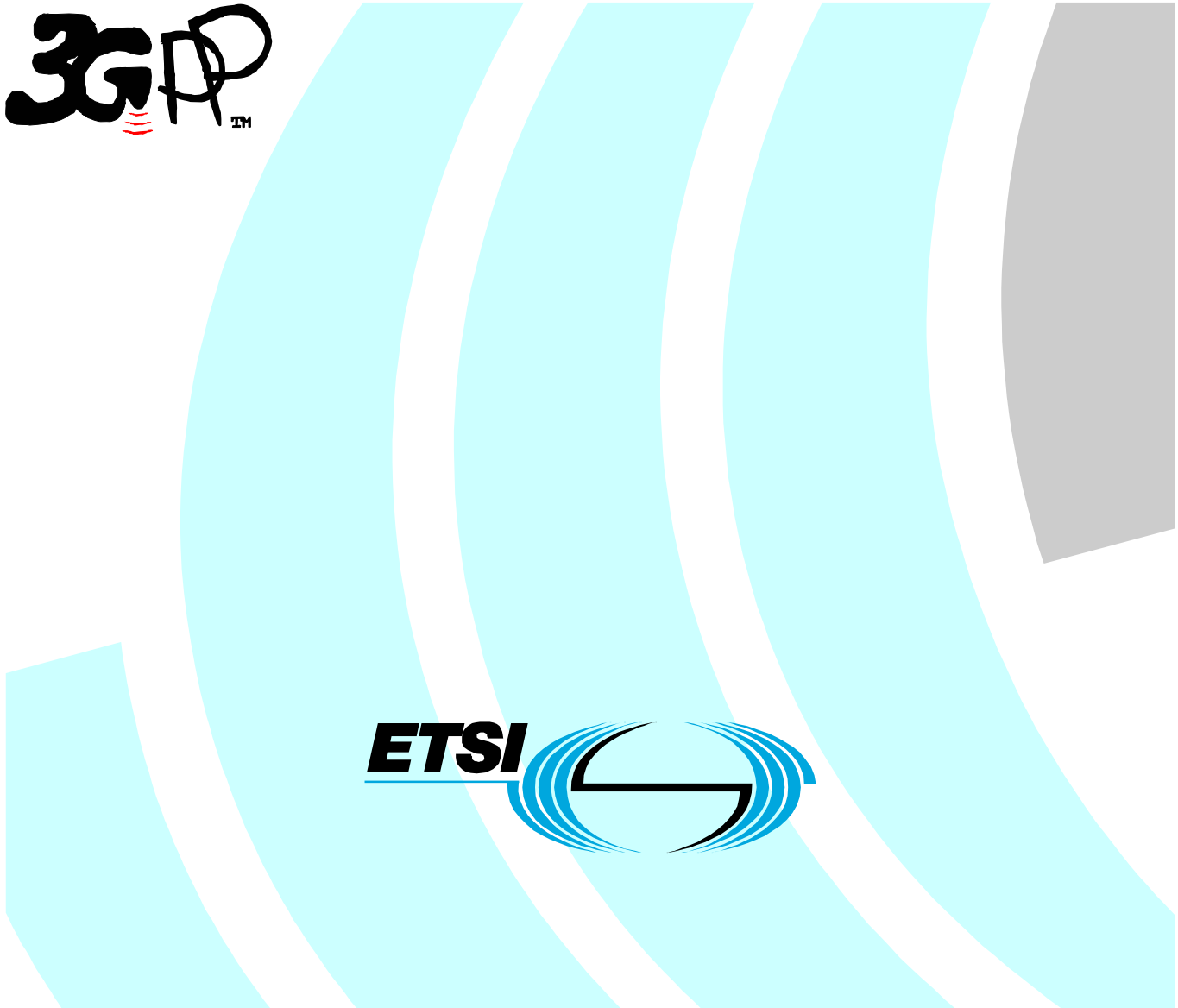
ETSI TS 122 127 V5.5.0 (2002-12)

Technical Specification

Universal Mobile Telecommunications System (UMTS);
Service Requirement for the Open Services Access (OSA);
Stage 1
(3GPP TS 22.127 version 5.5.0 Release 5)



Reference
RTS/TSGS-0122127v550

Keywords
UMTS

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 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is 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 (http://webapp.etsi.org/IPR/home.asp).

All published ETSI deliverables shall include information which directs the reader to the above source of information.

Foreword

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

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

The cross reference between GSM, UMTS, 3GPP and ETSI identities can be found under www.etsi.org/key .

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

This document specifies the stage 1 requirements for realisation of an Open Service Access (OSA).

OSA enables applications to make use of network functionality through an open standardised interface (the OSA API). OSA provides the glue between applications and network functionality. In this way applications implementing the services become independent from the underlying network technology.

Applications which make use of network functionality offered through the OSA interface are not standardised by 3GPP.

The network functionality offered through the OSA interface may or may not be standardised by 3GPP.

OSA is one toolkit, amongst others, that enables certain aspects of the requirements of the Virtual Home Environment (VHE) concept to be realised.

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] Void

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

2.2 Informative references

[10] World Wide Web Consortium Composite Capability/Preference Profiles (CC/PP): A user side framework for content negotiation (www.w3.org)

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

Access Rules: constraints on how the presence service makes presence information available to watchers. For each presentity's presence information, the applicable access rules are managed by the principal that controls the presentity

Note: This Release 5 Access Rules does not refer to the Access Rules of the 3GPP Presence Service that is in Release 6.

Applications: software components providing services to users by utilising service capability features.

Application Interface: standardised Interface used by applications to access service capability features.

Availability: a property of a user denoting his/her ability and willingness to communicate based on factors such as the identity or properties of the requester of the information and the preferences and/or policies that are associated with the user. This property may be computed through information available from various capabilities within the network including (but not necessarily) the presence service.

Call: A logical association between several users pertaining to the CS CN domain..

Charging: A function whereby information related to a chargeable event is formatted and transferred in order to make it possible to determine usage for which the charged party may be billed.

HE-VASP: Home Environment Value Added Service Provider. For the definition see [3]

Home Environment: For the definition see [3]

IM : IP Multimedia. For definition see [8]

IM Session: For definition see [8]

Local Service: For the definition see [1]

Personal Service Environment: For the definition see [1]

Policy: is a formalism that may be used to express business, engineering or management criteria. A policy is represented by a set of rules. Rules are expressed as condition(s)-actions(s) pairs. When the conditions associated with a rule are satisfied the associated actions are executed.

Note: Policies created by applications are matched against the policies of a Network.

Policy Event : A policy event is associated with the action part of designated rule(s). The event is generated when the action part is executed.

Policy Management: is the capability to create, modify and delete policy related information, including policy events.

Policy Enabled Service: is a Service which has some or all of its properties expressed in terms of policy rules. E.g. Charging Service wherein charging criteria are expressed in terms of policy rules

Policy Decision Point: A function of the network where the applicable policy is chosen.

Policy Enforcement Point: A function of the network where the chosen policy is applied.

Policy Repository: A function of the network where policies are stored.

Policy Enabled network: is a network that supports at least one instance of a Policy Repository and Policy Decision Point and Policy Enforcement Point.

Presence Information: is a set of attributes characterising current properties of presentities such as status.

Note: This Release 5 Presence Information does not refer to the Presence Information of the 3GPP Presence Service that is in Release 6.

Presence Entity (presentity): is any uniquely identifiable entity that is capable of providing presence information.

Note: This Release 5 Presence Entity does not refer to the Presence Entity of the 3GPP Presence Service that is in Release 6.

Service Capabilities: bearers defined by parameters, and/or mechanisms needed to realise services. These are within networks and under network control.

Service Capability Feature: functionality offered by service capabilities that are accessible via the standardised application interface.

Service Provider: an organisation which delivers services to the subscriber. This can be e.g. the operator of the subscriber's Home Environment or an authorised VASP.
Note: In the context of this specification it is assumed, that at least one application providing the services of the Service Provider makes use of OSA functions

Services: a service is the user experience provided by one or more applications.

User: For the definition see [1]

Virtual Home Environment: For the definition see [1]

Watcher: any uniquely identifiable entity that requests presence information about a presentity, or watcher information about a watcher.

Note: This Release 5 Watcher does not refer to the Watcher of the 3GPP Presence Service that is in Release 6.

Watcher Information: information about watchers that have received or may receive presence information about a particular presentity within a particular recent span of time.Note: This Release 5 Watcher Information does not refer to the Watcher Information of the 3GPP Presence Service that is in Release 6.

Further 3G related definitions are given in 3G TR 21.905 [3].

3.2 Abbreviations

For the purposes of this TS the following abbreviations apply:

API	Application Programming Interface
CAMEL	Customised Application For Mobile Network Enhanced Logic
HE	Home Environment
PS	Packet Switched
PSE	Personal Service Environment
VHE	Virtual Home Environment
OSA	Open Service Access
SCF	Service Capability Feature
MExE	Mobile Execution Environment

Further 3G related abbreviations are given in 3G TS 21.905 [3].

4 General Description of OSA

In order to be able to implement future applications/end user services that are not yet known today, a highly flexible Framework for Services [1] is required. The Open Service Access (OSA) enables applications implementing the services to make use of network functionality. Network functionality offered to applications is defined in terms of a set of Service Capability Features (SCFs). These SCFs provide functionality of network capabilities which is accessible to applications through the standardised OSA interface upon which service developers can rely when designing new services (or enhancements/variants of already existing ones).

The aim of OSA is to provide a standardised, extensible and scalable interface that allows for inclusion of new functionality in the network with a minimum impact on the applications using the OSA interface.

5 The role of OSA within the VHE framework for services

The goal of standardisation in 3GPP with respect to services is to provide a framework within which services can be created based on standardised service capability features (c.f. [1]). 3GPP services will generally not rely on the traditional detailed service engineering (evident for supplementary services in second-generation systems), but instead provides services using generic toolkits.

OSA is one of these toolkits, standardised within 3GPP, for the support of services within 3GPP system (see chapter 5.1).

Services can be implemented by applications using service capability features [1], which are accessible via the OSA interface towards these SCFs in the network.

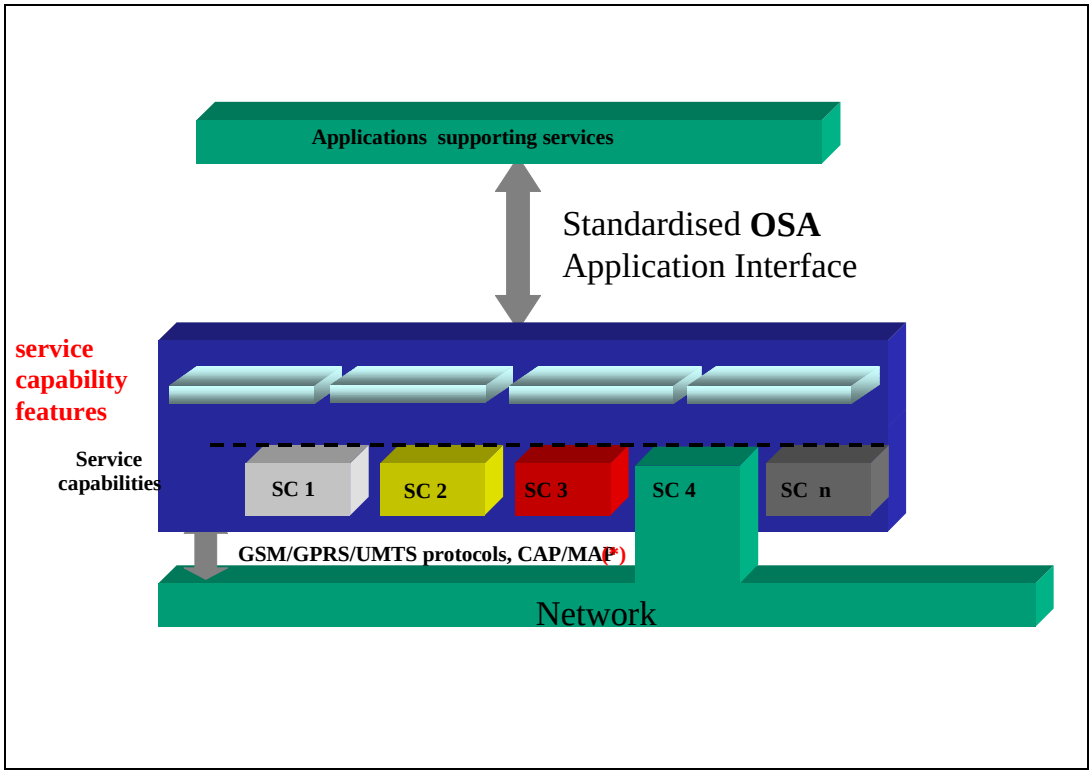


Figure 3: Applications access Service Capability Features via the standardised OSA Application Interface

5.1 Physical location of applications using the OSA interface

The physical location of applications accessing the OSA application programming interface is an implementation matter. This TS places no requirements on the physical location of the applications accessing the OSA application programming interface.

The only requirement on such applications accessing the OSA application programming interface is that they shall only do so via the framework for services [1].

The architectural support of the OSA application programming interface shall permit applications access to the OSA API independent of where the applications are physically executing.

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 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.

7 Void

8 Charging requirements

The charging functionality of OSA allows an application to raise a charge against a subscriber's account for goods and services provided to her. It enables the invoicing, by the operator, of soft (e.g. download of software, music,...) and hard goods (e.g. CDs, books,...), which potentially are provided by third parties.

Additionally, the charging functionality of OSA shall provide for the maintenance of non-monetary subscriber accounts. An application may add or deduct non-monetary units to or from these accounts.

The responsibility for the subscriber accounts can be assigned to either the home network or elsewhere.:

- If the home network does not handle the accounts itself, charging requests are sent from the home network (and possible other applications) to a dedicated charging application, typically a charging centre. This case is out of scope of OSA.
- If the accounts are handled by the home network, the operator takes care of them.
  They may be used to charge for network resource usage (*call charging*, as it is done today) as well as any non-telecommunication related activity (any *E-commerce activity like service usage, online purchases*...)

OSA shall provide sufficient functions to support charging when the accounts are handled by the home network.

Two cases need to be considered in more detail:

Call, Session and Event Charging: OSA shall enable applications to control the charge of a call, a session (PS Session or IM Session) and / or an event that is under supervision of this application. OSA shall allow an application to provide additional charging information to the network;

Service Usage (e.g. Online Purchases): On the other hand, OSA shall allow to employ the charging capabilities of the network to charge subscribers for any kind of service or even online purchases. Calculation of the charge may be based on monetary and/or non monetary grounds.

Beyond this, there are **general** charging **functions** on subscriber accounts (monetary and non-monetary) that shall be available via OSA:

- Query the current account balance and current reservations.
- Monitor account access (send notifications if charges or recharges are applied to a subscriber's account).
- Retrieve the history of the transactions

9 Void

10 Security requirements

No requirements for this release are identified.

11 Requirements for Policy Management

Applications shall have the ability to interact with policy-enabled Service Capability Features in a secure manner. The network policies always take precedence over the application defined policies.

The OSA interface shall provide sufficient capabilities to enable applications to request:

- **To manage the application's policy-related information**
  This allows applications to create, modify and delete policies, policy events and to activate and deactivate policy rules.

- **To manage policy event notification**
  This allows applications to register for specific policy events. Once registered for such events, the application shall receive notification of the events until it explicitly requests the termination of the notification request

- **To collect policy statistics**
  This allows an application to collect policy related statistics from the network. Examples include success or failure of operations on policies and time stamps of policy events.

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.

- 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.

13 Functions offered by OSA

Functions that are offered by OSA shall be applicable for a number of different business and applications domains (including besides the telecommunication network operators also service provider, third party service providers acting as HE-VASPs, etc.).

All of these businesses have different requirements, ranging from simple telephony and call routing, virtual private networks to fully interactive multimedia to using MS based applications.

Service Capability Features:

Application/Clients access OSA functions in terms of service capability features via the standardised application interface. This means that service capability features are accessible and visible to application/clients via the method/operation invocations in the interface.

Service capability features shall be defined as much as possible in a generic way to hide the network specific implementation. To achieve this, it is necessary to identify the functionalities that can be provided in different ways by the use of different service capabilities. For example, User Location can be produced in several underlying ways.Each of these functionalities can then be defined as a single generic function and the different underlying service capabilities are not visible to the application. It is important that the generic part becomes as large as possible to enable applications to use functions without the need for knowledge of the underlying network capabilities

When applications use the generic service capability features, these applications become independent of the network domain ie network agnostic. Applications shall however still be able to request service capability features specific to a service capability (e.g. Call Setup from CAMEL) or specific to a particular network domain. This will increase dependency of the application on the used service capability while providing improved optimisation.

Note: The grouping of OSA functions into Service Capability features is out of scope of this document.

Three different types of OSA functions can be distinguished:

- **Framework functions**: provide commonly used utilities, necessary for access control, security, resilience and management of OSA functions;

- **Network functions**: these shall enable the applications to make use of the functionality of the underlying network capabilities.

- **User Data** related functions: these enable applications to access data of a particular user. Such data are e.g. the status of the user, her location or data in the user's User Profile.

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

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.

13.1.2 Service Registration feature

The Registration function enables the non-framework service capability features (i.e. service capability features that contain non-Framework functions) to register with the Framework. Registration must take place before authorised applications can find out from the Framework which non-framework service capability features are available. This means that the non-framework service capability features must be registered before they can be discovered and used by authorised applications. The service capability feature is finally registered if the registration process is successfully completed.

Note that only the non-framework service capability features have to be registered. The Framework service capability features (containing only Framework functions) are available by default since they provide basic mechanisms.

13.1.3 Service De-Registration function

The De-Registration function enables the non-framework service capability features (i.e. service capability features that contain non-Framework functions) to de-register with the Framework. When a service capability feature de-registers the service capability feature shall discontinue providing service to all applications. Further, the service capability feature can no longer be discovered.

13.1.4 Service Discovery feature

The Discovery function enables the application to identify the total collection of service capability features that it can use. Upon request of the application, the Discovery function indicates the non-framework service capability features that are available for use by the application. The list of available service capability features is created through the Registration process described in subclause 12.1.2. This means that a service capability feature must be registered at the Framework before it can be discovered by the application.

13.1.5 Integrity Management function

Integrity management provides the means to allow the framework to query and report conditions that relate to the integrity of the framework, the network service capability features and the client applications. Furthermore an application may query conditions that relate to the integrity of the framework ad the network service capability features and report on it's own conditions. As part of the integrity management functions, the framework may provide:

- supervision of the status of client applications to ensure continued operation, a process known as heartbeating.
- fault management reporting and control. Specific examples include the ability for the framework to notify applications of internal fault conditions as well as faults in the network service capability features and the ability for applications to request specific test executions in the framework.
- operations and maintenance access, more specifically, the ability for the application to synchronise with the system date and time.

13.2 Network functions

The Network functions represent the total collection of network resources.
The following subclauses define generic network functions e.g. for Message Transfer.

13.2.1 Call and Session Control functions

This subclause details with Call and Session Control functions. The purpose of this function is to allow applications to control and monitor calls, packet switched sessions and IM Sessions.

The application may request the quality of service when first negotiated at the start of the call and may also request the network to notify the application of any changes in QoS (conversational, background, interactive and streaming class - see [4]) which take place during the call.

For QoS information, the Call and Session Control Functions allow applications to monitor the amount of used traffic channels and bandwidth (e.g. for HSCSD) and used timeslots (e.g. for GPRS).

13.2.1.1 CS Call Control functions

This subclause details with circuit switched call control functions. The purpose of this function is to allow applications to control and monitor calls.

Applications should have the ability to :

- Release Calls:

  This provides the ability for the application to force the release of a call. The application may provide an indication of the reason for release of the call.

- Control Calls:

  This provides the ability for an application to modify the information pertaining to the call at the time of establishment of the call. The application may also allow the call to continue with or without the modified information pertaining to the call. The application shall have the ability to request call events of the call under control to be observed by the network and reported back to the application.

- Request call information:

  This provides the ability for an application to request information relating to the call of interest specified in advance. Requested information includes at least call duration, call end time.

- Monitor calls:

  This provides the ability for an application to monitor for call duration and tariff switching moments. An application may specify a threshold for the duration of a call or a part thereof. The application shall have the ability to grant new thresholds when the expiry of a previously set threshold has been reported to the application. When an event is subject to be monitored and the event is met, the application shall get informed accompanied with sufficient information.

- Presentation of, or restriction of, information associated with a party involved in a call (e.g. calling line ID, calling name);

- Relinquish control over a call

  This allows an application to relinquish control over a call but still allowing the established call to continue. Once the control of the call has been relinquished, the application may not be able to regain control over that call.

- Interact with a user

  This provides the ability for an application to interact with a user. An application may be able to send specific information to the user and may request the collection of data from the user. Sending information to the user or collecting information from the user shall be supported when the user is engaged in a call (e.g. USSD, DTMF) or call-unrelated (e.g. USSD, SMS). The information sent to the user may include an indication of an announcement, text or user specific data.

Note 1: Call related user interaction may e.g. be used to play/record/customise user specific announcements while through call-unrelated user interaction e.g. service preferences may be managed.

For each call it shall be possible to specify:

- the events on which monitoring is required ([10]).

Note 2: The mapping to service capabilities is for further study (it shall be investigated to which extend the requirements above fit to CAMEL, MEXE and other service capabilities).

13.2.1.2 PS Session Control functions

This subclause details with PS session control functions. The purpose of this function is to allow applications to control and monitor PS sessions. A PS Session may consists of one or more GPRS PDP context.

Applications should have the ability to :

- Release a PDP context:

  This provides the ability for the application to force a PDP context to be released. The application may provide an indication of the reason for release of the PDP context.

- Control a PDP context:

  This provides the ability for an application to modify the information pertaining to the PDP context at the time of establishment. The application may also allow the PDP context to continue with or without the modified information pertaining to the PDP context. The application shall have the ability to request events to be observed by the network and reported back to the application.

- Monitor a PDP context:

  This provides the ability for an application to monitor for PDP context duration and tariff switching moments.. An application may specify a threshold for the duration of a PDP context or a part thereof. The application shall have the ability to grant new thresholds when the expiry of a previously set threshold has been reported to the application.

- Monitor a PS session:

  This provides the ability for an application to monitor for PS session data volume. An application may specify a threshold for the amount of data allowed to be transferred within a PS session. The application shall have the ability to grant new thresholds when the expiry of a previously set threshold has been reported to the application.

13.2.1.3 IM Session Control functions

IM Session Control

Create IM Sessions
The application shall be able to establish IM sessions between two or more parties with certain media capabilities. The application may add or remove parties at any time for any session. An application may add additional sessions with certain media capabilities between any parties already involved in an session. Sessions with multiple parties may lead to the creation of a multi-media Conference Call. This can either be an ad-hoc conference creation or it can refer to resources that were reserved in advance.

Release IM Sessions
This provides the ability for an application to force the release of an IM session. This may be limited to the release of certain parties from the session or may be the release of all the parties.

Relinquish control over an IM session
This allows an application to relinquish control over IM sessions.

Party join/leave control
The application shall be informed when a new call party wants to join/leave the conference. It shall be possible for the application to allow or reject the inclusion of the new party to a conference.

Presentation of, or restriction of, information associated with a party involved in a session (e.g. calling line ID, calling name);

Media Control

Control media channels
The application shall have the ability to control media channels originated by (or on behalf of) a user or media channels terminated to a user. This control includes, but is not limited to the barring of a media channel request, allowing the media channel establishment to continue with or without modified information, addition or removal of additional media channels, temporarily suspend a media channel (place on hold), open, close or modify the parameters of the media channels.

Relinquish control over specific media channels
This allows an application to relinquish control over the media stream. When it relinquishes control over certain media channels it does not lose control over the entire session.

Reserve/Free conference resources
The application shall be able to reserve resources in the network or free earlier reserved resources for a conference in advance.

Information

Request Notification of Media channel events
The application shall be able to request notification of certain events associated with a type of media channel. Events include, but not limited to: a user initiating or closing a session, an incoming IM session request to user or a terminating user unable to accept an incoming IM session request.

Monitoring of Media channels
The application shall be able to request all the media channels currently available on a IM session In addition the application must be able to monitor the opening and closing of channels for media for a specified session.

13.2.2 Void

13.2.3 Information Transfer function

The Information Transfer function shall enable an application to indicate to a user, or toan application in the UE or USIM about the presence of existing information for the user. Physically, this indication may be sent by the underlying network e.g. as a SMS or USSD message to the terminal. The Information Transfer function provides the means to inform the underlying network that an indication shall be sent to the user.

NOTE: For 3GPP mechanisms like USSD or SMS may be employed to transfer the indication to the users terminal.

The following functions shall be supported:

- **send information notification:**
  - the Send information notification function provides the means to inform the underlying network that an indication shall be sent to a user, or to an application in the UE or USIM about the presence of existing information for the user;
- **request message receipt notification:**
  - the application can request to receive a notification every time a message is received in the mailbox for the user. This allows the application to take the appropriate action, e.g. informing the user.

13.2.4 Charging functions

Call and Event Charging

Call and Event Charging functions enable the application to instruct the network and inform the user with charging information and to add some additional charging information to the network generated Call Detail Records. Some of the following charging facilities are available only if the network either controls the account or has access to it.

The OSA Call and Event Charging function shall enable an application to:

- define and manage thresholds (e.g. session duration, data volume) for a call;
- provide additional charging information to be included in the Call Detail Record. This may contain information transparent to the network;
- transfer Advice of Charge data (as defined in [5]) to the terminal.

Service Usage

These charging functions shall enable applications to augment subscriber accounts maintained by the network and to charge subscribers for using services. These applications are not necessarily telecommunication related. In addition to charging subscribers for service usage, these functions could also be used for payments in an online purchase scenario.

Provided, that these functions are supported by the underlying network an application shall be able to:

- Check, if – for the service to be provided by the application – the charge is covered by the subscribers account or credit limit
- Reserve – for the service to be provided by the application – a charge in the subscribers account, that can be deduced from the account after service delivery.
- Deduct an amount from the subscriber's account. If a reservation has been made earlier, this amount should be taken from the reserved amount.
- Request the network to split the deduction of an amount among several subscribers accounts or other chargeable entities according to a specified partitioning. It shall be possible to notify an individual subscriber's account or other chargeable entity about the percentage of the total amount, to which the deduction has been performed Note: this requirement also covers the case when the total amount to be deduced is calculated by the network.
- Release a reservation acquired earlier. If part of a reservation has been deducted already, just release the remaining reservation.
- Add non-monetary units to a subscriber's account.
- Deduct non-monetary units from a subscriber's account.
- Reverse a completed charge transaction, e.g. after repudiation.

The functions for charging application usage shall meet the following general requirements:

- Hide payment policy (e.g. prepaid/postpaid) from applications
- Hide payment type (credit card, cash, bank withdrawal) from applications
- Hide subscriber's identity towards the application. This would provide anonymity (like for prepaid customers).
- Support prepaid subscribers. This requires that the application immediately gets informed if the subscriber's account covers the service usage costs. If not, the application may reject serving the subscriber.
- Allow for Multi-currency support. This shall allow service providers to request charging in their preferred currency

General Account functions

These functions provide access to sensitive data. They shall be restricted to client applications that had been granted additional privileges via suitable means, i.e. as authorised by the framework function.

The OSA general Account function shall enable an application to:

- retrieve a transaction history of a subscriber's account, this may include
  - the retrieval of a list of monetary or non-monetary amounts that have been debited from or credited to a subscribers online account,
  - the request of additional information on the specific transaction (e.g. the application or service description provided with the actual transaction).
- check a subscriber's current account balance.
- monitor the subscribers account and may request to get informed of any change.
- ask the charged user for an explicit, interactive confirmation before any charging operation is performed. The General Account function will support a procedure to obtain confirmation by the user. Such a procedure shall be under the control of the network.

Note: There is no requirement to standardise this procedure.

In case an application retrieves a list for a subscribers' transaction history, it shall specify the time interval for which the transaction history shall be retrieved.

13.3 User data related functions

13.3.1 User Status functions

The User Status functions enable an application to retrieve the user's status, i.e. to find out on which terminals the user is available.

The following functions shall be provided:

- **retrieval of User Status:**
  - the application shall be able to retrieve the status of the user (e.g. the user is busy, her terminal is attached, or detached).
- **notification of User Status Change:**
  - the application shall receive notifications when the user's terminal attaches or detaches:
    - detach: the user's terminal is switched off or the network initiates detach upon location update failure;
    - attach: the user's terminal is switched on or there has been a successful location update after network initiated detach.
  - the application shall receive notifications when the user’s status moves from idle to busy, or from busy to idle.

Attach and detach applies for CS and PS.

The application shall be able for each terminal to start/stop receipt of notifications.

13.3.2 User Location functions

The User Location functions provide an application with information concerning the user's location.

The user location information contains the following attributes:

- **location** (e.g. in terms of universal latitude and longitude co-ordinates);
- **accuracy** (value depending on local regulatory requirements and level of support in serving/home networks; note that the accuracy of the serving network might differ from that in the home environment);
- **age** of location information (last known date/time made available in GMT).

The following functions shall be provided:

- **report of location information:**
  - the application shall be able to request user location information;
  - by default the location information is provided once; the application may also request periodic location reporting (i.e. multiple reports spread over a period of time).
- **notification of location update:**
  - the application shall be able to request to be notified when the user's location changes, i.e. when:
    - the user enters or leaves a specified geographic area;
    - the user's location changes more than a specified lower boundary. The lower boundary can be selected from the options provided by the network.

The application shall be able for each user to start/stop receipt of notifications and to modify the required accuracy by selecting another option from the network provided options.

- **Access control to location information:**

- the user shall be able to restrict/allow access to the location information. The restriction can be overridden by the network operator when appropriate (e.g. emergency calls).

13.3.3 User Profile Management functions

No requirements for this release are identified.

13.3.4 User Profile access Authentication/Authorisation functions

No requirements for this release are identified.

13.3.5 Terminal Capabilities functions

The Terminal Capabilities functions enable the application to determine the capabilities of the user's terminal .

Note 1: The ability to support this function is dependent on the ability of a terminal (through e.g. MExE or WAP) to notify its terminal capabilities. Therefore this function will *not* be able to supply terminal capabilities for terminals not supporting notification of their terminal capabilities.

Note 2: "Terminal" covers both (mobile) equipment and USIM.

The following functions shall be provided:

- **retrieval of Terminal Capabilities:**
  - the application shall be able to retrieve the capabilities of the terminal. This includes:
    - the media that the terminal is capable to deal with (e.g. audio, video, ; this information is needed by the application e.g. when the user wants to download messages from the mailbox);
    - the number of calls/sessions that the terminal can deal with simultaneously.

13.3.6 Void

13.4 Void

13.5 Presence related capability functions

13.5.1 Relationship to Release 6 Presence Service

The functionality of requirements defined in this set of functions do not refer to the Presence Service that will be supported in Release 6. Any presence information provided and supported by these functions do not supply or support Presence Information as may be defined by the Release 6 Presence Service.

13.5.2 Functions

The OSA interface shall allow an application access to presence capabilities within the network. Presence related information may be requested or supplied by an OSA application and may include, but not limited to presence information or user availability.

An OSA application may act as a requester of presence information (i.e. act as a watcher) and/or act as a supplier of presence information (i.e. act as a presentity).

An OSA application may manage or query availability status and/or preferences of a user which may be associated with one or more services (e.g. voice call, IMS sessions, MMS …etc.). Such availability may be determined from a range of existing capabilities.

The following OSA capabilities shall be supported for an application:

- **register as a presentity and/or watcher:**

  - the application shall be able to request the registration as a presentity and/or as a watcher in the presence service. This registration shall include the ability to establish as well as cancel a registration.

- **supply presence related information to the network:**

  - the application shall be able to supply and/or update presence related information (presence information or availability) at any time. An application may modify the availability of a user. - **request the querying and/or modification of presence related data:**

  - the application shall be able to request the querying and/or modification of data other than presence information related to watchers and/or presentities. Such data includes, but is not limited to any access rules pertaining to the presentity to be modified. An application may be able to request the management of availability preferences of a user. Management includes the setting, modification and deletion of availability preferences.

- **request Presence related Information :**

  - the application shall be able to request presence related information. The application shall be able to request presence information about a presentity or may request the availability of a user. Such requests may be for the current information, on a periodic basis or for future changes in the presence related information (e.g. arming of event notifications).

- **retrieve watcher information:**

  - the application shall be able to request watcher information about a presentity.

Annex A (informative) : Use cases

This informative annex describes how the OSA functions described in the normative section of this document could be used to deploy enhanced multimedia services.

A.1 Service Scenario Description

The service scenario described below is the following: a user has subscribed to a tourist board information service, and each time he will enter a new interesting location the service provider will offer him to watch a video showing the main attractions of the area. The service is charged 1 Euro per movie.

A.2 Step by step description

Note: The following description does not imply any physical location of the different functions, or any mapping between the SCFs and the network capabilities. The processes internal to the different entities are not detailed.

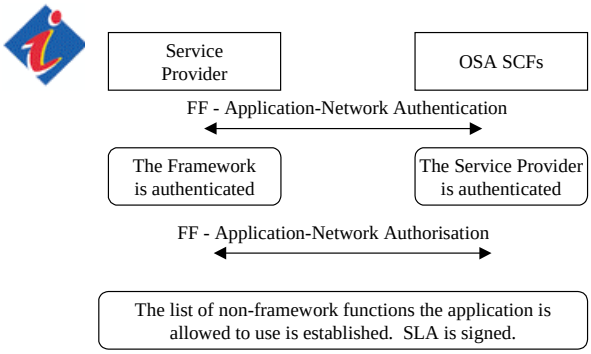
FF: Framework Function

NF: Network Function

UF: User data related Functions

Step 1: On-line Service Level Agreement

This step is intended to sign an on-line service level agreement (SLA) between the information service and the framework.



Step 2: Service initialisation

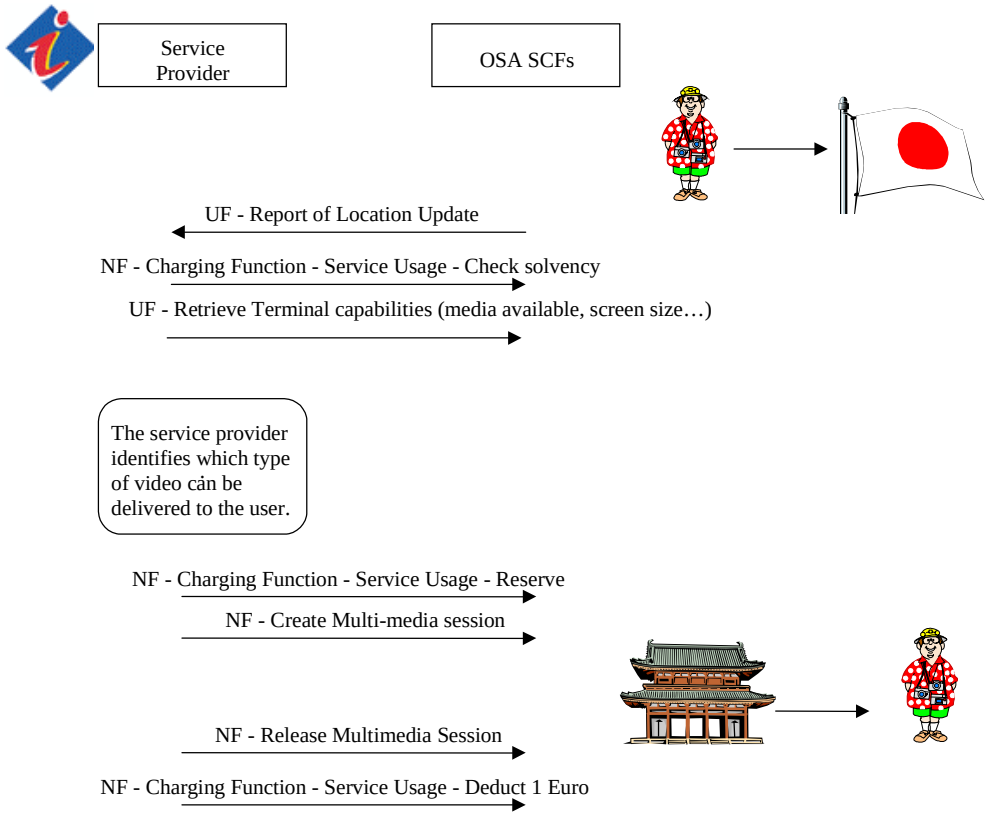
The Service Provider will discover all the service features available in the network (e.g. location update, service usage charging…), and set up the parameters necessary to render the service (i.e. the service provider asks to be notified whenever the user enters a specific geographic area). The list of available service features depends on the SLA.

Note: It is assumed that all the available Service Capability Features have already registered.

Step 3: Service Delivery

The service provider is informed that the user has entered a new geographical area (e.g. Japan). After checking that the user has enough money left on his account, the service provider retrieves the terminal capabilities. Based on this

information, the service provider can determine the type of content that can be sent to the user (for example a black and white video if the terminal does not support colour display,…). The service provider will then reserve 1 € in the account of the subscriber. A multimedia session will be established between the service provider and the user, and the user will then be displayed the sightseeing information. Once the movie's display is over, the session will be released and the service fee will be deducted from the user's account.



Annex B (informative): Change history

Version	Date	Comment
0.0.0	June 2000	Initial Draft (OISP parts extracted from 22.121 v 3.2.0)
0.1.0	July 2000	Output of OISP ad-hoc Retz/Austria, presented to S1 #9 (Taastrup)
0.2.0	July 2000	Output of OISP ad-hoc at S1 #9 (Taastrup)
0.3.0	August 2000	OISP renamed to "Open Service Access" (OSA) , Document number TS 22.127 received from MCC (editorial modification)
0.4.0	September 2000	Output of OSA ad-hoc Sophia-Antipolis
1.0.0	September 2000	Raised to version 1.0.0 by SA#9, identical with version 0.3.0
0.5.0	October 2000	Agreed contribution tdoc S1O00019 included, document tidied up (editorials)
1.0.1	October 2000	Based on 0.5.0 with editorial modification; input to S1 OSA adhoc, 18th to 19th of October 2000.
1.1.0	October 2000	Output of OSA ad-hoc Vienna (S1O00040)
1.1.1	November 2000	Cleanup by editor
1.2.0	December 2000	Edited by OSA ad hoc for presentation to SA #10 for approval.
2.0.0	December 2000	Raised to version 2.0.0 for approval at SA #10.
4.0.0	January 2001	Raised to version 4.0.0 after approval by SA #10.

Change history											
TSG SA#	SA Doc.	SA1 Doc	Spec	CR	Rev	Rel	Cat	Subject/Comment	Old	New	WI
SP-11	SP-010060	S1-010140	22.127	001		Rel-4	F	CR to 22.127 V 4.0.0 on CS Call Control (Release 4)	4.0.0	4.1.0	OSA1
SP-11	SP-010060	S1-010141	22.127	002		Rel-4	F	CR to 22.127 V 4.0.0 on User interaction(Release 4)	4.0.0	4.1.0	OSA1
SP-11	SP-010163	S1-010274	22.127	003		Rel-4	D	Clarify the situation when a user becomes available	4.0.0	4.1.0	OSA1
SP-11	SP-010163	S1-010276	22.127	005		Rel-4	D	Make the Scope more precise description of 22.127	4.0.0	4.1.0	OSA1
SP-11	SP-010163	S1-010277	22.127	006		Rel-4	D	Clarify charging requirements	4.0.0	4.1.0	OSA1
SP-11	SP-010163	S1-010278	22.127	007		Rel-4	D	OSA consistency within stage1 specification	4.0.0	4.1.0	OSA1
SP-11	SP-010164	S1-010279	22.127	008		Rel-4	C	Clarification to the requirements of the Event Notification Function	4.0.0	4.1.0	OSA1
SP-12	SP-010248	S1-010530	22.127	009		Rel-4	F	Detailed requirements for transaction history retrieval	4.1.0	4.2.0	OSA1
SP-12	SP-010248	S1-010391	22.127	011		Rel-4	F	Terminal capabilities	4.1.0	4.2.0	OSA1
SP-12	SP-010248	S1-010531	22.127	010		Rel-5	C	CR on Decoupling the OSA API	4.1.0	5.0.0	OSA1-IOAPI
SP-12	SP-010248	S1-010392	22.127	012		Rel-5	B	Introduction of OSA support to enable Policy Management	4.1.0	5.0.0	OSA1
SP-12	SP-010248	S1-010393	22.127	013		Rel-5	B	De-Registration Function	4.1.0	5.0.0	OSA1
SP-13	SP-010439	S1-010864	22.127	014	1	Rel-5	B	Re-introduction of R5 OSA function; Traceability, CR 22.127 - 14	5.0.0	5.1.0	OSA1
SP-13	SP-010439	S1-010658	22.127	015		Rel-5	B	Re-introduction of R5 OSA function; Multi Media Channel Control CR 22.127-15	5.0.0	5.1.0	OSA1
SP-13	SP-010439	S1-010659	22.127	016		Rel-5	B	Re-introduction of R5 OSA function; Retrieval of Network Capabilities CR 22.127-16	5.0.0	5.1.0	OSA1
SP-13	SP-010439	S1-010660	22.127	017		Rel-5	B	OSA support of information service function CR 22.127-17	5.0.0	5.1.0	OSA1
SP-13	SP-010439	S1-010661	22.127	018		Rel-5	B	OSA support of Presence service function CR 22.127-18	5.0.0	5.1.0	OSA1

Change history											
TSG SA#	SA Doc.	SA1 Doc	Spec	CR	Rev	Rel	Cat	Subject/Comment	Old	New	WI
SP-13	SP-010439	S1-010662	22.127	019		Rel-5	B	OSA requirements for User Data Management CR 22.127-19	5.0.0	5.1.0	OSA1
SP-13	SP-010439	S1-010663	22.127	020		Rel-5	B	OSA requirements on User Profile Access Management CR 22.127-20	5.0.0	5.1.0	OSA1
SP-13	SP-010439	S1-010664	22.127	021		Rel-5	F	Correction of Scope statement CR 22.127-21	5.0.0	5.1.0	OSA1
SP-13	SP-010436	S1-010890	22.127	024	1	Rel-5	F	Definitions of Home Environment and HE-VASP	5.0.0	5.1.0	VHE1
2001-10-09			22.127			Rel-5		Editorial correction of Specification	5.1.0	5.1.1	Correct
SP-14	SP-010675	1105	22.127	026		Rel-5	F	CR to TS 22.127 v 5.1.1, (Cat F R5)on OSA Information Service Modification	5.1.1	5.2.0	OSA1
SP-14	SP-010675	1107	22.127	027		Rel-5	C	CR to TS 22.127 v 5.1.1, (Cat C R5) User Data Management Modifications	5.1.1	5.2.0	OSA1
SP-14	SP-010675	1108	22.127	028		Rel-5	C	CR to TS 22.127 v 5.1.1, (Cat C R5) User Data Management Security Modifications	5.1.1	5.2.0	OSA1
SP-14	SP-010675	1109	22.127	029		Rel-5	D	CR to TS 22.127 v 5.1.1, (Cat D R5) Editorial corrections for the Support of Presence Service	5.1.1	5.2.0	OSA1
SP-14	SP-010675	1111	22.127	030		Rel-5	F	CR to TS 22.127 v 5.1.1, (Cat F R5) High Level requirements concerning OSA impact on SCF´s	5.1.1	5.2.0	OSA1
SP-14	SP-010675	1112	22.127	031		Rel-5	C	CR to TS 22.127 v 5.1.1, (Cat C R5) Support for presence related capability functions	5.1.1	5.2.0	OSA1
SP-14	SP-010675	1113	22.127	032		Rel-5	C	CR to TS 22.127 v 5.1.1, (Cat C R5) Backward Compatibility	5.1.1	5.2.0	OSA1
SP-14	SP-010675	1344	22.127	033		Rel-5	B	CR to TS 22.127 V 5.1.1 (Cat B R5) Adding IM Session Control Funct	5.1.1	5.2.0	OSA1
SP-15	SP-020054	S1-020267	22.127	034		Rel-5	D	Editorial Corrections	5.2.0	5.3.0	OSA1
SP-15	SP-020054	S1-020268	22.127	035		Rel-5	B	OSA use cases	5.2.0	5.3.0	OSA1
SP-15	SP-020054	S1-020269	22.127	036		Rel-5	C	CR on Network Capability Retrieval	5.2.0	5.3.0	OSA1
SP-15	SP-020054	S1-020270	22.127	037		Rel-5	F	Clarification of OSA functions related to user´s status	5.2.0	5.3.0	OSA1
SP-15	SP-020054	S1-020271	22.127	038		Rel-5	F	CR to 22.127 R5 on Correction of Service Capability Feature to SC Server	5.2.0	5.3.0	OSA1
SP-15	SP-020054	S1-020283	22.127	039		Rel-5	C	CR on Charging Requirements	5.2.0	5.3.0	OSA1
SP-15	SP-020054	S1-020338	22.127	040		Rel-5	F	Security requirements on User Profile Management	5.2.0	5.3.0	OSA1
SP-15	SP-020054	S1-020591	22.127	041		Rel-5	C	CR to 22.127 R5 on Charging Requirements	5.2.0	5.3.0	OSA1
SP-15	SP-020045	S1-020457	22.127	043	-	Rel-5	A	Editorial CR to correct terms and references	5.2.0	5.3.0	CORRECT
SP-16	SP-020249	S1-020868	22.127	044		Rel-5	F	Reduction of scope of OSA R5	5.3.0	5.4.0	OSA1
SP-16	SP-020249	S1-020903	22.127	045		Rel-5	F	Proposal to remove feature "Retrieval of Visited Network Capabilities' from OSA Release 5'	5.3.0	5.4.0	OSA1
SP-16	SP-020249	S1-021059	22.127	046		Rel-5	F	A more Flexible Event Notification mechanism	5.3.0	5.4.0	OSA1
SP-16	SP-020249	S1-020867	22.127	047		Rel-5	F	Clarifications of the terms used for the control of GPRS Sessions and IM Sessions	5.3.0	5.4.0	OSA1
SP-16	SP-020249	S1-021171	22.127	048		Rel-5	F	Removal of Presence Service	5.3.0	5.4.0	OSA1
SP-18	SP-020652	S1-022250	22.127	058		Rel-5	F	Event notification mechanism to inform applications about new SCS	5.4.0	5.5.0	OSA3

History

Document history		
V5.3.0	March 2002	Publication
V5.4.0	June 2002	Publication
V5.5.0	December 2002	Publication