Technical Specification Group Services and System Aspects
Meeting #10, Bangkok, Thailand, 11-14 December 2000

TSGS#10(00)0551

Source: **TSG SA1 OSA adhoc group**

Title: **Cover sheet to 22.127 version 2.0.0**

The attached document was endorsed within 3GPP TSG SA1 OSA adhoc group. The document describes OSA requirements for Release 4.

3GPP TSG SA1 gave authorisation to the OSA adhoc group to submit the document to 3GPP TSG SA for approval.

The attached document is submitted for approval for Release 4.

It describes OSA requirements for Release 4 only.

3G TS 22.127 2.0.0 (2000-12)

Technical Specification

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

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

Contents 4

Foreword 5

1 Scope 6

2 References 6
2.1 Normative references 6
2.2 Informative references 6

3 Definitions and abbreviations 7
3.1 Definitions 7
3.2 Abbreviations 7

4 General Description of OSA 8

5 The role of OSA within the VHE framework for services 8
5.1 Physical location of applications using the OSA interface 9

6 High level requirements to OSA 9

7 Requirements for user data management 9

8 Charging and traceability requirements 9
8.1 Charging requirements 9
8.2 Traceability requirements 10

9 Security requirements 10
9.1 Security requirements on User Profile management 10

10 Requirements for Policy Management 11

11 Event Notification Function 11
11.1 Subscriber Related events: 11
11.2 Network Related Events: 11

12 Functions offered by OSA 12
12.1 The Framework functions 12
12.1.1 Trust and Security Mangement 12
12.1.1.1 Authentication 12
12.1.1.2 Authorisation 13
12.1.2 Service Registration feature 13
12.1.3 Service Discovery feature 13
12.1.4 Integrity Management function 13
12.2 Network functions 14
12.2.1 Call Control functions 14
11.2.1.1 CS Call Control functions 14
12.2.1.2 PS Call Control functions 15
12.2.1.3 IM Call Control functions 15
12.2.2 Multi-Media Channel Control: 15
12.2.3 Information Transfer function 16
12.2.4 Charging functions 16
12.3 User data related functions 17
12.3.1 User Status functions 17
12.3.2 User Location functions 17
12.3.3 User Profile Management functions 18
12.3.4 User Profile access Authentication/Authorisation functions 18
12.3.5 Terminal Capabilities functions 18
12.3.6 Functions for retrieval of Network Capabilities 18

Annex A (informative): Change history 18

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 Service 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 4. In Release 99 Service requirements are described in the VHE stage 1 description [1].
Within the concept of VHE OSA enables operator- and third party services to make use of network functionality through an open standardised interface (the OSA API). OSA provides the glue between services and network functionality. In this way applications implementing the services become independent from the underlying network technology.
Applications make use of network functionality offered through the OSA interface. Services using OSA APIs 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] 3G3G TS 22.121: Universal Mobile Telecommunications System (3G); “The Virtual Home Environment”

[2] 3G3G TS 22.101: Service principles

[3] 3G3G TS 21.905: Vocabulary for 3GPP Specifications

[4] 3G3G TS 23.107: QoS Concept and Architecture

[5] 3G3G TS 22.024: Description of Charge Advice Information (CAI)

[6] 3G TS 29.198: Open Service Architecture; Application Programming Interface; Part 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:
Applications: software components providing services to users by utilising service capability features.
Application Interface: standardised Interface used by applications to access service capability features.
Billing: A function whereby CDRs generated by the charging function are transformed into bills requiring payment.
Call: A logical association between several users (this could be connection oriented or connection less).
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 [1]
Home Environment: For the definition see [1]
Local Service: For the definition see [1]
Personal Service Environment: For the definition see [1]
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 Execution Environment: For the definition see [1]
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]
Value Added Service Provider: For the definition see [1]

Further 3G3G related definitions are given in 3G TS 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
PSE	Personal Service Environment
VHE	Virtual Home Environment
OSA	Open Service Access
SCF	Service Capability Feature
MExE	Mobile Execution Environment

Further GSM related abbreviations are given in GSM 01.04.
Further 3G3G related abbreviations are given in 3G3G 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, extendible and scalable interface that allows for inclusion of new functionality in the network and/or by third party service providers in future releases 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 3G with respect to services is to provide a framework within which services can be created based on standardised service capability features (c.f. [1]). 3G 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 3G (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.

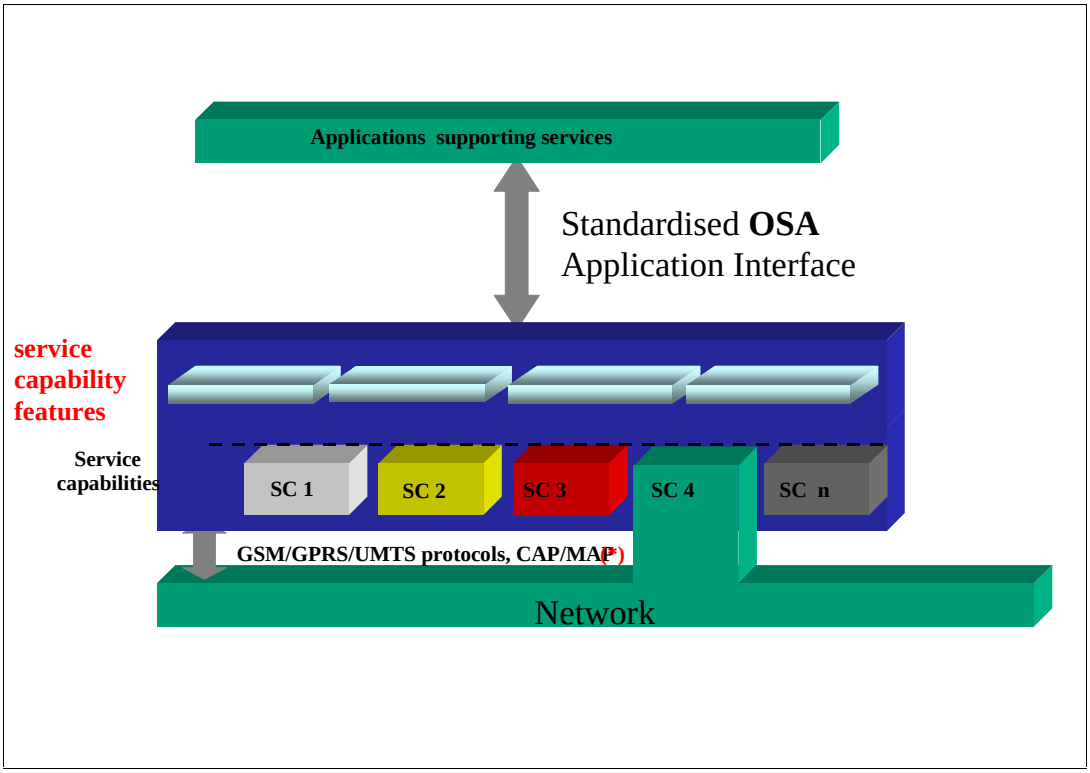

Figure 3: Applications access Service Capability Features via the standardised OSA Application Interface

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 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.;
- OSA shall be aligned as far as possible with equivalent work in other bodies, such as ETSI SPAN and Parlay;
- 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.

7 Requirements for user data management

No requirements for this release are identified

8 Charging and traceability requirements

8.1 Charging requirements

The charging functionality of OSA allows an application to charge a subscriber's account for the services provided to her. It enables the invoice of soft (e.g. download of software, music,...) and hard goods (e.g. CDs, books,...) (which potentially are provided by third parties) to the operator. Additionally, the charging functionality of OSA shall provide for the maintenance of non-monetary subscriber accounts. The operator (or possibly third parties) 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 OSA client 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 Charging: Within OSA Call Control, an OSA application shall be able to control the charging of a call that is under supervision of this application. OSA shall allow for the following options:
- The service provider defines how much is charged to the subscriber for the usage of the service.
- The charges for the call are split between the involved parties (subscriber and service provider)
- The revenue for the call is split between the network operator and the service provider.
- Allow services to add information to network based charging records

Service Usage (e.g. Online Purchases): On the other hand, OSA shall allow to employ the charging and billing capabilities of the network to charge subscribers for any kind of service or even online purchases. This includes:
- Enable the operator to add charges to a subscriber's account for any (non-telecommunication) related service
- Enable the operator to provide charging/billing as a service to 3rd parties, typically service providers. In this case, the operator will charge subscribers for service usage on behalf of the service provider. The charged amounts may be shared between to the service provider and the network operator, but this is outside the scope of the specification.
- Enable the operator to add non-monetary units to a subscriber's account.
- Enable the operator to deduct non-monetary units from a subscriber's account.
- Enable the operator to provide non-monetary accounting capabilities to 3rd parties, typically application providers.
- Enable the operator to reverse a completed charge transaction, e.g. after repudiation.
- Enable the operator to provide charge reversal capabilities to 3rd parties.

Beyond this, there are **general operations** 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).

8.2 Traceability requirements

No requirements for this release are identified.

9 Security requirements

9.1 Security requirements on User Profile management

No requirements for this release are identified.

10 Requirements for Policy Management

No requirements for this release are identified.

11 Event Notification Function

The Event Notification Function shall allow an application to specify the initial point of contact which it is interested in. It provides the necessary mechanisms which enables an application to request a notification if a subscriber or network related event occurs.
For all subscriber Related Events the application shall always specify the subscriber for which the Event Notification Function is valid.
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 above are described in [6].

11.1 Subscriber Related events:

- A new network service or network service capability registers,
  when a new network service capability feature registers with the Registration Function and this event is armed by an application, that application shall be notified.
- A user becomes available.
  when a subscriber registers to a network and this event is armed by an application, that application shall be notified.
- 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 given user changes her status (e.g. from idle to busy) and this event is armed by an application, that application shall be notified.

- 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 a given user changes her terminal capabilities (e.g. from non MExE to a MExE capable terminal) and this event is armed by an application, that application shall be notified.

11.2 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.

12 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.

12.1 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*.

12.1.1 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.

12.1.1.1 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.

12.1.1.2 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.

12.1.2 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.
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.

12.1.3 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.

12.1.4 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.

12.2 Network functions

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

12.2.1 Call Control functions

This subclause details with Call Control functions. The purpose of this function is to allow applications to control and monitor calls.
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 Control Function allows applications to monitor the amount of used traffic channels and bandwidth (e.g. for HSCSD) and used timeslots (e.g. for GPRS).

11.2.1.1 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 :

- **Create Calls:**
  This provides the ability for an application to initiate a new call on behalf of a subscriber. Once the call has been initiated, the application may apply the functions described in this subclause.

- **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 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 in progress. Such requested information includes 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.

- **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. The information sent to the user may include an indication of an announcement, text or user specific data.

For each call it shall be possible to specify:
- the events on which monitoring is required ([10]).

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).

12.2.1.2 PS Call Control functions

This subclause details with packet switched call control functions. The purpose of this function is to allow applications to control and monitor GPRS sessions. A GPRS Session may consists of one or more GPRS PDP context.
Applications should have the ability to :

- **Create a PDP context:**
  This provides the ability for an application to initiate a new PDP context on behalf of a subscriber. Once the PDP context has been initiated, the application may apply the functions described in this subclause.

- **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 GPRS session:**
  This provides the ability for an application to monitor for GPRS session data volume. An application may specify a threshold for the amount of data allowed to be transferred within a GPRS 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.

12.2.1.3 IM Call Control functions

No requirements for this release are identified

12.2.2 Multi-Media Channel Control:

No requirements for this release are identified.

12.2.3 Information Transfer function

The Information Transfer function 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 function provides the means to inform the underlying network that an indication shall be sent to the user.

NOTE: For 3G release 99 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 respectively an application in the UE or USIM about the presence of existing information for her;
- **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.

12.2.4 Charging functions

Call Charging

The 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 following functions 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 to relate application generated charging information to the network generated charging information);
- transfer of Advice of Charge data (as defined in [5]) to the terminal.

Service Usage

These OSA functions shall enable service providers to use subscriber accounts maintained by the network to charge subscribers for using their application. Services provided by these service providers are not necessarily telecommunication related. In addition to charging subscribers for service usage, these operations could also be used for payments in an online purchase scenario.

Provided, that these functions are supported by the underlying network an application providing a service to the subscriber 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.
- 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 operations 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 Operations

These operations provide access to sensitive data. They shall be restricted to client applications that had been granted additional privileges via suitable means.

- The OSA application shall be able to retrieve a transaction history of a subscriber's account
- The OSA application shall be able to check a subscriber's current account balance.

12.3 User data related functions

12.3.1 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.
- **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 be able for each terminal to start/stop receipt of notifications.

12.3.2 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).

12.3.3 User Profile Management functions

No requirements for this release are identified.

12.3.4 User Profile access Authentication/Authorisation functions

No requirements for this release are identified.

12.3.5 Terminal Capabilities functions

The Terminal Capabilities functions enable the application to find out what capabilities the user's terminal supports (note: "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.

12.3.6 Functions for retrieval of Network Capabilities

No requirements for this release are identified

Annex A (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 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.

Rapporteur: Jörg Swetina (SIEMENS AG)

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