TSGS#26(04)0727

Source: **SA1**

Title: **CRs to 22.127 to delete requirements from Rel-6**

Document for: **Approval**

Agenda Item: **7.1.3**

Meeting	SA Doc	TS No.	CR No	Rev	Rel	Cat	Subject	Vers. Current	Vers New	SA1 Doc
SP-26	SP-040727	22.127	072	-	Rel-6	F	Delete Requirements for User-Application Authentication functions”	6.6.0	6.7.0	S1-040920
SP-26	SP-040727	22.127	073	-	Rel-6	F	Delete Requirements for User Data Management (OSA support for GUP)”	6.6.0	6.7.0	S1-040921
SP-26	SP-040727	22.127	074	-	Rel-6	F	Delete Requirements for IP session function”	6.6.0	6.7.0	S1-040922

TSG-SA WG1 #26 **S1-040920**
Sophia Antipolis, France, 11th to 15th October **Agenda Item:**

---

joint-API-group (Parlay, ETSI Project OSA, 3GPP TSG_CN WG5) **N5-040563**
Meeting #28, Piscataway, New Jersey, USA, 09-13 August 2004

CR-Form-v7

CHANGE REQUEST

⌘ **22.127** **CR** **072** ⌘**rev** **-** ⌘ Current version: **6.6.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network ☒

Title:	⌘	Delete Requirements for "User-Application Authentication functions"
Source:	⌘	SA1 (CN5)
Work item code:	⌘	OSA3
Date:	⌘	12/08/2004
Category:	⌘	**F**
Release:	⌘	*Rel-6*

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	No stage 3 contributions supporting this requirement have been received.
Summary of change:	⌘	Delete Requirements for "User-Application Authentication functions"
Consequences if not approved:	⌘	Misalignment between Stage 1 (OSA Requirements in 22.127) and Stage 3 (OSA APIs)

Clauses affected:	⌘	13.1.1.1 Authentication 13.2.5 User-Application Authentication functions

	Y	N			
Other specs affected:	⌘		X	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	

Other comments:	⌘	Draft Rel-6 CR 22.127 sent for SA1 Approval attached to the LS in N5-040562.

13.1.1 Trust and Security Management

The trust and security management feature provides the necessary mechanisms which define the security parameters in which client applications may access the network. This includes the availability of a framework initial access point through which all client applications are authenticated and authorised and the ability to allow the signing of on-line service level agreements between the client applications and the framework.

13.1.1.1 Authentication

Authentication is used to verify the identity of an entity (user, network, and application).

Three types of authentication are distinguished:

- User-Network Authentication:

  Before a user can access her subscribed applications, the user has to be authenticated by the network that provides access to the application. This allows the network to check to what applications the user has subscribed to. User-network authentication *is handled within the network and therefore outside the scope of the OSA ~~present document.~~*

- ~~—~~Application-Network Authentication:

  Before an application can use the capabilities from the network, a service agreement has to be established between the application and the network. Establishment of such a service agreement starts with the mutual authentication between application and network. If a service agreement already exists, modification might be needed or a new agreement might supersede the existing.

- User-Application Authentication:

  Before a user can use an application or perform other activities (e.g. modifying profile data) the application must authenticate the user. When the network already authenticates the user, authentication is not needed anymore. When the network is transparent and the user accesses an application directly, authentication is needed between user and application. This is outside the scope of the OSA.

13.1.1.2 Authorisation

13.2.5 VoidUser-Application Authentication functions

The User-Application Authentication functions provide to applications support for authentication of their users. It also provides an "application-specific user identifier" to be used as a parameter in invocation of other OSA Network functions, when requested by the application.

The User-Application Authentication functions shall authenticate an user upon requests of an application; this requires the application to provide as an input the subscriber's credentials, which enable secure method of authentication (e.g. subscriber's certificates).

The User-Application Authentication functions shall return to the invoking application an "application-specific user identifier" (a true identity or alias) that identifies the authenticated user, when requested by the application. The identifier may be used by the application to recognize a user through several accesses to the application; it may also be used by the application as a parameter in invocation of other OSA network functions (e.g., for User Location function).

The User-Application Authentication functions shall support privacy settings defined by the user.

If the subscriber's privacy settings so require, the "application-specific user identifier", returned by User-Application Authentication function to the invoking application, shall be an alias. Otherwise, the "application-specific user identifier" shall be the true identity of the subscriber (e.g. MSISDN).

When the application invokes OSA Network functions related to subscriber (e.g. Location, Presence), the subscriber's identifier shall be included in the request. An application may request it from the User-Application Authentication function.

When an OSA Network function receives the request from the application and the subscriber's identifier is an alias, the OSA Network Function shall invoke the User-Application Authentication function to translate the alias to the subscriber's true identity (e.g. MSISDN).

13.3 User data related functions

joint-API-group (Parlay, ETSI Project OSA, 3GPP TSG_CN WG5) **N5-040565**
Meeting #28, Piscataway, New Jersey, USA, 09-13 August 2004

CR-Form-v7

CHANGE REQUEST

⌘ **22.127** **CR** **073** ⌘ **rev** **-** ⌘ Current version: **6.6.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network ☒

Title:	⌘	Delete Requirements for "User Data Management (OSA support for GUP)"
Source:	⌘	SA1 (CN5)
Work item code:	⌘	OSA3
Date:	⌘	12/08/2004
Category:	⌘	**F**
Release:	⌘	*Rel-6*

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	Missing clear OSA requirements for support of the Generic User Profile (GUP)
Summary of change:	⌘	Delete Requirements for User Data Management (OSA support for GUP)
Consequences if not approved:	⌘	Misalignment between Stage 1 (OSA Requirements in 22.127) and Stage 3 (OSA APIs)
Clauses affected:	⌘	2 References 7 Requirements for User Data Management 13.3.3 User Profile Management functions

		Y	N		
Other specs affected:	⌘		X	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	

Other comments: ⌘ Draft Rel-6 CR 22.127 sent for SA1 Approval attached to the LS in N5-040564.

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*.

2.1 Normative references

[1] 3GPP TS 22.121: "Universal Mobile Telecommunications System (3G); “The Virtual Home Environment”.

[2] 3GPP TS 22.101: "Service principles".

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

[4] 3GPP TS 23.107: "QoS Concept and Architecture".

[5] 3GPP TS 22.024: "Description of Charge Advice Information (CAI)".

[6] 3GPP TS 29.198: "Open Service Architecture; Application Programming Interface; ~~Part 1~~".

[7] 3GPP TS 22.141: "Presence Service Stage 1".

[8] 3GPP TS 22.228: "IP Multimedia Subsystem (IMS) Stage 1".

[9] 3GPP TS 22.071: "Location Services (LCS) Stage 1".

7 Void~~Requirements for User Data Management~~

~~The User Profile logically is a set of information relevant for a given user. . This set of information might be distributed over various physically separated entities in the network andit is provided by Service Capability Servers and – if permitted – from Value Added Services. In case the Generic User Profile (GUP) is deployed in the network, the User Profile may be provided by both the GUP data and the user profile information that are outside the scope of GUP but provided by SCSs and VAS.~~

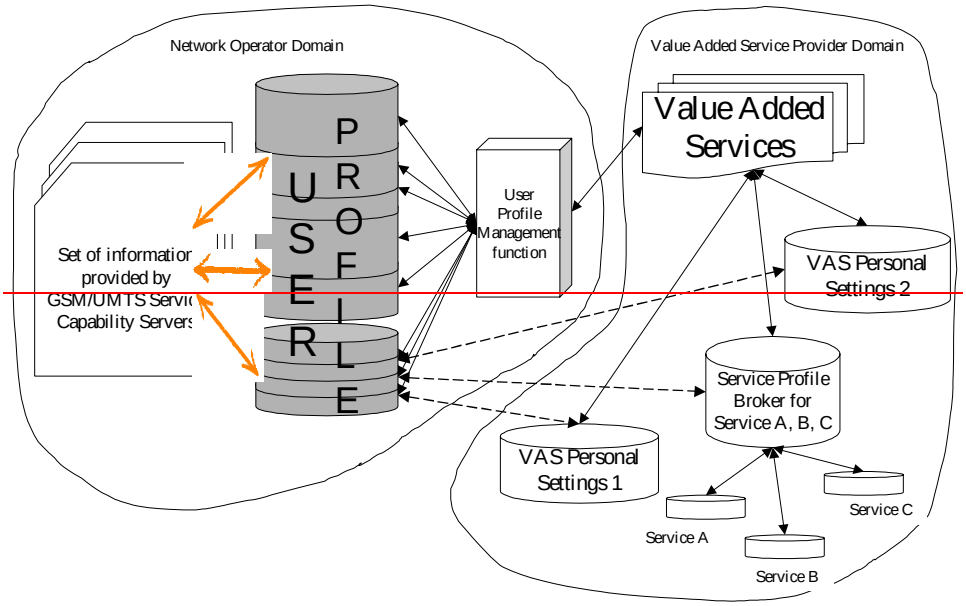
~~Note: The detailed content of the User Profile and the way it is distributed is outside the scope of this specification.~~

~~Subscriber, who subscribe or use services provided by Value Added Service Providers, may customise these VAS according to their needs equally as the subscriber customise her services provided by the network operator. To avoid malicious attacks or conflicting situations, it is needed to allow VAS to access the users User Profile. However VAS shall not be allowed to access the User Profile without permission.~~

~~The OSA Framework functions restrict the applications' access to the User Profile Management functions (section 13.3.3).~~

~~The co-existence of several services and the correct inter-working between them are founded on sufficient information about other services subscribed to.~~

~~The figure below gives a logical overview of the relation between VAS, User Profile Management function and the User Profile itself.~~



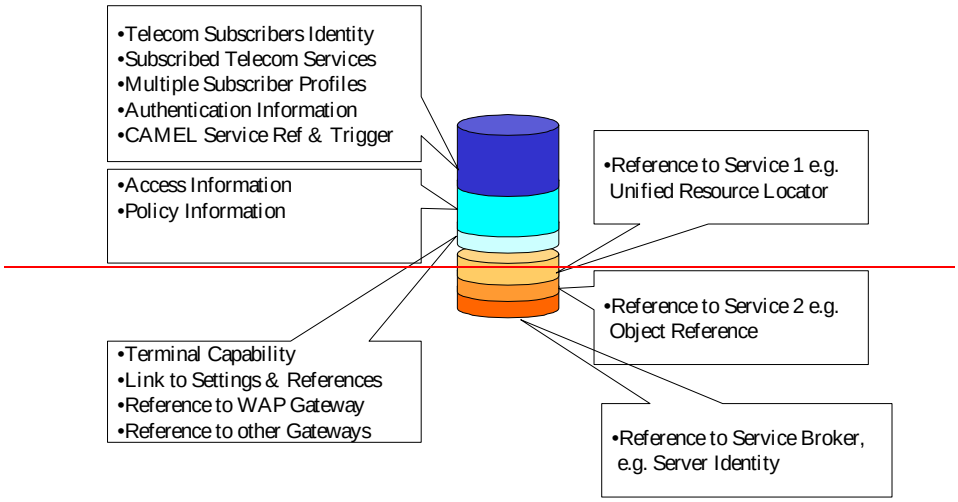
~~Figure 2: Logical overview of relation between User Profile Management function and the User Profile itself~~

~~Note: the dotted line refers to additional Personal Settings. The reference itself shall unambiguously identify the location of the additional personal settings.~~

~~User specific information from the e.g. HLR and/or HSS are equally part of the User Profile as terminal settings and VAS specific preferences. The User Profile in principle is the summary and collection of information with a relevance for the services supported for a given subscriber.~~

~~The figure above shows User and Network Service and VAS specific information, customised by the user. It is assumed that the User Profile consists of several parts. The User Profile elements shall at least be capable to store a reference to additional information stored else where. The User Profile shall act as a root towards all user specific information.~~

~~Even when the content of the User Profile is outside this specification, the following figure shows how a content could look like.~~



~~Figure 3: Example of how a User Profile content could look like~~

~~On the left side of the figure above, typical 3GPP system related information are listed (this is not an exhaustive list).~~

~~The right side depict references to VAS specific information. The representation of references to VAS specific information above, is an example and does not insist to be complete.~~

13.3.3 VoidUser Profile Management functions

The User Profile Management functions enables the (authorised) applications to access the User Profile data, checking before the application's rights related to each separate part of the User Profile. The User Profile data accessed by the application could be independent of specific application but necessary to personalise the application according to the user preferences (an example could be the preferred language of end-user).

Depending on the authorisation, the User Profile Management functions may permit the VAS to read from and/or to add to and/or to modify the User Profile or parts of it. This decision is based on:

- Subscriber identity
- Access information on specific part of the User Profile of the subscriber
- Application identity
- Access type (read, add or modify)

Access information shall contain the user specific access rights per application. These may be given either for individual parts of the User Profile or for a group of data or even all data in the User Profile.

13.3.4 Void

joint-API-group (Parlay, ETSI Project OSA, 3GPP TSG_CN WG5) **N5-040566**
Meeting #28, Piscataway, New Jersey, USA, 09-13 August 2004

CR-Form-v7

CHANGE REQUEST

⌘ **22.127** **CR** **074** ⌘ **rev** **-** ⌘ Current version: **6.6.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network ☒

Title:	⌘	Delete Requirements for “IP session function”
Source:	⌘	SA1 (CN5)
Work item code:	⌘	OSA3
Date:	⌘	12/08/2004
Category:	⌘	**F**
Release:	⌘	*Rel-6*

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	No stage 3 contributions supporting this requirement have been received.
Summary of change:	⌘	Delete Requirements for “IP session function”
Consequences if not approved:	⌘	Misalignment between Stage 1 (OSA Requirements in 22.127) and Stage 3 (OSA APIs)
Clauses affected:	⌘	13.6 IP session function

	Y	N		
Other specs affected: ⌘		X	Other core specifications	⌘
		X	Test specifications	
		X	O&M Specifications	

Other comments: ⌘ Draft Rel-6 CR 22.127 sent for SA1 Approval attached to the LS in N5-040564.

13.6 VoidIP session function

The IP session function enables applications to access information about IP sessions in progress between a UE and IP networks (i.e., the MSISDN and Session Correlation identifier) using the IP address of the UE. An IP session comprises a flow or a set of flows through a network element during a certain time interval. An IP flow is defined to be a stream of packets that have a set of common properties. The properties include source IP address/port and destination IP address/port, protocol type etc. Flows can be grouped into sessions by specifying wildcards for properties (e.g. the set of flows going to port 80, or the set of flows with target IP address X.X.X.X.)

Applications shall have the ability to :

- Release flows in an IP session:

  This provides the ability for an application to force the termination of an IP session. The application may provide an indication of the reason for release of the IP session.

- Control an IP session:

  This provides the ability for an application to request the modification of the parameters of an IP session both during establishment of the session and while the sessions are in progress. The application may also allow the IP Session to continue with or without the modified information pertaining to the IP Session. This may also include the ability to refuse session establishment, to request modification of Quality of Service parameters, to request modification of the destination IP address (including the IP port) and the modification of volume thresholds (e.g. to allow an application to change the threshold at which a notification is raised).

- Monitor an IP Session:

  This provides the ability for an application to monitor an IP session. The application will specify a particular IP session and event condition. When the condition is met an event is generated and the application shall be informed accompanied with sufficient information. For example, an application could be notified when the data volume threshold of a particular user (defined by source IP address) is exceeded.

- Request flow Information

  This provides the ability for an application to request information about the session of interest. This includes quality of service parameters, target IP address and port, duration of session, and data volume of session

The access to the data, which is typically stored within a network authentication server, is obtained via the OSA gateway (i.e., through this SCF). The IP session information/data shall be released based on specific defined policies between the network operator and the application service provider.

13.7 Multimedia Messaging function