ETSI TR 122 904 V18.0.1 (2024-05)

5G;
Study on user-centric identifiers and authentication
(3GPP TR 22.904 version 18.0.1 Release 18)

Reference
RTR/TSGS-0122904vi01

Keywords
5G

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Legal Notice

This Technical Report (TR) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities. These shall be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between 3GPP and ETSI identities can be found under https://webapp.etsi.org/key/queryform.asp.

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Contents

Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

1 Scope

The present document aims to study the introduction of an optional, user-centric authentication layer on top of the existing subscription authentication, supporting various authentication mechanisms and interactions with external authentication systems as well as a degree of confidence (i.e. a value that allows differentiated service policies depending on the reliability of the User Identifier).

The new authentication layer shall not replace existing subscription credentials. The security and privacy of subscriber or end user data shall not be compromised.

Use cases are developed and potential requirements derived how to use the new User Identifier within the 3GPP system e.g. to provide customized services and enhanced charging and how to provide this identifier to external entities to enable authentication for systems and services outside 3GPP.

Use cases for use within 3GPP include

- providing different users using the same UE with customized services
- identifying users of devices behind a gateway with a 3GPP subscription, but without the devices having a dedicated 3GPP subscription
- using a User Identifier being linked to a subscription to access 3GPP services via non-3GPP access
- using a User Identifier for slice authorization.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in 3GPP TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in 3GPP TR 21.905 [1].

Gateway UE: a UE, which acts as a gateway providing access to and from the 3GPP network for one or more non-3GPP devices that are connected to the gateway UE.

User: As defined in TR 21.905 [1]: An entity, not part of the 3GPP System, which uses 3GPP System services. Example: a person using a 3GPP System mobile station as a portable telephone.

Additional examples for a user in the context of this TR: a non-3GPP device connected to the 3GPP system via a gateway, or an application running on a UE.

User Identity: information representing a user in a specific context. A user can have several user identities, e.g. a User Identity in the context of his profession, or a private User Identity for some aspects of private life.

User Identifier: a piece of information used to identify one specific User Identity in one or more systems.

User Identity Profile: A collection of information associated with the User Identities of a user.

4 Overview

4.1 Background and motivation

Current mobile networks are subscription-centric, which allows mobile operators to protect the access to the network and respect legal obligations. From a use case perspective this was sufficient in times when a user typically only had one phone with one subscription, using only a few services provided by the operator such as telephony and SMS.

However, times have changed: Today a person may have different kinds of devices (phones, tablets, laptops), some of which might belong to the user, others might be shared with someone else or belong to some other party to access various operator and non-operator services. Things are increasingly connected (sensors, gateways, actuators etc.) and there are many different flavours in the relation between the owner of the thing, the holder of the subscription and the actual user of the thing.

Presently it is common for each service to perform its own authentication, often based on username and password. For users it becomes more and more cumbersome to manage the different credentials of the growing number of services.

So-called identity providers address the above problem by providing identity information to entities and authentication to services for those entities. Such mechanisms could be used over the top of any data connections, but integration or interworking with operator networks provides additional advantages.

Identifying the user in the operator network (by means of an identity provided by some external party or the operator) enables to provide an enhanced user experience and optimized performance as well as to offer services to devices that are not part of 3GPP network. The user to be identified could be an individual human user, using a UE with a certain subscription, or an application running on or connecting via a UE, or a device (“thing”) behind a gateway UE.

Network settings can be adapted and services offered to users according to their needs, independent of the subscription that is used to establish the connection. By acting as an identity provider the operator can take additional information from the network into account to provide a higher level of security for the authentication of a user.

4.2 Basic concept and relations of identity management

In the context of identity management something outside a system that needs to be identified in the system is referred to as “entity”. In 3GPP such an entity is called a user. A user is not necessarily a person, it could also be an application or a device (“thing”).

The entity is uniquely represented by an identity in the system. The identity can dependent on the role of the entity in the system (e.g. which kind of service is used for which purpose). As such, a user can have several user identities – e.g. one user identity representing the professional role of the (human) user and another one representing some aspects of her private life. There is a 1:n relation between user and user identity.

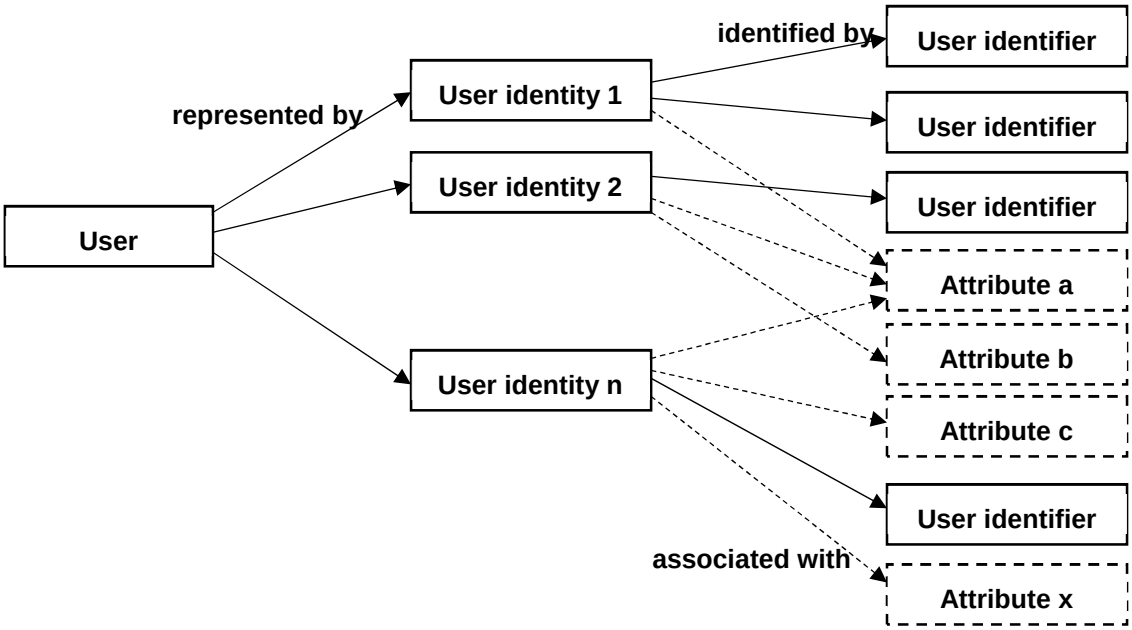

Figure 1: relation between user, identities, identifiers and attributes

A user identity is associated with some pieces of information, which are generally called attributes. One special form of attributes are identifiers. The relation between identity and identifier is 1:n.

Each user identity is identified in the system by one or more user identifiers. An identifier could take the form of an NAI, email address or some number, could be permanent (comparable to the IMSI), or temporary (comparable to the TMSI).

E.g., in the internet-world a user might choose to use her company email address when registering and using services (access to web portals) that she needs for her work. For access to other sites, e.g. online shopping or login to information servers concerning some hobby, she might use other email addresses. In this example the email addresses are the user identifiers that identify the different identities of the user for certain web services.

Other attributes could contain information about the date of birth of a user, the private address, the company name and address, job title etc. Attributes that are no identifiers may be associated with more than one identity, e.g. date of birth might be relevant in the professional as well as in the private context. One identity typically is associated with several attributes.

With having multiple user accounts the above information is distributed over multiple servers. An identity provider creates, manages and stores this information in one place, authenticates a selected user identity (i.e. verifies a claimed user identity) for a service and provides the result and necessary attributes to the service.

4.3 Impact on the 3GPP system

The goal of this activity is not to define an identity provisioning service. The assumption is that operators can use existing systems to act as identity providers if they wish to do so. The actual process of identity creation, provisioning, managing, authentication etc. does not need to be defined within 3GPP.

The focus of this work is the interaction of such a service with the 3GPP system:

- how to take a user identity into account for adapting network and operator-deployed service settings (e.g.policies, IMS, Gi-LAN service chain) and for network slice selection

- support of providing the user identity to external services via the 3GPP network

- extending 3GPP services to non-3GPP devices that are identified by user identifiers, e.g. to enable network and service access by these devices and to make them addressable and reachable from the network

- additionally, if the operator acts as identity provider, how to improve the level of security or confidence in the identity by taking into account information from the network

5 Use cases

5.1 Several users sharing one UE

5.1.1 Description

Different users can share one UE. To improve the user experience it would be beneficial to automatically change settings of operator deployed services according to the users' settings.

This requires the user to be identified in addition to the existing identification of subscription.

5.1.2 Pre-conditions

Lucy and Linus live at their parents' home and use their mother's tablet PC (actually a UE) mainly to surf the web.

The mother is subscriber of operator TTT who has deployed some child protection service (web filter).

Both Lucy and Linus have a user account at operator TTT. The user account contains some User Identifier and specific service settings.

The tablet is configured in a way that Lucy and Linus can use it with their accounts.

5.1.3 Service Flows

Linus unlocks the tablet using the fingerprint sensor. Due to this the UE (tablet) selects Linus' user account and triggers a user authentication procedure towards operator TTT.

Linus is successfully authenticated over the 3GPP network. He starts to surf the web. Based on the user specific configuration stored in or linked with his user account the operator's web filter is configured according to Linus' needs to prevent him from receiving inappropriate content.

For a while Linus is distracted and does not use the tablet. After 5 minutes of inactivity it automatically enters the locked mode and the user account is deactivated.

When he picks up the tablet again, he can quickly reactivate. For example, for the first log in after a long time a two-step authentication may be needed, but now one step is sufficient.

After a while, Linus wants to call the neighbour kid, Charlie. Instead of searching his own UE, which is hidden under a blanket in his room, he calls from the tablet. The network's communication settings are according to his user account settings and so Charlie sees an incoming call with Linus' User Identity. Charlie answers the call and they decide to meet outside for playing baseball.

Linus leaves the house. Now Lucy picks up the tablet and unlocks it. Her user account is selected and she is authenticated by the network. The service settings including the web filter are reconfigured according to Lucy's account settings.

5.1.4 Potential Requirements

[PR 5.1-1] The 3GPP system shall be able to provide a User Identifier to a user. The User Identifier shall be independent of existing identifiers relating to subscription (e.g. IMSI, MSISDN, IMPI, IMPU, SUPI, GPSI). The User Identifier may be provided by some entity within the operator's network or by a 3rd party.

[PR 5.1-2] The 3GPP system shall support a mechanism to perform authentication of a User Identity, regardless of the access, the UE and its HPLMN as well as the provider of the User Identifier.

[PR 5.1-3] The 3GPP system shall be able to store or link user specific service settings and parameters with the User Identifier. Those shall include network parameters (e.g. QoS parameters), IMS service (e.g. MMTEL supplementary services) and operator deployed service chain settings.

[PR 5.1-4] The 3GPP system shall be able to take user specific settings into account when delivering a service.

[PR 5.1-5] The operator shall be able to enable or disable the use of a User Identifier in his network.

[PR 5.1-6] The operator shall be able to set the boundaries within which the user specific settings are taken into account in his network. The operator shall be able to restrict the feature depending of the provider of the User Identifier, the roaming status of the UE, the service and its specific parameters.

[PR 5.1-7] The operator shall be able to restrict the number of simultaneously active User Identifiers per UE.

[PR 5.1-8] The user shall be able to activate and deactivate the use of the User Identifier and the associated user account settings. With deactivation all links between a subscription and a certain User Identifier shall be erased.

[PR 5.1-9] The 3GPP system shall be able to include the User Identifier in the charging data for on- and offline charging.

[PR 5.1-10] The 3GPP system shall be able to support automatic deactivation of an active user identity after a certain period of time of inactivity, as configured by the operator.

[PR 5.1-11] The 3GPP system shall be able to support a fast activation mechanism, based on MNOs' configuration.

5.2 Identity provisioning to external services

5.2.1 Description

With the option to identify the user the 3GPP system can support an operator to act as identity provider and enable auto-log-in and single-sign-on to operator and non-operator services.

This use case is an enhancement of functionalities described in the use case in clause 5.1 and the potential requirements are in addition to those described in clause 5.1.4.

5.2.2 Pre-conditions

Dorothea is a subscriber of operator TTT. She also has a user account at operator TTT. She is logged in on her UE with her user account and her User Identity has been authenticated over the 3GPP system, using a strong authentication mechanism.

Dorothea also owns a bank account and has referred to her TTT user account when registering to the bank's online services.

5.2.3 Service Flows

Dorothea uses her UE for online banking for which the bank requires strong user authentication. As she has already been authenticated by the 3GPP system there is a high level of confidence with regard to her identity. This level of confidence is increased by the fact that Dorothea uses her own UE from the location of her home address and was authenticated less than 1 minute ago when unlocking her UE.

Based on application layer information transferred by the 3GPP system, the banking system accepts her request to access her banking account without further need for Dorothea to provide additional credentials.

As later on Dorothea places an order to the bank for a money transfer, the bank however requests her strong re-authentication by the 3GPP system so as to ensure that she is still the actual user behind the UE, which is achieved by having Dorothea re-authenticating by operator TTT, e.g. over the fingerprint sensor of the UE.

5.2.4 Potential Requirements

[PR 5.2-1] The 3GPP system shall be able to support operators to act as identity provider and to authenticate users for accessing operator and non-operator deployed (i.e. external non-3GPP) services.

[PR 5.2-2] The 3GPP system shall be able to provide information to services concerning the level of confidence of the User Identity and authentication process.

[PR 5.2-3] The 3GPP system shall be able to assess the level of confidence of the User Identity and authentication process by taking into account information regarding the used authentication mechanism (e.g. algorithms, key-length, time since last authentication), information from the network (e.g. UE or device in use, access technology, location).

[PR 5.2-4] The 3GPP system shall protect the privacy of the user by only transferring information that is necessary to provide the service and the user has consented when registering for the service.

5.3 Use case of Authorizing Others to Access One's Resources

5.3.1 Description

One user manages some kind of resources such as a home video camera and others may want to access it. Only users that are authorized by the manager are able to access the managed resources and the manager knows in real time who is accessing the resources. Thus the manager needs to know who the visitor is to be able to authorize him.

5.3.2 Pre-conditions

A Video camera (Ax) is installed at Tom's house and Tom is responsible to configure and manage it.

Camera (Ax) has an eSIM and is subscribed to MNO X's 5G service. The camera has an integrated web server and is configured to inform the manager when somebody wants to access and this is only allowed when the manager authorizes it.

Tom's mobile phone uses MNO X's service and Tom has a profile on MNO X's system. Tom's profile contains information that he is the owner of camera Ax and that for accessing the camera's web server a certain authentication method and security level (e.g. finger print or face scanning) is needed as well as the use of his UE (e.g. identified by IMSI and IMEI).

Jenny, Tom's cousin, uses MNO Y's service and has a profile on MNO Y's system. Jenny's profile also contains information concerning the necessary authentication method and security level as well as which UE she uses (e.g. identified by IMSI and IMEI).

Tom has a new baby recently and many relatives would like to have a look at the cute baby via cameras remotely.

Note: Jenny could also use MNO X's service, the same with Tom, then in this case the process happens only in the MNO X's system. Thus no requirement for system inter-operation is wanted.

5.3.3 Service Flows

a) Jenny wants to see the new baby so she keys in the website of the camera on her phone.

b) The camera Ax gets the request with Jenny's User Identity and securely informs Tom about the request. .

c) Tom gets it and requests authentication from the 3GPP system.

d) The system authenticates Jenny and returns the result.

e) After the successful authentication of Jenny Tom authorizes her to access the video from the camera.

f) The 3GPP system records the charging data for the authentication request.

5.3.4 Potential Requirements

[PR 5.3-1] The 3GPP system shall be able to store a User Identity Profile, which can include the following information

- User Identifiers,

- used UEs (identified by their subscription and device identifiers),

- the capabilities the used UEs support for authentication,

- information regarding authentication policies (required authentication mechanism and level of confidence) for different services.

[PR 5.3-2] The 3GPP system shall be able to authenticate the User Identity according to the authentication policies.

[PR 5.3-3] The 3GPP system shall be able to record charging data for user authentication.

5.4 Slice authentication by 3rd party

5.4.1 Description

A gaming company provides 3 tiers of service, bronze, silver, gold, to its subscribers who can then login to play games with different capabilities (e.g., QoS). The gaming company provides its own devices to gamers, each of which has a subscription with the local MNO. Each device is capable of supporting multiple users where each user has a separate subscription with the gaming company.

The gaming company leases 3 slices, each with appropriate resources, from the MNO to support the three tiers of service. The MNO know the gaming company UEs are authorized to gain access to the gaming company slices but the MNO does not manage which exact slice a UE is entitled to use for each access attempt. The gaming company maintains its own database indicating which tier of service is allowed for each subscriber. This allows changes to the tier associated with a particular UE, which may be based on changes in the user's gaming company subscription (e.g., user changes subscription option or company offers a short term promotion) or on a change of user using the device who has a different subscription option, to be transparent to the MNO. This also allows users to login on different gaming devices and get the same service regardless of device.

Any gaming company subscriber can login to the gaming device with the gaming company user ID and credentials, which causes a new network access attempt to be initiated by the gaming device. Access authentication is then performed by the MNO on the UE credentials of the gaming device. Based on the network awareness that the UE is associated with the gaming company, before the UE is attached to a particular slice, the gaming company is requested to perform a second authentication and authorization of the user which determines the appropriate slice for the UE based on the subscription option for the current user.

5.4.2 Pre-conditions

The gamer has a silver subscription with the gaming company.

The gamer receives a gaming device from the company which includes a subscription with the local MNO.

The gaming company maintains the association of the subscription with the slice for silver service.

5.4.3 Service Flows

The gamer logs onto the gaming device with the gaming company credentials

Based on the new access attempt, the gaming device is authenticated by the network as having a valid subscription with MNO.

The network determines the device also has a subscription with the gaming company that requires an interaction with a gaming company entity to determine what slice it should attach to.

The network requests the gaming company to authenticate the user and determine the appropriate slice. After authenticating the user, authorization for the gaming device to access the silver slice is conveyed to the network.

The gaming device is connected to the gaming company slice for silver service.

5.4.4 Potential Requirements

[PR 5.4-1] The 3GPP system shall support a mechanism to determine whether 3rd party authentication is needed for slice assignment.

[PR 5.4-2] The 3GPP system shall support a mechanism to interwork with a 3rd party network entity to authenticate the user and authorize the UE for slice access.

[PR 5.4-3] The 3GPP system shall support a mechanism to receive a slice authorization from a 3rd party network entity.

5.5 Secondary slice authentication by 3rd party – failure case

5.5.1 Description

This use case follows the same description as the use case in clause 5.4.

5.5.2 Pre-conditions

The gamer has a silver subscription with the gaming company.

The gamer receives a gaming device from the company which includes a subscription with the local MNO.

The gaming company maintains the association of the subscription with the slice for silver service.

The gamer's younger brother does not have a subscription with the gaming company.

5.5.3 Service Flows

The gamer's younger brother picks up the device and turns it on.

Based on the new access attempt, the gaming device is authenticated by the network as having a valid subscription with MNO.

The network determines the device also has a subscription with the gaming company that requires a secondary authentication to determine what slice it should attach to.

The gaming company attempts to authenticate the device user and determines that the current user does not have an active subscription (e.g., based on receiving invalid user credentials from the younger brother).

The gaming device is not connected to the gaming company slices.

5.5.4 Post-conditions

Based on operator policy, subscription options of the gaming device, and device capabilities (e.g., it is also a smartphone), the device may be denied service or it may be connected to another part of the network, where, for example, the younger brother could make a voice call using the device which has been successfully authenticated for network access.

5.5.5 Potential Requirements

[PR 5.5-1] The 3GPP system shall be able to store a User Identity Profile for a user, which can include the following information:

- information regarding authentication policies required by different slices to authenticate a User Identity for access to these slices.

[PR 5.5-2] The 3GPP system shall support a mechanism to interact with a 3rd party network entity for User Identity authentication.

[PR 5.5-3] The 3GPP system shall support a mechanism to deny a UE access to a slice based on unsuccessful User Identity authentication, while still allowing access to other services associated with the UE subscription.

5.6 Updating user account based on authorization from 3rd party

5.6.1 Description

A gaming company provides two kinds of services, default service and enhanced service, to its game players. Comparing to the default service, the enhanced service could provide better game experience, e.g., lower latency, higher data rate. The gaming company leases 2 slices, each with appropriate resources, from the MNO to support the two tiers of service.

A game player could online purchase the enhanced service, e.g., via the game application provided by the game company. Then the game player could either use his own smartphone or other's one, to access the MNO's slice that providing enhanced service. The game player will enjoy the game with better game experience.

5.6.2 Pre-conditions

The gaming company leases 2 slices, each with appropriate resources, from MNO(s) to support default service and enhanced service, respectively.

A game player Andy has a user account at the MNO. The user account contains the User Identifier and specific service settings and parameters. In this case, the user account contains the information that allow 3GPP network to permit Andy to access the slice for default service, but not the slice for enhanced service.

5.6.3 Service Flows

Andy logs on the game by using his smartphone. Andy is successfully authenticated by the MNO's network, and allowed to access the slice for default service according to the user account.

Andy plays the game for a while. He is a little annoyed since the network lag impacts his gaming skills.

Andy online purchases the enhanced service by using the game app provided by the gaming company.

The MNO updates Andy's user account according to the authorization of the gaming company, i.e., the information in the user account now allows the 3GPP network to permit Andy to access the slice for enhanced service.

Andy's smartphone now is connected to the slice for enhanced service. Andy spends a very happy gaming time as there is no annoying lag anymore.

Later, Andy uses his friend Bob's smartphone to start the game. As Andy's purchased enhanced service as well as the information in the user account are still valid, if allowed by the MNO of Bob's smartphone according to the agreement between the game company and the MNOs, Andy could enjoy the game by using Bob's smartphone, via the slice for enhanced service.

5.6.4 Potential Requirements

[PR 5.6-1] The 3GPP system shall be able to store and link User Identity Profile with the User Identifier. The User Identity Profile shall include specific network parameters (e.g., QoS parameters), and/or specific network resources (e.g., network slice).

[PR 5.6-2] The 3GPP system shall be able to update the User Identity Profile related to a User Identifier, according to the information shared by a 3rd party.

[PR 5.6-3] The 3GPP network shall be able to take the User Identity Profile into account when assigning a UE to a network slice, moving a UE from one network slice to another, and removing a UE from a network slice.

5.7 Several users or devices behind one gateway UE

5.7.1 Description

One or more devices (IoT, wearables etc.) without own subscription can be connected via gateway UEs to the network. With the option to identify the devices (users) behind the UE (gateway) the 3GPP system can act as identity provider, enable auto-log-in and single-sign-on as well as change settings in the operator's network to enable the best user experience.

This use case is an enhancement of functionalities described in the use cases in clauses 5.1 and 5.2. The potential requirements are in addition to the requirements described there.

5.7.2 Pre-conditions

Rosy has some serious health condition. She regularly uses a portable ECG, which records her heart rate and function and is able to transmit the data to a medical centre, using a UE as a gateway.

For medication, amongst others, she uses a connected inhaler. It tracks the medication use and can also transmit data to Rosy's medical centre, again over a gateway UE.

Finally for her own information she has a smart watch that measures her heart rate at the wrist, counts her activity during the day etc. The data from the smart watch can be synchronized with her smart phone and a cloud service from time to time.

Rosy has got a user account at operator TTT. Rosy is subscriber of operator TTT with her UE, her husband Joseph is subscriber of operator ONO.

Rosy paired all her medical devices and wearables with her smart phone.

5.7.3 Service Flows

Rosy registers at the medical centre, referring to her user account at operator TTT, as well as for the smart watch cloud service. So her account is updated with a User Identifier for Rosy's ECG, another one for Rosy's inhaler and third one for Rosy's watch.

Rosy wears her ECG. The ECG establishes a data connection to the network via the smart phone as a gateway UE. This triggers the authentication process with operator TTT and enables the log-in at the medical centre, as Rosy's ECG. The network provides the necessary resources (guaranteed bitrate) to enable a reliable real time transmission of ECG data.

In parallel Rosy uses her smart phone to synchronize her smart watch with the cloud service. Credentials derived from her watch identifier in her user account are used to log in. The data are exchanged on a best effort basis (i.e. there is no guaranteed bitrate).

After some time Rosy takes off the ECG, the data transmission is stopped and the device logged out from the service.

A bit later Rosy's smart phone needs re-charging. As she has to leave the house she takes the UE of her husband Joseph with her. Her devices (i.e. the smart watch and the inhaler) are paired with this phone because she had already done the configurations earlier.

When Rosy uses her inhaler it connects to the medical centre via Joseph's UE, and is logged in as Rosy's inhaler, because of the previous user authentication over the 3GPP system.

5.7.4 Potential Requirements

[PR 5.7-1] The 3GPP system shall be able to provide a User Identifier for a non-3GPP device that is connected to the network via a UE that acts as a gateway.

NOTE 1: The user identified with a User Identifier could be a person, a device or an application.

[PR 5.7-2] The 3GPP system shall support a mechanism to perform authentication of a User Identity used by devices that are connected via a UE that acts as a gateway.

NOTE 2: The above requirements are additional requirements to those described in clause 5.1, especially those for storing and applying user specific settings within the 3GPP network and for operator deployed services as well as for charging.

5.8 Access via non-3GPP with a User Identity linked to a subscription

5.8.1 Description

Existing subscribers may want to add non-3GPP devices to their subscription to be able access the network and its services using these devices via non-3GPP access. By identifying the user and linking the User Identity to a subscription the 3GPP system can enable such scenarios.

This use case is based on functionality described in the use case in clause 5.1 and the potential requirements are in addition to those described in clause 5.1.4.

5.8.2 Pre-conditions

Dorothea is a subscriber of operator TTT with her UE and has a user account at operator TTT.

5.8.3 Service Flows

Dorothea buys a new tablet PC, equipped with WLAN. She wants to add this tablet PC to her subscription e.g. to be able to make phone calls with it.

She connects to the internet via WLAN and downloads the operator's communication client app. She logs in at the app with her user account and an authentication procedure is triggered towards operator TTT. As she uses her account from this tablet for the first time, some verification message is sent to Dorothea's UE, where she has to confirm, that she currently wants to link a new device with her subscription.

Dorothea confirms by entering her PIN or using the fingerprint sensor on her UE and the network downloads some credentials to the tablet that enable the tablet to access the operator's network and its services via WLAN. From now on, Dorothea can use the operator TTT communication services on her tablet, until the credentials are no longer valid (context-based, e.g. until the tablet is locked, after x minutes/hours/days, …). Furthermore, since Dorothea's user account contains some user-specific network service settings (e.g. add-blocking option, traffic encryption over VPN), those settings are automatically applied to the tablet PC's network connection.

She uses the tablet with the operator's communication client app to setup a call to her friend Martin, who sees her preferred alias that is linked with her account as incoming call identity. Therefore, he answers the call and they arrange to go out for sports together.

5.8.4 Potential Requirements

[PR 5.8-1] The 3GPP system shall be able to permanently link a user account with a subscription.

[PR 5.8-2] The 3GPP system shall support authenticating User Identities from devices that connect via the internet and securely downloading credentials to those devices to enable them to access the network and its services via non-3GPP access.

[PR 5.8-3] The 3GPP system shall support using aliases with a User Identity for 3GPP and non-3GPP services.

[PR 5.8-4] The 3GPP system shall be able to create charging data containing the User Identifier for access and use of network services by a device that was authorized with its User Identifier.

[PR 5.8-5] The operator shall be able to set restrictions for devices accessing the network and its services via non-3GPP access with their user account based on the User Identity provider, the roaming status of the device and the network service.

5.9 Services Configuration of Shared Devices

5.9.1 Description

This use case is based on the functionality described in clause 5.7.

Operators provide a variety of services which users might want to use from different devices. Some of these devices may be shared between several users. To improve the user experience a user should be able to configure which services are available on which devices.

5.9.2 Pre-conditions

- Jimbo and Ryder are two children of the family.
- Both of them live with their parents in the same house.
- A pad is shared in the family, which supports HD voice, HD video and surfing the internet.
- Both of them have their own UEs.

5.9.3 Service Flows

- Ryder uses the pad to watch movies and play somatic games. But he does not want to make calls and send messages from the pad.
- Ryder uses the pad to watch movies and play somatic games. But he does not want to make calls and send messages from the pad.
- Ryder logs in at the pad at home, for surfing the Internet. He can still send or receive phone calls, send or receive messages on his UE.
- Ryder can configure whether he wants to use data, telephone or message services on the pad.
- Jimbo wants to use voice and messaging services on the pad as well. After logging in, he can receive calls on the pad, using VoWiFi with the same service settings as he has for VoLTE.

5.9.4 Potential Requirements

[PR 5.9-1] The 3GPP system shall enable a user to configure, within the boundaries set by the network operator, which services shall be available on a device where a user logs in. These services include voice, video, and messaging.

[PR 5.9-2] The service settings shall be the same as if they were used from the user's UE.

6 Consolidated potential requirements

6.1 User Identifiers and user authentication

[PR 5.1-1 part 1] The 3GPP system shall be able to provide User Identities with related User Identifiers for a user.

[PR 5.1-1 part 2] The User Identifier shall be independent of existing identifiers relating to subscription or device (e.g. IMSI, MSISDN, IMPI, IMPU, SUPI, GPSI, IMEI) and of other User Identifiers.

[PR 5.1-1 part 3]The User Identifier may be provided by some entity within the operator's network or by a 3rd party.

[PR 5.4-2] The 3GPP system shall support to interwork with a 3rd party network entity for authentication of the User Identity.

[PR 5.1-2] The 3GPP system shall support to perform authentication of a User Identity regardless of the user's access, the user's UE and its HPLMN as well as the provider of the User Identifier.

[PR 5.7-1] The 3GPP network shall be able to provide a User Identifier for a non-3GPP device that is connected to the network via a UE that acts as a gateway.

[PR 5.7-2] The 3GPP network shall support to perform authentication of a User Identity used by devices that are connected via a UE that acts as a gateway.

[PR 5.1-4] The 3GPP system shall be able to take User Identity specific service settings and parameters into account when delivering a service.

[replacing PR 5.8-1] A subscriber shall be able to link and unlink one or more user Identities with his 3GPP subscription.

[PR 5.8-2] The 3GPP system shall support user authentication with User Identifiers from devices that connect via the internet; the 3GPP system shall support secure provisioning of credentials to those devices to enable them to access the network and its services according to the 3GPP subscription that has been linked with the User Identity.

[PR 5.2-3] The 3GPP system shall be able to assess the level of confidence in the User Identity by taking into account information regarding the used mechanism for obtaining that User iIdentity (e.g. algorithms, key-length, time since last authentication), information from the network (e.g. UE or device in use, access technology, location).

[PR 5.1-7] The operator and the subscriber shall be able to restrict the number of simultaneously active User Identifiers per UE.

6.2 Access to services

The 3GPP System shall support to authenticate a User Identity to a service with a User Identifier.

Note: The requirement applies to 3GPP services and non-3GPP services that are accessed via the 3GPP System

[PR 5.2-2] The 3GPP system shall be able to provide information to services concerning the level of confidence of the User Identity and authentication process.

[replacing PR 5.3-2] A service shall be able to request the 3GPP network to only authenticate users to the service for which the association of the user with a User Identifier has been established according to specified authentication policies of the service.

[replacing PR 5.3-2] When a user requests to access a service the 3GPP System shall support authentication of the User Identity with a User Identifier towards the service if the level of confidence for the correct association of a User Identity with a User Identifier complies to specified policies of the service.

[PR 5.6-3] The 3GPP network shall be able to take the User Profile into account when assigning a UE to a network slice, moving a UE from one network slice to another, and removing a UE from a network slice.

[merging PRs 5.4-1 and 3] The 3GPP system shall support to allow a UE access to a slice based on successful User Identity authentication.

[PR 5.5-3] The 3GPP system shall support to deny a UE access to a slice based on unsuccessful User Identity authentication.

6.3 Charging for services

[PR 5.1-9] The 3GPP system shall be able to include the User Identifier including information concerning the provider of the User Identifier in the charging data for on- and offline charging.

[PR 5.3-3] The 3GPP system shall be able to record charging data for user authentication.

[PR 5.8-4] The 3GPP system shall be able to create charging data containing the User Identifier and the 3GPP subscription to which it is linked for access and use of network services by a non-3GPP device that was authorized with its User Identifier linked to a 3GPP subscription.

6.4 User Identity Profile and its User Identities

[PR 5.3-1] The 3GPP system shall be able to store and update a User Profile for a user.

The User Profile shall include a User Identifier.

The User Profile may include one or more pieces of the following information:

- Additional User Identifiers of the user's User Identities and potentially linked 3GPP subscriptions,
- used UEs (identified by their subscription and device identifiers),
- capabilities the used UEs support for authentication,
- information regarding authentication policies required by different services and slices to authenticate a user for access to these services or slices.

[PR-5.1-3] User Identity specific service settings and parameters.
Those shall include network parameters (e.g. QoS parameters), IMS service (e.g. MMTEL supplementary services) and operator deployed service chain settings.

[PR 5.6-1] User Identity specific network resources (e.g., network slice).

[PR 5.1-8] The user shall be able to activate, deactivate and suspend, i.e. temporarily deactivate, the use of the User Identifiers per device or UE and the associated settings in its user profile.

Note 1: Suspending (temporarily deactivating) a User Identifier on a UE could also be automatically performed by the device on behalf of the user after a period of inactivity of the user at that device. The time period of inactivity of the user at that device after which a device should suspend a User Identifier may depend on home operator policy.

Note 2: Re-activation of a suspended User Identifier on a UE where it was suspended could involve simplified authentication (e.g. using fingerprint) at the device.

[PR 5.6-2] Subject to operator policy the 3GPP system shall be able to update User Profile related to a User Identifier, according to the information shared by a trusted 3rd party.

6.5 Operator requirements

[PR 5.1-5] The operator shall be able to enable or disable the use of a User Identifier in his network.

[PR 5.2-1] The 3GPP System shall support operators to act as User Identity provider and to authenticate users for accessing operator and non-operator deployed (i.e. external non-3GPP) services

[PR 5.1-6] The operator shall be able to set the boundaries within which the user specific settings are taken into account in his network. The operator shall be able to restrict the feature depending of the provider of the User Identifier, the roaming status of the UE, the service and its specific parameters.

[PR 5.8-5] The operator shall be able to set restrictions for devices accessing the network and its services via non-3GPP access with their User Identity linked to a 3GPP subscription. The 3GPP system shall support restrictions based on the User Identity provider, the roaming status of the linked 3GPP subscription, and the network service that is accessed.

[PR 5.9-1] The 3GPP system shall enable a user to configure, within the boundaries set by the network operator, which services shall be available on a device where a user logs in. These services include voice, video, and messaging.

6.6 Privacy requirements

[PR 5.2-4] The 3GPP system shall protect the privacy of the user by transferring to a service only User Identity information that is necessary to provide the service and for which the user has consented to when registering for the service.

Annex A (informative): Change history

Change history							
Date	**Meeting**	**TDoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
2018-02	SA1#81	S1-180007				TR Skeleton	0.1.0
2018-02	SA1#81	S1-180388				Addition of Scope	0.1.0
2018-02	SA1#81	S1-180389				Use case of several users sharing one UE	0.1.0
2018-02	SA1#81	S1-180392				Use case of identity provisioning to external services	0.1.0
2018-02	SA1#81	S1-180391				Use Case of Authorizing Others to Access One's Resources	0.1.0
2018-02	SA1#81	S1-180390				3rd party slice authentication	0.1.0
2018-02	SA1#81	S1-180577				Use case of several users or devices behind one relay UE	0.1.0
2018-02	SA1#81	S1-180011				Use case of linking a user identity to a subscription for access	0.1.0
2018-05	SA1#82	S1-181007				Editorial updates	1.1.0
2018-05	SA1#82	S1-181511				Definitions	1.1.0
2018-05	SA1#82	S1-181024				Overview	1.1.0
2018-05	SA1#82	S1-181514				Secondary slice authentication by 3rd party – failure case	1.1.0
2018-05	SA1#82	S1-181516				Services Configuration of Shared Devices	1.1.0
2018-05	SA1#82	S1-181686				Updating user account based on authorization from 3rd party	1.1.0
2018-05	SA1#82	S1-181684				Automatically De-register Function	1.1.0
2018-05	SA1#82	S1-181685				Proposed "Consolidated potential requirements"	1.1.0
2018-05	SA#80	SP-180339				MCC Clean-Up for presentation to SA	2.0.0
2018-06	SA#80	SP-180339				Raised to v.16.0.0 following SA's approval	16.0.0

Change history											
TSG SA#	**SA Doc.**	**SA1 Doc**	**Spec**	**CR**	**Rev**	**Rel**	**Cat**	**Subject/Comment**	**Old**	**New**	**WI**
SP-81	SP-180780	S1-182703	22.904	0001	2	Rel-16	B	Consolidation of potential requirements	16.0.0	16.1.0	FS_LUCIA

Change history							
Date	**Meeting**	**TDoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
2022-03	SA#95e	-	-	-	-	Updated to Rel-17 by MCC	17.0.0
2024-03	SA#103	-	-	-	-	Updated to Rel-18 by MCC (and issue with v.18.0.0 upload)	18.0.1

History

Document history		
V18.0.1	May 2024	Publication