Technical Specification Group Services and System Aspects
Meeting #18, New Orleans, USA, 9-12 December 2002

TSGS#17(02)0659

Source: **SA1**

Title: **Release 6 CRs to 22.127 on OSA (Various subjects)**

Document for: **Approval**

Agenda Item: **7.1.3**

SA Doc	Spec	CR	Rev	Phase	Cat	Subject	Old Vers	New Vers	SA1 Doc
SP-020659	22.127	059		Rel-6	B	CR to 22.127 on OSA interfaces at different levels of abstractions	6.1.0	6.2.0	S1-022249
SP-020659	22.127	060		Rel-6	B	Introduction of migration support mechanism	6.1.0	6.2.0	S1-022251
SP-020659	22.127	061		Rel-6	C	Enhancements to IP Session Function in OSA for the control and monitor of IP Flows (Follow up from S1-021927)	6.1.0	6.2.0	S1-022252
SP-020659	22.127	062		Rel-6	B	CR to 22.127 on User Profile	6.1.0	6.2.0	S1-022258
SP-020659	22.127	063		Rel-6	B	CR to 22.127 on Network functions for end-user/application interaction support	6.1.0	6.2.0	S1-022366
SP-020659	22.127	064		Rel-6	B	CR to 22.127 on Framework Function for Federation	6.1.0	6.2.0	S1-022368

TSG-SA1 SWG #18 **S1-022249**
Beijing, China, 14 -18 October 2002 **Agenda Item: 10.6**

CR-Form-v7

CHANGE REQUEST

⌘ **22.127** **CR** **059** ⌘ **rev** **-** ⌘ Current version: **6.1.0** ⌘

*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:	⌘	OSA interfaces at different levels of abstractions
Source:	⌘	SA1 (Telecom Italia)
Work item code:	⌘	OSA3
Date:	⌘	11/11/2002
Category:	⌘	**B**
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:	⌘	This contribution proposes to enforce the alignment with Parlay, by introducing the possibility that the OSA-defined functions (both framework and non-framework ones) could be accessed through additional sets of interfaces at different levels of abstractions and with different programming formalisms
Summary of change:	⌘	Changes in High-level requirements. Introduction of new requirements dealing with different levels of abstraction for the interfaces
Consequences if not approved:	⌘	Reduction of alignement with Parlay (i.e. Parlay X interfaces)
Clauses affected:	⌘	Changes in clause 6. Introduction of a new clause of requirements (e.g., reuse of clause 9, currently Void), to be collocated before the sections describing the functions

		Y	N			
Other specs affected:	⌘	X		Other core specifications	⌘	23.127; 29.198
				Test specifications		
				O&M Specifications		

Other comments: ⌘

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm.
Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

First Modified Section

6 High level requirements to OSA

The following high level requirements apply to the OSA application programming interface (API). The standardised API shall be:

- independent of vendor specific solutions;
- independent of programming languages, operating systems, underlying communication technologies, etc. used in the service capabilities;
- secure, scalable and extensible;
- independent of the location where service capabilities are implemented;
- independent of supported server capabilities in the network;
- independent of the transport mechanism between the service capability features server and the application server;
- It shall be possible for an OSA application to continue operation in case of a consecutive upgrade of the underlying OSA capabilities. This ability to operate may be limited to a specific time period which is managed by the network operator.
- Access to Service Capability Features shall be realised using modern state of the art access technologies, e.g. distributed object oriented technique and Web Services technologies might be considered.;
- OSA shall be aligned as far as possible with equivalent work in other bodies, such as ETSI SPAN,Parlay and JAIN;
- OSA shall allow applications access to home network service capability features. Access to Service capability features other than those provided by the home network is not required;
- It is not required that network entities, which provide the implementation of OSA interfaces (SCFs), be mappable to 3GPP standardised functionality, nor that the existence of a standardised interface / protocol to communicate with 3GPP standardized network elements is required. Thus it is permissible to e.g. build a OSA API function into a WAP gateway to retrieve terminal capabilities from terminal supporting the WAP protocol.

Note: If the network entity, to which OSA provides an API interface, is a 3GPP standardised entity and if a standardised interface / protocol to communicate with that network entity exists it is recommended that 3GPP defines a mapping of the OSA API functions to that interface / protocol.

Second Modified Section

9 Requirements on interfaces at different levels of abstractions

The OSA-defined functions may be accessed through interfaces at different levels of abstractions and according to different programming formalisms, in addition to those defined in the previous Releases. The abstraction levels and the programming formalism should be identified according to the needs of the programmers' communities. Initially, those interfaces should consist in a simplified version of the already standardised OSA APIs defined according to the Web Services principles (e.g., Parlay X, OMA).

All the interfaces shall be integrated in the context of the OSA architecture:

- they shall guarantee a secure and controlled access to the service capabilities;
- it shall be possible to introduce them in an incremental way;
- they should allow applications be triggered by network events.

The interfaces shall be defined using state of the art specification formalisms (e.g., UML, WSDL), and realised using different distributed processing technologies.

End of document

TSG-SA1#18 **S1-022251**

Busan, Korea, 11 – 15 November 2002 **Agenda Item: 10.6 OSA**

CR-Form-v7

CHANGE REQUEST

⌘ **22.127** **CR** **060** ⌘ **rev** **-** ⌘ Current version: **6.1.0** ⌘

*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 **X**

Title:	⌘	Introduction of support to inform applications about new SCSs and their level of Backward compatibility
Source:	⌘	SA1 (Ericsson)
Work item code:	⌘	OSA3
Date:	⌘	04/11/2002
Category:	⌘	**B**
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:	⌘	It should be possible to announce to interested applications that when a new SCS is registered to the Framework to what extent the new SCS is backward compatible with an SCS the application is currently using. This allows applications to get informed automatically for instance about possibilities to migrate to a newer SCS. A special case is when there is an SCS available that immediately replaces an SCS the application is currently using as the latter needs to be taken “out of service”.
Summary of change:	⌘	The Notification Function is extended to allow applications recieve this information.
Consequences if not approved:	⌘	Applications get no information, like an indication on the level of backward compatibility, about newer SCSs No support for redirecting applications to a alternative SCS when the one they are currently are using is being replaced.
Clauses affected:	⌘	12.2

		Y	N			
Other specs affected:	⌘	**X**		Other core specifications	⌘	29.198-3
				Test specifications		

	O&M Specifications	
Other comments: ⌘		

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

12 Event Notification Function

The Event Notification Function shall allow an application to specify the initial point of contact which it is interested in. The Event Notification Function provides the necessary mechanisms which enables an application to request the notification of subscriber or network related event(s). An application may in addition request the cancellation of subscriber or network related event notification.

For all subscriber related events the Event Notification Function shall support two ways for an application to subscribe to notifications: the application shall either specify the subscriber for which the Event Notification Function is valid or indicate that it is ready to receive user related notifications for any subscriber. The application may be responsible for the explicit provisioning of the subscriber related event notification or it may leave the provisioning of the notifications to the Home Environment operator and just indicates that it is ready to receive notifications. An application may use both mechanisms at the same time. Once an application has enabled the notification of event(s), the Event Notification Function shall report the event(s), including the identification of the user to which the event applies, until such time the application explicitly requests the termination of the event(s) notification.

When the event occurs, the application that requested the event is informed.. The notification of the event shall be accompanied by unambiguous information identifying the original request and event related data.. For example, in case of an application is interested in “message” the notification to the application shall indicate whether it is incoming or outgoing, in case of chargeable events, the application shall receive details as used at the network to create a Call Detail Record. In this case, processing in the network is not suspended after notification of the event to the application.

The Event Notification Function includes the availability of offering additional criteria to be specified by the application. The set of criteria is individual and may vary for the event requested. The detailed set of criteria available for each of the events below are described in [6].

12.1 Subscriber Related events:

- An initial call processing event occurs.

  when a call to or from a given user is created and this event is armed by an application, that application shall be notified.

- A message is sent or received.

  when a message to or from a given user is sent or received and this event is armed by an application, that application shall be notified.

- A chargeable event happens.

  when a chargeable event occurs for a given user and this event is armed by an application, that application shall be notified.

- The user´s status is changed.

  when a subscriber registers to a network or when a given user changes her status (e.g. from idle to busy) and this event is armed by an application, that application shall be notified. Registration in this sense is further detailed in the chapter on User Status Functions. Attach and detach applies for CS and PS.

- The user´s location is changed.

  when a given user changes her location (e.g. leaving a certain area which is “identifiable” by the network) and this event is armed by an application, that application shall be notified.

- The Terminal Capabilities are changed.

  when the capabilities of a terminal change (e.g. when a keyboard is attached) and this event is armed by an application, that application shall be notified.

Note: The ability to support this function is dependent on the ability of a terminal (through e.g. MExE or WAP) to notify changes in its capabilities. Therefore this function will *not* be able to supply event notifications for terminals not supporting notification of their terminal capabilities.

12.2 Network Related Events:

- A network fault management condition is met,

  when a fault management condition occurs at the underlying network (e.g. congestion of network components) and this event is armed by an application, that application shall be notified.

- A network service or network service capability registers,

  when a network service capability feature registers with the Framework all applications which have subscribed to this event and are currently authorised to use this service capability feature shall be notified. In case there is already a service capability feature of the same type that is in use, all applications which are authorised and have subscribed to recieve information about this event will be informed about information related to backward compatibility between the new service capability feature and the version currently in use. This information allows an application provider to have an indication about the effort on his side required in migrating from the older to the newer version.

- A network service or network service capability de-registers,

  when a network service capability feature de-registers with the Framework all applications which are currently authorised to use this service capability feature shall be notified.

12.3 Other Related Events:

- A change in presence related information.

If any presence related information changes (such as one or more presence information attributes or a user's availability), and this event is armed by the application, that application shall be notified. Presence information may be associated with a user, device or service, or any abstract entity that has the ability to report presence information.

TSG-SA WG 1 (Services) #18 **S1-022252**
Busan, Korea, 14-18th November 2002 **Agenda Item: OSA**

CR-Form-v7

CHANGE REQUEST

⌘ **22.127** **CR** **061** ⌘ **rev** **-** ⌘ Current version: **6.1.0** ⌘

*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:	⌘	Proposal for enhancements for the monitor and control of IP Sessions
Source:	⌘	SA1 (Lucent Technologies)
Work item code:	⌘	OSA-3
Date:	⌘	1st November 2002
Category:	⌘	**C**
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:	⌘	Provide detailed requirements as to the capabilities for an OSA application relating to IP Sessions.
Summary of change:	⌘	The subclause that describes the IP Session function now contains a clear indication of the meaning of an "IP Session". This can be a flow OR a set of flows defined by a source and destination IP address/port and destination. The functions that may be performed by an application may include • Release an IP Session • Control an IP session • Monitor an IP session • Request information pertaining an IP session
Consequences if not approved:	⌘	Lack of clarify in the requirement leading to insufficient understanding by other WGs and incorrect implementation of the requirement.

Clauses affected:	⌘	13.6

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

Other comments:	⌘	Additional background information, including uses cases for these requirements is given in S1-021926

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

13.6 IP session function

The IP session function enables applications to access information ~~(read only)~~ 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.

TSG-SA1 SWG #18 **S1-022258**
Busan, Korea, 11 -15 November 2002 **Agenda Item: 10.6**

CR-Form-v7

CHANGE REQUEST

⌘ **22.127** **CR** **062** ⌘ **rev** **-** ⌘ Current version: **6.1.0** ⌘

*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:	⌘	User Profile Management
Source:	⌘	SA1 (Telecom Italia, Siemens)
Work item code:	⌘	OSA3
Date:	⌘	12/11/2002
Category:	⌘	**B**
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:	⌘	This CR proposes a revision of the old version of the User Data Management text reintroduced in Durango for release 6 (previously deleted from release 5). Moreover it is a first step in understanding the relation between OSA User Profile and the Generic User Profile.
Summary of change:	⌘	Tidy-up of the text concerning the Requirments for User Data Management. The text describing the User profile Management function is moved to the corrisponding subclause (13.3.3) previously void
Consequences if not approved:	⌘	The TS will have an old and confused version of the text concerning the User Data Management (written before the GUP work existence!)

Clauses affected:	⌘	Changes in subclause 7, 13.3.3.

Other specs affected:	⌘	Y	N		⌘	
		X		Other core specifications		23.127; 29.198
				Test specifications		
				O&M Specifications		

Other comments: ⌘

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm.
Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

First Modified Section

7 Requirements for ~~u~~User ~~d~~Data ~~m~~Management

~~Note that the work on Generic User Profile may have an influence and needs to be studied carefully.~~

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 and~~.~~ it 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.

~~The set of information is provided by Service Capability Servers and – if permitted – from Value Added Services. The amount of User Profile information might be distributed over various physically separated entities. *The concept of distributed information is not within the scope of this specification. The detailed content of the User Profile is not subject herein.* However, subscribers are able to subscribe or use services provided from Value Added Service Providers.~~ 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~~SER~~ 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.

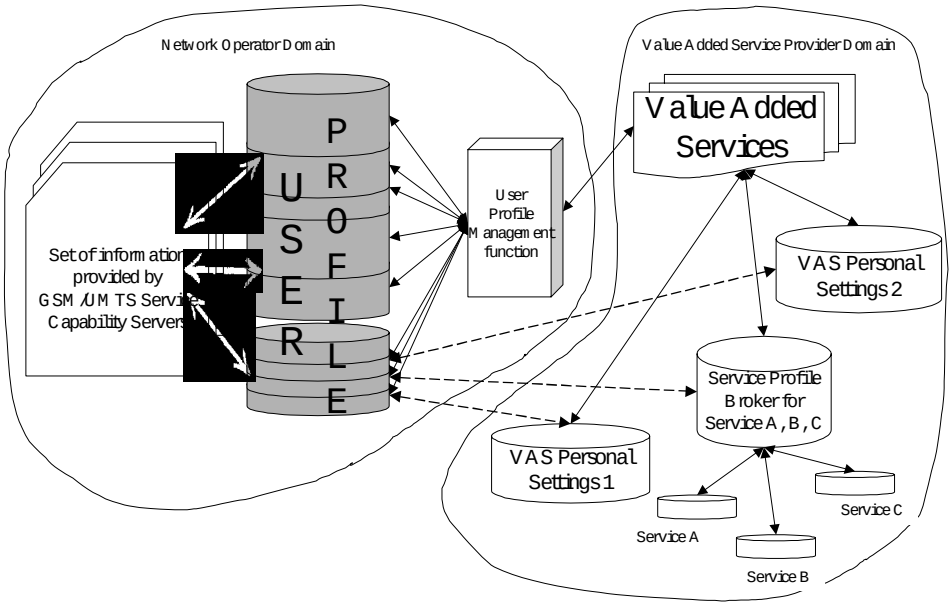
~~VAS shall not be allowed to access the User Profile without permission. It is important to prevent the User Profile from malicious attacks. The OSA Framework functions restrict the applications' access to the User Profile Management (UPM) functions.~~

~~UPM functions check the application's rights to make these actions regarding each separate part of the user profile. 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 in 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.~~

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

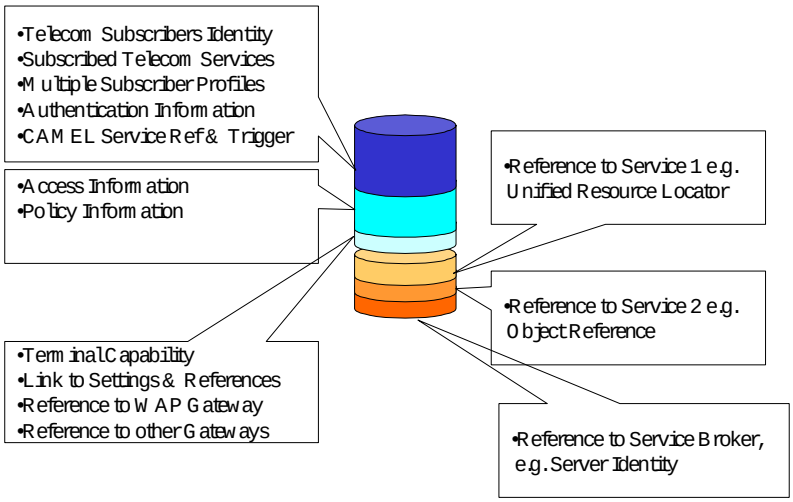


Note: the dotted line refers to additional Personal Settings. The reference itself shall unambiguously identify the location of the additional personal settings.

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 ~~u~~User ~~p~~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.



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.

Second Modified Section

13.3.3 User Profile Management functions

~~No requirements for this release are identified.~~

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 User Profile access Authentication/Authorisation functions~~

~~No requirements for this release are identified.~~

End of document

TSG-SA1 SWG #18 **S1-022366**
Busan, Korea, 11 -15 November 2002 **Agenda Item: 10.6**

CR-Form-v7

CHANGE REQUEST

⌘ **22.127** **CR** **063** ⌘ **rev** **-** ⌘ Current version: **6.1.0** ⌘

*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:	⌘	Network functions for user/application interaction support
Source:	⌘	SA1 (Telecom Italia, Nokia)
Work item code:	⌘	OSA3
Date:	⌘	11/11/2002
Category:	⌘	**B**
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:	⌘	This CR proposes the enhancement of the support that an OSA gateway can provide to interactions among applications and their users, introducing support for user-application authentication, privacy for users accessing applications
Summary of change:	⌘	Introduction of an User-Application Authentication function.
Consequences if not approved:	⌘	It would not be possible to provide support for User-Application Authentication and privacy of users accessing applications.

Clauses affected:	⌘	Changes in subclause 13.1.1.1. Introduction of a new subclause (e.g. 10.2) in clause 10. Introduction of a new subclause (e.g. 13.2.5) in subclause 13.2.

	Y	N			
Other specs affected: ⌘	X		Other core specifications	⌘	23.127; 29.198
			Test specifications		
			O&M Specifications		

Other comments: ⌘

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm.
Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

First Modified Section

13.1.1 Trust and Security Mangement

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 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 ~~but this is outside the scope of the present document~~;.

13.1.1.2 Authorisation

Authorisation is the activity of determining what an authenticated entity (user, network, and application) is allowed to do.

NOTE: Authentication must therefore precede authorisation.

Two types of authorisation are distinguished:

- Application-Network Authorisation:

  Verifies what non-framework functions the application is allowed to use. Once an application has been authorised to use one, more or all non-framework functions no further authorisation is required as long as the "allowed" non-framework functions are used.

- User-Application Authorisation:

  The application verifies what actions the user is allowed to perform (e.g. deactivation of functionality, modification of application data). This is transparent to the network and therefore outside the scope of the present document.

Second Modified Section

10 Security and Privacy requirements

10.1 Security requirements on User Profile Management

Note: The work on Generic User Profile may have an influence and needs to be studied carefully.

The User Profile Management functions shall be able to grant or deny access to individual parts of the subscriber's User Profile as described in the clause 7.

The User Profile Management functions ~~s~~hall ensure that all operations on parts of User Profile data are authorized.

The type of access is one out of:

- Reading user profile information; in case parts of the User profile is subject for reading it shall unambiguously be identified by the application,
- Adding information to the user profile,
- Modify existing information in the user profile.

The control of access rights is in principle on the user's discretion. The user shall have the possibility to allow or restrict the retrieval and presentation of her user related data. The mechanism how a user is able to maintain access rights is for further study.

10.2 Privacy requirements on Subscriber Identity

It shall be possible for the subscriber to hide his/her true identity from the OSA Applications and replace it with an alias. The alias shall be unique identification that has a one-to-one relationship to the true identity (e.g. MSISDN) of the subscriber and may be permanent or temporary (e.g. session based).

Third Modified Section

13.2.5 User-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).

End of document

TSG-SA1 SWG #18 **S1-022368**
Beijing, China, 14 -18 October 2002 **Agenda Item: 10.6**

CR-Form-v7

CHANGE REQUEST

⌘ **22.127** **CR** **064** ⌘ **rev** **-** ⌘ Current version: **6.1.0** ⌘

*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:	⌘	Access to SCFs in another network
Source:	⌘	SA1 (Telecom Italia)
Work item code:	⌘	OSA3
Date:	⌘	12/11/2002
Category:	⌘	**B**
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:	⌘	An operator may wish to allow access to the SCF by applications in another administrative domain. E.g. an application in one network can be allowed to access the SCF in another network where the networks are owned by operators in the same group.
Summary of change:	⌘	Changes in the High-level requirements. Changes in the Framework function introduction A use case added in the Annex
Consequences if not approved:	⌘	It would not be possible to handle federation scenarios.

Clauses affected:	⌘	Changes in clause 6. Changes in clause 13.1. Introduction of an use case (A.3) in the Annex

		Y	N			
Other specs affected:	⌘	X		Other core specifications	⌘	23.127; 29.198
				Test specifications		
				O&M Specifications		

Other comments:	⌘	

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

First Modified Section

6 High level requirements to OSA

The following high level requirements apply to the OSA application programming interface (API). The standardised API shall be:

- independent of vendor specific solutions;
- independent of programming languages, operating systems, underlying communication technologies, etc. used in the service capabilities;
- secure, scalable and extensible;
- independent of the location where service capabilities are implemented;
- independent of supported server capabilities in the network;
- independent of the transport mechanism between the service capability features server and the application server;
- It shall be possible for an OSA application to continue operation in case of a consecutive upgrade of the underlying OSA capabilities. This ability to operate may be limited to a specific time period which is managed by the network operator.
- Access to Service Capability Features shall be realised using modern state of the art access technologies, e.g. distributed object oriented technique might be considered.;
- OSA shall be aligned as far as possible with equivalent work in other bodies, such as ETSI SPAN,Parlay and JAIN;
- ~~—~~OSA shall allow applications access to home network service capability features. Access to Service capability features in another network shall be possible.
- When access to Service capability features in another network or administrative domain exists, the following requirements apply:
    - The application shall not be aware that the SCF is in another network
    - The SCF shall not need to support additional functionality in order to be accessed from a different network
    - The network providing the SCF shall be able to control the visibility and usage of the SCF by another network.

~~other than those provided by the home network is not required;~~

- It is not required that network entities, which provide the implementation of OSA interfaces (SCFs), be mappable to 3GPP standardised functionality, nor that the existence of a standardised interface / protocol to communicate with 3GPP standardized network elements is required.Thus it is permissible to e.g. build a OSA API function into a WAP gateway to retrieve terminal capabilities from terminal supporting the WAP protocol.

Note: If the network entity, to which OSA provides an API interface, is a 3GPP standardised entity and if a standardised interface / protocol to communicate with that network entity exists it is recommended that 3GPP defines a mapping of the OSA API functions to that interface / protocol.

Second Modified Section

13.1 The Framework functions

The framework provides the essential capabilities that allow OSA applications to make use of the service capabilities in the network. The framework shall support the ability for applications to access SCFs in another network.

There are three distinct features that comprise the framework: *Trust and Security Management, Service Registration and Discovery functions* and *Integrity Management.*

Third Modified Section

A.3 Access to SCFs in another network

Service Scenario Description

Two operators, a wireline operator A and a wireless operator B, belonging to the same telecommunication group, have adopted OSA solutions. Each of them introduced in its service platform an OSA Gateway, to provide to application layers (also in 3rd party domains) a relevant subset of capabilities implemented in its network.

Let assume that a corporate is implementing a rich VPN-like service by exploiting the features provided by the wireline operator (i.e., the corporate subscribed a subset of the SCFs provided by wireline operator). If such a corporate wants to enhance its application with the capability to handle with SMSs sent/received by the members of its VPN (e.g., its employees) and the wireline operator does not provide any appropriate network capabilities, according to the current specifications, the corporate must subscribe the needed SCF (e.g., a User Interaction implemented through SMSs) provided by another operator (e.g., the wireless operator B). But in this case, the corporate must deal with two subscriptions, its VPN application must cope with two OSA Gateways; in addition, the corporate could select a different wireless operator, not belonging to the same group of the operator A.

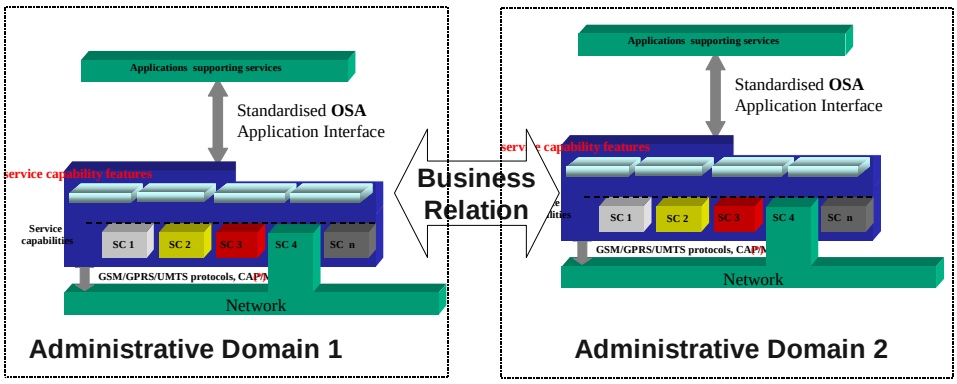


Figure 1: Operator A and Operator B relationship

Such a situation could be dealt by enhancing the OSA specifications in order to allow the OSA Gateways belonging to A and B to be "federated", in order to allow the subscribers to the OSA Gateway in A to access also, in a controlled way, the service capabilities provided by the OSA Gateway in B. This means that the applications do not have to deal with the complexity of handling two OSA Gateways, the application service provider does not have to

open a new customer relationship with another operator, and the operator A has not to introduce additional service capabilities in its infrastructure.

End of document