifies the User Profile among all User Profiles. One or more user identities can be associated with a user profile ID;  - User Profile information referenced with a User Profile ID in AM subscription data:  - User profile includes one or more devices (i.e. PEIs) that can use this User Profile;-  - User profile information references with a user profile ID in SM subscription data:  - User profile includes authentication information, such as credentials (e.g. a password, digital certificated, etc.) and authentication types;  - User profile ID references specific PDU session related control data:  There may be more than one User Profiles each associated with a User Profile Reference ID that are linked to the 3GPP subscription (SUPI).  During registration request:  - AMF retrieving User Profile information stored in the UDM  During PDU session request:  - AMF identifying active user and providing User Profile associated to user to SMF andPCF  [ZTE] If the User Profile   * The User Profile is stored in the UDM/UDR. * Linking is based on the AF request or OAM. * If the User Profile contains the user specific Qos setting or Service information, the PCF can use this to generate the PCC rule * The NAI is preferred for the format of the user identifier. * For the User identifier activation, Registration or new NAS message is preferred.   [Ericsson] None, but NAI can be assumed  [OPPO] OPPO proposes to agree on some high-level solution principles, and then move into specific principles. We provided a paper on the framework of solution principles for agreement.  [CATT] We think that the following principle would be a good for interim / partial conclusions:   * The User Profile is stored in the UDM/UDR. * Linking is based on the AF invoking an NEF Service or provisioned by operator via OAM. * QoS Information from the User Profile is considered by the PCF when generating PCC Rules. * The format of the user identifier is an NAI.   For others we need more discussion and should be clear on the requirements and prefer to have less impact on existing 5GS procedures.  [Samsung] linking require interaction between NEF and AF or can be done via OAM.  [HW] User ID format, User profile definition, and the extension of UE subscription data.  [Xiaomi] for our view, User profile is stored in UDR/UDM, but which parameters are in UDM, which are in UDR, need further clarification. more time are needed for the conclusions. |
| (1g) Rapporteur Summary: | 12 Companies Replied.  The following principles seem to have a noticeable level of support.   * 10 companies indicated that user profile is stored in the UDM/UDR. * 9 Companies indicated that management of the user profile (e.g. linking) can be based on an NEF API. * 9 Companies indicated that linking can be based on an OAM. * 9 companies indicated some preference for saying that the User Identity format can be NAI. * 9 Companies indicated that the PCF considers the user specific policies when generating PCC Rules.   The intention of question 1c was to collect input about what procedure might trigger a user to be authenticated and authorized so that the user can become active. The company replies did not show clear consensus.  The intention of question 1e was to collect input about what services other than a PDU Session (e.g. SMS) might need to consider the user identifier. For example, maybe the user identifier impacts whether a UE can access a service. The company replies did not show clear consensus.  Proposal: Document the 5 bullets above in TR 23.700-32 as an intermediate conclusion. |

**Key Issue #2**

|  |  |
| --- | --- |
| (2a): What network function(s) or entities can trigger authentication of the user (e.g. AMF, SMF)? | Nokia: Refer to our response to 1c, the registration procedure shall handle the authentication and authorization of the User Identity. So, it is inevitable that AMF carries out the authentication procedures for a User, the similar way it is done by the AMF for the UE.  [LGE] AMF.  [InterDigital] AMF or SMF (Depending on the KI#1 conclusion, see question 1a).  [Lenovo] User authentication is optional in the network as it can be carried out via app layer means. However, the SMF can re-use the secondary authentication procedure during PDU session establishment/modification  [ZTE] AMF is preferred.  For the SMF (i.e. PDU session establish/modify method), how to handle other PDU sessions are needed. Another issue is, whether the activation is encapsulated in the SM NAS or MM NAS?  [Ericsson] Authentication triggered at login using interface towards the entity managing the UIP e.g. UIP server outside 5GC while within HPLMN trust domain  [OPPO] It should AMF during registration procedures.  [CATT] It could be triggered by SMF before PDU session modification is performed.  [Deutsche Telekom] SMF.  [Samsung] Either the AMF can use specific NAS MM message to trigger User authentication, or it can just transparently pass request from some other NF (e.g. from UDM/NEF in case UDM/NEF triggers for User authentication). It may depend on the answer of 1c.  [HW] SMF during the PDU session procedure.  [NEC] AMF  [Xiaomi] AMF |
| (2a) Rapporteur Summary: | 12 Companies Replied.  7 companies expressed a preference that the AMF trigger authentication of the user.  5 companies expressed a preference that the SMF trigger authentication of the user.  1 company prefers that authentication takes place in the application layer. |
| (2b): User Identity Authentication takes place between the UE and what entity (e.g. AAA Server)? | Nokia: AMF triggered Authentication/Authorization takes place between UE, AMF, and AUSF/UDM. SA3 shall consider authentication with AAA-S Nnsaaf Authentication, ARPF (UDM) Nudm Authenticate, AF Naf Authentication.  [LGE] AAA Server via NSSAAF or UDM via AUSF.  [InterDigital] AAA Server  [Lenovo] Re-use the secondary authentication procedure during PDU session establishment/modification  [ZTE] similar with Nokia  [Ericsson] Authentication triggered at login using interface towards the entity managing the UIP e.g. UIP server outside 5GC while within HPLMN trust domain  [OPPO] an AAA Server hosted by operator is a reasonable option.  [CATT] AAA Server may be used.  [Deutsche Telekom] AAA Server.  **[Samsung]** Can be specific to what SA3 decides.  -If specifically done by the network, it can be done between UE and the AAA server  -If the network is only to be notified about the active user of the UE/or if the user is active, then authentication can be performed locally by the UE (based on pre-configuration between the UE and the network), and UE just indicates the active user to the network..  [HW] between UE and AUSF/UDM when the user id credential is stored in UDM/UDR, or between the UE and AAA server deployed by the operator or the 3rd party, when the user id credential is stored in AAA server.  [NEC] between UE and the AAA-S |
| (2b) Rapporteur Summary: | 12 Companies Replied.  8 companies expressed a preference that the User Identity Authentication takes place between the UE and a AAA-S.  3 companies also expressed that the User Identity Authentication takes place between the UE and a the AUSF/UDM.  2 companies are open to AUSF/UDM and AAA-S but the answer depends on other factors.  1 company expressed a preference that the User Identity Authentication takes place between the UE and a UIP server. |
| (2c): To what degree does SA2 specify the authentication procedure (e.g. SA2 says that it takes place via control plane/EAP or over the user plane and SA3 defines the rest, etc.)? | Nokia: SA2 shall specify which human User identifiers and UE identifiers are used for Authentication/Authorization) and when (i.e. as part of the association of a human User with the UE). This also includes the Network Functions that are involved (e.g. UE, AMF, and AUSF/UDM when the Registration procedure is selected for the association).  SA3 shall consider authentication with AAA-S Nnsaaf Authentication, ARPF (UDM) Nudm Authenticate, AF Naf Authentication. So, it is left to SA3 how the authentication procedures are carried out.  [LGE] Authentication via control plane.  [InterDigital] EAP based Authentication via control plane.  [Lenovo] We do not see any need for SA3 involvement if we re-use the the secondary authentication procedure during PDU session establishment/modification  [ZTE] Control plane. The split between SA2 and SA3 follows the existing principle, such as the Registration procedure.  [Ericsson] Depends on solution and can be agreed in co-operation with SA3, and SA2 should not duplicate procedures in other stage 2 WGs like SA3.  [OPPO] SA2 specifies high level procedure, e.g. when will the authentication happen in the call flow, and what entities will be involved. The details about authentication, including encryption algorithms should be in SA3 regime.  [CATT] SA2 should specify during which procedure (e.g. PDU session or registration) authentication is required and what information could be used for authentication, and the detailed authentication procedure is left to SA3.  [Samsung] Solutions can at least be specified in details in the TR, and those solutions can be referred by SA3 in order to perform their normative work.  [HW] SA2 specifies the generic procedure and mechanism, and can leave the details on how to execute the authentication to SA3.  [NEC] Control plane |
| (2c) Rapporteur Summary: | 11 Companies Replied.  7 companies expressed a preference that the authentication procedure take place via the control plane.  4 companies provided good input but did not express a clear control plane / user plane preference.  At least 7 companies seem to agree that SA2 specifies or re-uses high level procedures and further details can be developed by SA WG3. |
| (2d): Once a user is authenticated, what NF(s) need to enforce any restrictions on the user? What are restrictions based on (e.g. information in the user profile)? | Nokia: AMF, SMF and PCF. The SDM data (combination of UE Subscription data and User Profile data) provided by UDM is used for the enforcement procedures.  It is assumed that selective User profile information is stored in the UDR. This allows to enforce any restrictions in a flexible way as policies and rules via the PCF to SMF.  [LGE] The UDM ensures only one user is activated for a UE at a given time.  [InterDigital] The AMF can enforce 1 active user per UE. The SMF or PCF can enforce restrictions that based on information from the User Profile.  [Lenovo] For session related policies SMF and SM-PCF use the user profile information available in , SM subscription data and Policy control subscription data  [ZTE] UDM can ensure only one active UE. PCF generate the PCC rule related to the active User, and SMF enforce the PCC rule.  [Ericsson] PCF using existing procedures and with some new information  [OPPO] The enforcement NFs could be AMF, SMF and PCF. The restrictions could be based on, e.g. user state, the number of active user identifiers, etc.  [CATT] UDM can ensure only one active UE. PCF generate the PCC rule related to the active User, and SMF enforce the PCC rule.  [Deutsche Telekom] Future proof solution that can be easily extended to multiple users per UE in future releases needs to be considered (PCF or UDM based?).  [Samsung] Depends upon the particular scenarios what specific restrictions they may be, but UDM/PCF can be used to enforce restrictions.  [HW] AMF and/or SMF, depending on the type of restriction, e.g. if it is to restrict whether the user is allowed to access this UE, then could be performed by AMF based on the link between the UE and user id, or if it is to restrict whether this DNN is allowed for this user, then by SMF, because the AMF only checks whether this DNN is allowed for the UE or not, and the DNN can be allowed for the UE but may not be allowed for the user.  [NEC] AMF  [Xiaomi], prefer UDM |
| (2d) Rapporteur Summary: | 11 Companies Replied.  5 responses are interpreted to mean that restrictions on the user can be based on information that is stored in the user profile.  5 companies indicate that the AMF has some involvement in enforcing restrictions on the user.  6 companies indicate that the SMF has some involvement in enforcing restrictions on the user.  6 companies indicate that the PCF has some involvement in enforcing restrictions on the user.  4 companies indicate that the UDM has some involvement in enforcing restrictions on the user.  The replies seem misaligned because the question was too generic. The question asked about restrictions on the user. One type of restriction relates to QoS of a PDU Session. Another type of restriction relates to the number of active users. It is natural that different restrictions are enforced by different NFs.  There seems to be consensus that the PCF generates PCC Rules based in the user. Most companies seem to agree that the PCF bases the PCC Rules on information from the User Profile.  There also seems to be some support for the UDM being involved in the enforcement of the restriction that only one user is active with a subscription at a time. |
| (2e): At SA #162, what Key Issue #2 solution principles are agreeable for an interim / partial conclusion? | Nokia: We strongly consider having the User details being fetched, authenticated, and authorized during the Registration procedure. The UDM takes a decision and provides the SDM response as being provided currently, but also additionally considering the User Identity profile parameters; this method allows greater flexibility while not bringing more interface changes.  [InterDigital] The AMF or SMF triggers authentication. The user is authenticated by a AAA Server via EAP based Authentication over the control plane.    [Lenovo] Re-use the secondary authentication procedure during PDU session establishment/modification  [ZTE] see answer to 2b)  [Ericsson] None  [OPPO] OPPO proposes to agree on some high-level solution principles, and then move into specific principles. We provided a paper on the framework of solution principles for agreement.  [CATT] Need to discuss during which procedure (e.g. PDU session or registration) authentication is required and what information could be used for authentication.  [Samsung] UE can be triggered to perform User authentication via NAS. AMF can trigger the user authentication (either by passing a NAS container from other NF transparently, or specifically sending an NAS indication).  [HW] need to decide whether to impact the registration procedure or to define the new procedure or to reuse the PDU session procedure to authenticate the user id. |
| (2e) Rapporteur Summary: | 9 companies replied to question 2e, 12 companies replied to key issue #2 questions.  The following principles seem to have a noticeable level of support.   * There seems to be consensus that the PCF generates PCC Rules based in the user. Most companies seem to agree that the PCF bases the PCC Rules on information from the User Profile. * There also seems to be some support for the UDM being involved in the enforcement of the restriction that only one user is active with a subscription at a time.   7 companies expressed a preference that the authentication procedure take place via the control plane. There is not consensus on whether the control plane procedure is based on PDU Session Establishment or Registration.  Proposal: Document the 2 bullets above in TR 23.700-32 as an intermediate conclusion. |

**Key Issue #3**

|  |  |
| --- | --- |
| (3a): How is user profile information and functionality exposed (e.g. NEF APIs)? | Nokia: Yes, NEF APIs  [LGE] By using NEF service.  [InterDigital] NEF APIs.  [ZTE] NEF API  [Ericsson] depends on usage, but currently we do not see the need to expose information specified by SA2  [OPPO] Yes, through NEF APIs.  [CATT] NEF API.  [Deutsche Telekom] NEF APIs.  [Samsung] NEF APIs can be used.  [HW] via NEF APIs  [Xiaomi] NEF AIPs |
| (3a) Rapporteur Summary: | 9 Companies Replied.  8 companies expressed a preference that exposure be achieved via NEF APIs.  1 company questioned whether exposure is needed. |
| (3b): What user profile information can be exposed (e.g. linked subscription identifiers)? | Nokia: User profile information and to which UE the User Identity is linked can be exposed to a trusted AF or to a linked AF (as per the User Profile Information).  Privacy protections shall be discussed with SA3.  [LGE] Authentication result, Activated User Identifier, GPSI of linked subscription.  [InterDigital] Authentication Results. The User Identit(ies) that are linked to a GPSI. The GPSI(s) that are linked to the User Identity.  [ZTE] User profile, linkage and activation information can be exposed.  [Ericsson] depends on usage, but currently we do not see the need to expose information specified by SA2  [OPPO] Most of user profile information can be exposed to 5GS NFs. But only Authorization/authentication results along with User Identifiers could be exposed to 3rd parties.  [CATT] All the examples in the KI description could be exposed, but requires confirmation from SA3 if there is any privacy issue.  [Deutsche Telekom] tbd.  [Samsung] Need to justify use cases if the purpose of the exposure is to obtain specific information out (like linked GPSIs) from the User profile or authentication result history for a specific UE.  [HW] at least the authentication result for the user ID.  [Xiaomi] after authorized, all the content of user profile can be exposed, and authentication/authorization results |
| (3b) Rapporteur Summary: | 9 Companies Replied.  6 companies seem to express support for exposing exposure of the content of the user profile, linkage information, and exposure of authorization/authentication results. Multiple companies indicated that privacy concerns need to be checked with SA WG3, this consideration is also documented in the key issue. |
| (3c): What user profile functionality can be exposed (e.g. the ability to check if a user is actively using a subscription)? | Nokia: User to UE association, UE to a User association may be provided when providing the query for a User or for a UE; this shall be only to a trusted AF or a linked AF. Authentication and Authorization results for the User, Group of Users, or even UE could also be exposed.  [InterDigital] An API that allows the AF to check if a user identity is actively using a subscription that is identified by a GPSI.  [ZTE] User profile provisioning, Link, status checking  [Ericsson] depends on usage, but currently we do not see the need to expose information specified by SA2  [OPPO] The User State/Status, e.g. active, inactive, suspended  [CATT] Authentication result and linked GPSI.  [Deutsche Telekom] tbd.  [Samsung] Following can be considered:   1. Pushing QoS related polices for a specific User ID, which can be applied to the particular UE on which the corresponding User Identifier is currently active/linked. 2. Ability to get Authentication result for a particular User Identifier.   [HW] subject to the scenarios |
| (3c) Rapporteur Summary: | 8 Companies Replied.  6 of the responses are interpreted to be supportive of an API that exposes whether a user identity is currently active with a subscription. |
| (3d): At SA #162, what Key Issue #3 solution principles are agreeable for an interim / partial conclusion? | Nokia: User Profile information and the associations shall be exposed. Trusted AF and linked AF for a User Identity or UE shall be considered. For providing the Authentication or Authorization results, NEF shall rely on the NWDAF/DM and shall not impact or interface with transactional NF – UDM.  [InterDigital] User Profile information and functionality are exposed via NEF APIs. The following APIs and functionality can be exposed:   * An API allows the AF to request that a user identity be linked with a GPSI. * An API that provides the User Identit(ies) that are linked to a GPSI. * An API that provides the GPSI(s) that are linked to the User Identity * An API that allows the AF to check if a user identity is actively using a subscription that is identified by a GPSI.   [ZTE] User profile provisioning, Link, status checking  [Ericsson] None  [OPPO] OPPO proposes to agree on some high-level solution principles, and then move into specific principles. We provided a paper on the framework of solution principles for agreement.  [CATT] Need to discuss what information can be exposed and for what purpose.  [Samsung] A third party (acting as AF) can request for User Authentication/Authentication Result for a specific User Identity (identified by a User Identifier) using NEF exposure.  [HW] open for discussion  [Xiaomi] can be discussed, but may not ready for agreement |
| (3d) Rapporteur Summary: | 8 companies replied to question 3d, 7 companies replied to key issue #3 questions.  The following principles seem to have a noticeable level of support.   * exposure be achieved via NEF APIs. * Some user profile content can be exposed but what is exposed should be checked with SA WG3. * authorization/authentication results can be exposed but what is exposed should be checked with SA WG3. * an API can expose whether a user identity is currently active with a subscription but what is exposed should be checked with SA WG3.   Proposal: Document the 4 bullets above in TR 23.700-32 as an intermediate conclusion. |