Technical Specification Group Services and System Aspects **TSGS#9(00) 0417**
Meeting #9, Hawaii, USA, 25-28 September 2000

Source:	**TSG SA1**
Title:	**TS22.127 v 1.0.0 "Service Requirement for the Open Services Access (OSA)"**
Document for:	**Information**
Agenda Item:	**7.1.3**

This specification is presented to SA #9 for information.

3G TS 22.127 1.0.0 (2000-08)

Technical Specification

3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects
Service aspects;
Service Requirement for the Open Services Access (OSA)
Stage 1
(Release 2000)

Reference

DTS/TSGS-0122121U

Keywords

<keyword[, keyword]>

3GPP

Postal address

3GPP support office address

650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet

http://www.3gpp.org

Contents

Foreword

This Technical Specification has been produced by the 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 this TS, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version 3.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 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 specification;

1 Scope

This document specifies the stage 1 requirements for realisation of an Open Services Access (OSA). OSA realises the standardised interface towards the network that is required for the Framework for Services in the VHE stage 1 description [1].
This document is only applicable to OSA release 2000 and later. In Release 99 Service requirements are described in the VHE stage 1 description [1].

Within the concept of VHE [1] OSA enables operator- and third party applications to make use of network functionality through an open standardised interface (the OSA API). OSA provides the glue between applications and service capabilities provided by the network. In this way applications become independent from the underlying network technology.

Applications make use of service capability features offered through the OSA interface. Applications using OSA are not standardised by 3GPP.

2 References

References may be made to:

a) Specific versions of publications (identified by date of publication, edition number, version number, etc.), in which case, subsequent revisions to the referenced document do not apply; or

b) All versions up to and including the identified version (identified by "up to and including" before the version identity); or

c) All versions subsequent to and including the identified version (identified by "onwards" following the version identity); or

d) Publications without mention of a specific version, in which case the latest version applies.

A non-specific reference to an ETS shall also be taken to refer to later versions published as an EN with the same number.

2.1 Normative references

[1] UMTS TS 22.121: Universal Mobile Telecommunications System (UMTS); “The Virtual Home Environment”

[2] UMTS TR 22.976

2.2 Informative references

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

Definitions and abbreviations

3.1 Definitions

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

Applications: software components providing services to end-users by utilising service capability features.
Application Interface: standardised Interface used by applications to access service capability features.
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.
Services: services are made up of different service capability features.
Virtual Home Environment: For the definition see [1]
Value Added Service Provider: For the definition see [1]
HE-VASP: Home Environment Value Added Service Provider. For the definition see [1]
Local Service: For the definition see [1]
Service Execution Environment: For the definition see [1]
Personal Service Environment: For the definition see [1]
Home Environment: For the definition see [1]
User: For the definition see [1]
User Profile: For the definition see [1]
User Interface Profile: For the definition see [1]
User Services Profile: For the definition see [1]

Further UMTS related definitions are given in 3G TS 22.101.
Editors note: above list will be checked for constancy and completness.

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
PSE	Personal Service Environment
VHE	Virtual Home Environment
OSA	Open Services Access
SCF	Service Capability Feature

Further GSM related abbreviations are given in GSM 01.04. Further UMTS related abbreviations are given in UMTS TS 22.01.

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 Services Access (OSA) enables applications to make use of network capabilities. The applications will access the network through the OSA interface that is specified in this Technical Specification.

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 application developers can rely when designing new applications (or enhancements/variants of already existing ones).

The aim of OSA is to provide an extendible and scalable interface that allows for inclusion of new service capability features and SCSs in future releases of UMTS 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 UMTS with respect to services is to provide a framework within which services can be created based on standardised service capability features (c.f. [1]). UMTS 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.

Services can be built using service capability features [1], which are accessed via OSA, a standardised interface towards these SCFs in the network.
An example of how a service can be built on service capability features could be "call to nearest restaurant", this will make use of call set-up, authorisation, location and database lookup.

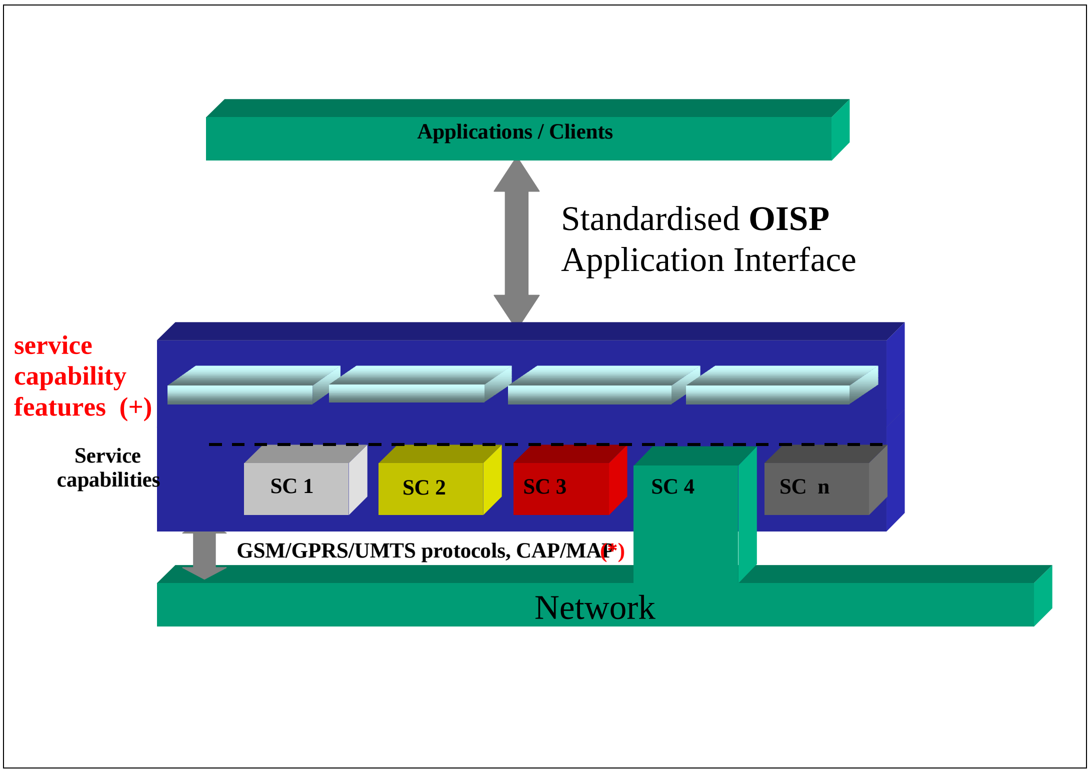

Figure 3: Applications access Service Capability Features via the standardised OSA Application Interface

High level requirements to OSA

The following high level requirements apply to OSA:

- the standardised application interface shall be independent of vendor specific solutions;

- independence of programming languages, operating systems 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;
- 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.

Editor’s Note:
1.) It needs to be addressed that OSA allows access to only those SCFs that belong to the operator that operates the OSA interface
2.) Fine grained authorisation needs to be addressed

Requirements for user data management

Editor's note: e.g. Requirements for the support User specific data management. This concerns accessibility, privacy, etc of User (Profile) data. The user profile (architecture, location, content ..) is currently under investigation by groups like VHE, MExE, S2, T2... FFS.

This chapter reflects requirements from application point of view.
Level of authorisation: Service vs. Subscriber level.
It is assumed, that the data structure and distribution of the user profile need not be known to define the level of authorisation.

8 Charging and traceability requirements

8.1 Charging requirements

The OSA shall offer sufficient charging options to:

- Supervise user activities for online charging features,
- allow applications to access the account. This could be done by e.g. accessing an online account or impact the postprocessing.
- Allow applications to add charging information to network based charging records
- Inform applications on network based charging event

Editor's note: Other charging requirements may be identified and are for FFS.

8.2 Traceability requirements

Editor's note: Applications, that use the OSA interface, may perform actions in the network that might cause costs or undesired effects to the user or operator.
Requirements for traceability of such actions may be identified and are for FFS.

The OSA shall provide sufficient capabilities to allow applications to fulfil traceability requirements for 3GPP. FFS

9 Security requirements

Editor’s note: FFS.

Relation with chapter 7 exists.

10 Service Capability Features

Services Capability Features are open, technology independent building blocks accessible via a standardised application interface. This interface 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, fully interactive multimedia to using MS based applications.

The service capability features shall enable applications to make use of the service capabilities (e.g. CAMEL, MExE, etc.) of the underlying UMTS network in an open and secure way.

Application/Clients access the service capability features via the standardised application interface. This means that a single service capability feature is accessible and visible to application/clients via the method/operation invocations in the interface.

Two different types of service capability features can be distinguished:

- **Framework service capability feature**: this SCF shall provide commonly used utilities, necessary for the non-framework service capability features to be accessible, secure, resilient and manageable;

- **Non-Framework service capability features**: these shall enable the applications to make use of the functionality of the underlying network capabilities (e.g. User Location service capability features).

10.1 The Framework service capability feature

Editor’s Note: Clarification / Input to this chapter expected from LUCENT

The Framework service capability feature will be used e.g. for authentication, authorisation, registration, notification, etc. and provide functionality that is independent of any particular type of service.

10.1.1 Trust and Security Mangement function

It provides mechanism for applications and framework to initiate communications, authenticate each other and mechanism for applications to be authorised and access network capability features.

Editors Note: text above taken from R99 but needs more clarification.

10.1.2 Integrity Management function

It provides the support of integrity for both the OSA APIs and the application (e.g. load manager, fault manager. OAM and Heartbeat manger)

Editors Note: text above taken from R99 but needs more clarification.

10.1.3 Authentication function

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 provider 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.*

10.1.4 Authorisation function

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:** the network verifies what non-framework service capability features s or framework service capability feature the application is allowed to use. Once an application has been authorised to use one, more or all (non-framework) service capability features no further authorisation is required as long as the "allowed" (non-framework) service capability features 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*.

10.1.5 Registration function

The Registration functionenables the non-framework service capability features (e.g. User Location) to register at 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.
Note that only the non-framework service capability features have to be registered. The Framework service capability features (defined in subclause 10.1) are available by default since they provide basic mechanisms.

10.1.6 Discovery function

The Discovery functionenables the application to identify the total collection of service capability features that it can use. Upon request of the application, the Discovery functionwill indicate the non-framework service capability features that are available for the application. The list of available service capability features is created through the Registration process described in subclause 10.1.3. This means that a service capability feature must be registered at the Framework before it can be discovered by the application.

Editor's Note: It was agreed that a requirement for a notification functionality should be stated in the relevant SCFs whenever applicable and not as a standalone function..
Such a notification functionality should allow applications to enable, disable and receive notifications of application related events that have occurred in the underlying GSM/UMTS network (e.g. indication that a new call is set-up or a message is received).

10.2 Non-Framework (Network) service capability features

The Non-Framework service capability features represent the total collection of service capability features that are not included in the Framework. These non-framework service capability features enable the application to make use of the functionality provided by the network and service capabilities.

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 functionality that is provided by more than one service capabilities. For example, User Location can be produced in several underlying ways. This functionality can be captured once when defined the service capability features in a generic way. It is important that the generic part becomes as large as possible.

When applications use the generic service capability features, these applications become independent of (portable over) underlying service capabilities. Applications shall however still be able to request service capability features specific to a service capability (e.g. Call Setup from CAMEL). This will increase dependency of the used service capability.

The following subclauses define generic service capability features e.g. for Session Control and Message Transfer.

10.2.1 Data Session Maintenance service capability features

This subclause details the Data Session Maintenance service capability features. The purpose of this SCF is to provide Quality of Service to the application if requested before. The QoS could be requested when negotiated or whenever it is changed.

Applications should always have the option to :

- allow the session to continue with modified information (e.g. changed destination number);
- release the session (i.e. removing all parties from the session);
- request session information (i.e. information like session duration, session end time);
- supervise session (e.g. monitor for session duration or data volume, tariff switching moments and changes in QoS);
- presentation of, or restriction of, information associated with a party involved in a session (e.g. calling line ID, calling name);
- collect information from user (i.e the application shall be able to request data from the user. For example, the user might enter some code number).

For each session it shall be possible to specify:

- the events on which monitoring is required ([3]).

NOTE: 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).

Editor's Note: Clarification / Input to this chapter expected from ERICSSON

Editor's Note: It was agreed that Security/Privacy issues (such as encryption of user data and signalling) should be addressed as function in affected SCFs and not as a standalone SCF .

10.2.2 IP Multimedia Handling SCF

In IP Multimedia calls the media channels are negotiated between the parties in the call. Which media channels are opened depends on the requirements of the service in the terminal handling the call, the user profile and the terminal capabilities.

Editor's note: The IP Multimedia Handling SCF does not impact the Data Session Maintainance SCF

Multi-Media Channel Control:
These capabilities allow an application to control individual channels in an IP Multimedia session. An application shall be capable of:

- **Notification of Media channel events**
  The application shall be able to be notified when a certain type of media channel is opened or closed. This may be dependent on additional criteria (tbd.)
- **Information/Monitoring of Media channels**
  The application shall be able request all the media channels currently available on the call Leg. In addition the application must be able to monitor on the opening and closing of channels for media for a specified call leg.
- **Media channels Open/Close/Modify**
  The application shall be able to open, close and modify the parameters of a media channel on a certain call leg.

Multi-Media Conference Call Control:

- **Reserve/Free conference resources**
  The application shall be able to reserve or free earlier reserved resources for a conference in advance.
- **Create Multi-media Conference**
  The application shall be able to create an IP Multi-media Conference Call. This can either be an add-hoc conference creation or it can refer to resources that were reserved in advance
- **Party join/leave control**
  The application shall be capable to be informed when a new call party wants to join/leave the conference. It shall be possible to attach the call leg to the conference or reject the join

Editors Note: It may become necessary to modify or add to this list of capabilities according to the IM call control model based on SIP

10.2.4 Information Transfer service capability features

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

NOTE: For UMTS release 99 mechanisms like USSD or SMS may be employed to transfer the indication to the users terminal.

The following service capability feature shall be supported:

- **send information notification:**
  - the Send information notification service capability feature provides the means to inform the underlying network that an indication shall be sent to a user respectively an application in the UE or USIM about the presence of existing information for her;
  - this indication shall contain sufficient information for the receiving entity to react in an appropriate manner, e.g. an announcement ID, URL, a string, etc. In addition the application or execution environment in the terminal (e.g. MExE SAT), that is to display this information, needs to be referenced.
- **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.

10.2.5 Charging service capability features

The Charging service capability features 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.
The following service capability features shall be provided:

- define and manage the threshold (e.g. session duration, data volume) for the required service;
- send charging data (this data is included in a "free format" field in the network generated Call Detail Records. It may contain information like a application generated Call Id, used by the application provider to relate application generated charging information to the network generated charging information);
- transfer of Advice of Charge data (as defined in GSM02.24) to the terminal.

An application providing a service to the user shall be able to:

- Check, if – for the service to be provided by the application – the charge is covered by the users account.
- Reserve – for the service to be provided by the application – a charge in the users account, that can be deduced from the account after service delivery.
- Retrieve a transaction history of it's charging activity

The OSA interface shall be able to:

- Hide payment policy (e.g. prepaid/postpaid) from application providers
- Hide payment type (credit card, cash, bank withdrawal) from application providers
- Hide subscriber’s identity towards the application service provider. This would provide anonymity (like for prepaid customers).
- Allow for Multi-currency support. This shall allow application providers to request charging in their preferred currency

10.3 User data related capability features

10.3.1 User Status service capability features

The User Status service capability features enable an application to retrieve the user's status, i.e. to find out on which terminals the user is available.
The following service capability features shall be provided:

- **retrieval of User Status:**
  - the application shall be able to retrieve the status of the user.
- **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 on 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 be able for each terminal to start/stop receipt of notifications.

10.3.2 User Location service capability features

The User Location service capability features 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 service capability features 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).

Editors note: should be checked for potential mismatch with LCS

10.3.3 User Profile Management service capability features

The User Profile Management service capability features allow the application to retrieve the user profile (see subclause 7 for more information on user profiles).
In R99 the retrieval was limited to terminal capabilities (in case when provided by the terminal) and Camel facilities (ATI, ATM and ATN).
In addition to the R99 utilities, the User Profile Management SCF shall provide all subscriber information allowed for retrieval. What kind of subscriber information may be exposed to the applicationdepends on the level of authorisation needed for information retrieval. For a more detailed definition of the authorisation level, see chapter 7.
Applications using the UPM SCF may need to authorise themselves before. The authorisation depends on the sensitivity of the requested user profile information. The authorisation information provided by the application will be verified at the network.
If authorisation is needed, the User Profile access Authentication/Authorisation SCF will be involved.

10.3.4 User Profile access Authentication/Authorisation SCF

Editor's note: The application might need to prove it's authorisation to retrieve/modify certain user data. FFS.
Question: isn't that covered in the previous chapter ?

10.3.5 Terminal Capabilities service capability features

The Terminal Capabilities service capability features enable the application to find out what capabilities the user's terminal supports (note: "terminal" covers both (mobile) equipment and USIM).

The following service capability features 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, PC data, WAP data; 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.

Editor's Note: The limitation from R99 to retrieve Terminal information from WAP terminals only shall be removed. Above Requirements shall apply to any type of terminal.

10.3.6 Home- and visited Network Capabilities service capability features

Editor's note: The application might need to know the capabilities of the (visited) network. FFS.

Annex B (informative): Change history

Change history										
TSG SA#	**SA Doc.**	**SA1 Doc**	**Spec**	**CR**	**Rev**	**Rel**	**Cat**	**Subject/Comment**	**Old**	**New**

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 Services Access" (OSA) , Document number TS 22.127 received from MCC (editorial modification)
1.0.0	Sept. 2000	Raised to version 1 for presentation to SA #9

Rapporteur: Jörg Swetina (SIEMENS AG)

Email: joerg.swetina@siemens.at Telephone: +43-51707-21422