1. Scope

This document defines the requirements for the OMA Parlay Service Access (PSA) APIs v.1.0.

The aim of this OMA PSA RD is to address (per OMA processes) those requirements in [3GPP TS 22.127] for which no technical work has been done in 3GPP and for which the responsibility of defining the resulting solution specification has been moved to OMA ARC WG. For this reason, no new requirements with respect to those frozen 3GPP Release 8 Stage 1 ones will be considered as part of this OMA PSA APIs v.1.0.

Applications/enablers which make use of network functionality offered through the PSA interface are out of scope of this document.
2. References

2.1 Normative References


2.2 Informative References

[3GPP TS 23.198] “Open Service Access (OSA); Stage 2”, TS23.198
URL: http://www.3gpp.org/ftp/Specs/html-info/23198.htm

[3GPP TS 29.198] “Open Service Access (OSA); Application Programming Interface (API)” TS29.198 Series
URL: http://www.3gpp.org/ftp/Specs/html-info/29-series.htm

[3GPP TS 29.199-02] “Open Service Access (OSA); Parlay X Web Services, Part 2: Third party call”, TS 29.199-02, Release 8,
URL: http://www.3gpp.org/ftp/Specs/html-info/29-series.htm

[3GPP TS 29.199-xx] “Open Service Access (OSA); Parlay X Web Services”, TS29.199-01 to TS 29.199-22, Release 8,
URL: http://www.3gpp.org/ftp/Specs/html-info/29-series.htm

[PIOSE] “Parlay In OSE”, Version 1.0, Open Mobile Alliance™, OMA-RP-PIOSE-V1_0,
URL:http://www.openmobilealliance.org/
3. Terminology and Conventions

3.1 Conventions

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in [RFC2119].

All sections and appendixes, except “Scope” and “Introduction”, are normative, unless they are explicitly indicated to be informative.

3.2 Definitions

- **OSA API**
  See Parlay API

- **Parlay API**
  A suite of API specifications, also referred to as OSA API, with which service application developers can access to network functionality, features and enablers through a secure, open, standardised interface. The Parlay APIs are defined using UML as the methodology with which to specify interface classes, methods, parameters and state transition diagrams. This set of UML based APIs supports three different technology realizations as described below.

  - **Parlay - CORBA/IDL Realization**
    A realization of the Parlay UML model in OMG IDL.

  - **Parlay - Java Realization**
    A realization of the Parlay UML model in Java.

  - **Parlay - Web Services Realization**
    A realization of the Parlay UML model in WSDL.

  - **Parlay X (API)**
    Parlay X provides simple, abstracted Web Services-based use of network functionality, features and enablers, consistent with the Parlay APIs and supplemented where necessary to meet the needs of Web Service developers. The Parlay X APIs are defined as WSDLs, which are not derived from the Parlay UML, and conform to a defined Web Services styleguide.

3.3 Abbreviations

- **CORBA**
  Common Object Request Broker Architecture

- **IDL**
  Interface Definition Language

- **JEE**
  Java Enterprise Edition

- **JSE**
  Java Standard Edition

- **OMA**
  Open Mobile Alliance

- **OMG**
  Object Management Group

- **OSA**
  Open Service Access

- **UML**
  Unified Modeling Language

- **WSDL**
  Web Services Description Language
4. Introduction

Open standardised APIs can be used to provide the glue between (IT) applications and telecom network functionality via secure, measured, and billable interfaces, making the applications implementing the services independent from the underlying network technology.

By releasing developers from underlying networks and environments, such open APIs to access network services expands the possible set of applications and allows network function owner to change implementations without changing applications.

The 3GPP [3GPP], in collaboration with its specification partners ETSI TISPAN [ETSI TISPAN] and Parlay Group [Parlay] industry consortium, has produced the OSA APIs (3GPP TS 23.198) "Open Service Access (OSA); Stage 2", TS23.198


[PIOSE] “Parlay In OSE”, Version 1.0, Open Mobile Alliance™, OMA-RRP-PIOSE-V1_0, URL:http://www.openmobilealliance.org/


Error! Reference source not found.), a set of technology-independent functionally-rich interfaces for a broad range of telecommunications enablers including Call Control, Messaging, Location, Presence, Policy, Charging etc., and a set of abstracted Telecom Web Services, Parlay X (3GPP TS 23.198) "Open Service Access (OSA); Stage 2", TS23.198


The Parlay APIs and Web Services may be used to promote easier access to and exploitation of both Parlay Service Capabilities and OMA enablers in the global developer community.

The Parlay In OSE (PIOSE) Enabler provides an OMA perspective on the use of Parlay and Parlay X as part of the OSE Error! Reference source not found.. This enabler provides further background and analysis on Parlay architecture and principles.
5. PSA release description

Following the affiliation of the Parlay Group into OMA, and the subsequent agreement between OMA and 3GPP that the OSA and Parlay X activities undertaken in 3GPP SA1 and CT5 being transferred to OMA, OMA is solely responsible for all technical activities related to the onward development and maintenance of OSA/Parlay APIs and Parlay X Web Services.

3GPP has frozen a 3GPP Release 8 Stage 1 requirements document for OSA/Parlay APIs and Parlay X Web Services ([3GPP TS 22.127]), that adds some new requirements with respect to 3GPP Release 7. For some of those requirements all technical work has been completed by 3GPP (including stage 2/3), for some others no technical work has been started in 3GPP.

This OMA PSA RD addresses (per OMA processes) requirements in [3GPP TS 22.127] for which no technical work has been done in 3GPP and responsibility has been moved to OMA ARC WG. For this reason, no new requirements with respect to those frozen 3GPP Release 8 Stage 1 ones will be considered as part of this enabler.

The requirements addressed in this document cover the following topics:

- Ensure Parlay-X composable with identity management frameworks, in particular Liberty Alliance ([3GPP TS 22.127] Clause 13.1.7: To ensure interworking with identity management frameworks within the wider web services industry)
- Privacy on Subscriber Identity (Liberty Alliance, OASIS) ([3GPP TS 22.127] Clause 10.2: Ensure API alignment with OASIS and Liberty Alliance on user identity privacy and federation)
- Topology Hiding ([3GPP TS 22.127] Clause 10.3: To ensure use of the APIs is abstracted from network topology, providing support for load distribution policies)
- Subscriber event notification ([3GPP TS 22.127] Clause 12.1: Generalise call event handling capabilities)
- Event notification ([3GPP TS 22.127] Clause 12.3: Add support for handling chargeable events)
- Access policy ([3GPP TS 22.127] Clause 13.1.1.3: Add support for managing access and usage of service capabilities)
- API usage accounting ([3GPP TS 22.127] Clause 13.1.6: Add support for supply and correlation on usage of the APIs)
- Service identification ([3GPP TS 22.127] Clause 13.2.7: Add support for indication of network and service type for use by applications)

5.1 Version 1.0

PSA version 1.0 completes the work on the 3GPP Release 8 requirements that have been transferred to OMA.
6. Requirements *(Normative)*

6.1 Modularisation

This section depicts the PSA release as a collection of different functional modules where each one is associated to a (group of) requirement(s) identified as related with the offering/delivering of a functionality. This is NOT an architectural model.

The modules identified are:

- **Support for Identity Management Framework and Privacy**: Liberty Alliance ([Liberty Alliance](http://www.libertyalliance.org)) and OASIS ([OASIS](http://www.oasis-open.org), [SAML](http://www.oasis-open.org/osi/saml)) specifications on Identity Management and Identity Federation are well accepted on the market, so they shall be taken into account to address issues related to subscriber identity;

- **Topology hiding**: When exposing network functionalities to third party applications there is the need to:
  - hide the network topology of the underlying network system;
  - set policies to enable the operator to choose the more appropriate underlying network node.

For this reason, requirements for topology hiding and service request distribution based on policies are to be taken into account.

- **Event Notification**: The Event Notification Function provides the mechanisms which enable an application to request to be notified of subscriber or network related event(s); additional events (e.g. chargeable and generalized call state) shall be taken into account;

- **Policy for service capability features access and usage**: to provide functions to manage and enforce policies on the access and usage of service capability features requested by the OSA Applications, so specific requirements are needed;

- **APIs Usage Accounting**: There might be the need for functions to supply and correlate information for accounting of the usage of APIs, so specific requirements are needed;

- **Service Request Capabilities**: Parlay APIs are intended to be used on many different underlaying network technologies, e.g. CS, PS and IMS networks, so the integration of services running on CS, Internet and IMS technologies necessitates the high-level identification of different services being utilized by 3rd party developers via these APIs; for this reason, specific requirements for support of service identification in Parlay is needed.

6.2 High-Level Functional Requirements

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
<th>Release</th>
<th>Functional module</th>
</tr>
</thead>
<tbody>
<tr>
<td>PSA-HLF-001</td>
<td>The Parlay OSA framework SHALL provide support for Identity Management. This SHALL take into account frameworks such as Liberty Alliance identity management framework. <strong>Informational Note</strong>: Endorsed from [3GPP TS 22.127] Clause 13.1.7 (§13 “Functions offered by OSA” -&gt; §13.1 “The Framework functions” -&gt; §13.1.7 “Support for Identity Management Framework”), to ensure interworking with identity management frameworks within the wider web services industry</td>
<td>PSA 1.0</td>
<td>Support for Identity Management Framework and Privacy</td>
</tr>
</tbody>
</table>
| PSA-HLF-002 | 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):  
**Informational Note:** Endorsed from [3GPP TS 22.127] Clause 12 (§12 “Event Notification Function”);  
1) A call processing event occurs: when a call to or from a given user changes state and this event is armed by an application, that application SHALL be notified.  
**Informational Note:** Endorsed from [3GPP TS 22.127] Clause 12.1 (§12 “Event Notification Function”, §12.1 “Subscriber Related events”), to generalise call event handling capabilities.  
2) A chargeable event happens: when a chargeable event occurs, which will be charged to the application provider and this event is armed by an application, that application SHALL be notified.  
**Informational Note:** Endorsed from [3GPP TS 22.127] Clause 12.3 (§12 “Event Notification Function”, §12.3 “Other Related Events”), to add support for handling chargeable events. | PSA 1.0 | Event Notification |
| PSA-HLF-003 | The framework SHALL provide functions to manage and enforce policies on the access and usage of service capability features requested by the OSA Applications, in addition to the policies implemented by the Service Capability Features themselves (e.g. through policy-enabled Service Capability Features).  
**Informational Note:** Endorsed from [3GPP TS 22.127] Clause 13.1.1.3 (§13 “Functions offered by OSA”, §13.1 “The Framework functions”, §13.1.1 “Trust and Security Management”, §13.1.1.3 “Policy for service capability features access and usage”), to add support for managing access and usage of service capabilities. Examples of such policies are: number of application requests for a specified period, frequency of application requests, check on syntax correctness and validity in term of lifetime for parameters, check if the requestor (OSA Application and/or subscriber) is in arrears. | PSA 1.0 | Policy for service capability features access and usage |
| PSA-HLF-004 | The framework SHALL provide functions to supply information for accounting of the usage of APIs.  
**Informational Note:** Endorsed from [3GPP TS 22.127] Clause 13.1.6 (§13 “Functions offered by OSA”, §13.1 “The Framework functions”, §13.1.6 “APIs Usage Accounting”), to add support for supply and correlation on usage of the APIs. | PSA 1.0 | APIs Usage Accounting |
| PSA-HLF-005 | The application SHALL have the ability to request a particular type of service, for example CS-video, or IP-voice, or Communication Service. If an application requests a particular type of service, the underlying network has the right to reject such a request and instead offer a default service.  
**Informational Note:** Endorsed from [3GPP TS 22.127] Clause 13.2.7 (§13 “Functions offered by OSA”, §13.2 “Network functions”, §13.2.7 “Service Request Capabilities”), to add support for indication of network and service type for use by applications. | PSA 1.0 | Service Request Capabilities |
| PSA-HLF-006 | The application SHALL have to ability to receive notifications and events related to the service running in the underlying network.  
**Informational Note:** Endorsed from [3GPP TS 22.127] Clause 13.2.7 (§13 “Functions offered by OSA”, §13.2 “Network functions”, §13.2.7 “Service Request Capabilities”), to add support for indication of network and service type for use by applications. | PSA 1.0 | Service Request Capabilities |
Table 1: High-Level Functional Requirements

6.2.1 Privacy

This section identifies the high-level privacy needs for the PSA enabler.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
<th>Release</th>
<th>Functional module</th>
</tr>
</thead>
<tbody>
<tr>
<td>PSA-PRV-001</td>
<td>It SHALL be possible to hide subscriber’s identity towards the OSA Applications and replace it with an alias. Liberty Alliance and OASIS specifications on Identity Management and Identity Federation (e.g. SAML 2.0) needs to be taken into account to address issues related to subscriber identity. Informational Note: Endorsed from [3GPP TS 22.127] Clause 10.2 (§10 “Security and Privacy requirements”, §10.2 “Privacy requirements on Subscriber Identity”), to ensure API alignment with OASIS and Liberty Alliance on user identity privacy and federation.</td>
<td>PSA 1.0</td>
<td>Support for Identity Management Framework and Privacy</td>
</tr>
</tbody>
</table>

Table 2: High-Level Functional Requirements – Privacy Items

6.3 Overall System Requirements

This section identifies the overall system needs for the PSA enabler.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
<th>Release</th>
<th>Functional module</th>
</tr>
</thead>
<tbody>
<tr>
<td>PSA-SYS-001</td>
<td>OSA SHALL enable an operator to set policies (e.g. based on the need of load distribution) on how OSA shall utilize the underlying network system. Informational Note: Endorsed from [3GPP TS 22.127] Clause 6 (§6 “High level requirements to OSA”), to ensure use of the APIs is abstracted from network topology, providing support for load distribution policies.</td>
<td>PSA 1.0</td>
<td>Topology hiding</td>
</tr>
<tr>
<td>PSA-SYS-002</td>
<td>It SHALL be possible to hide the topology of the underlying network systems. Informational Note: Endorsed from [3GPP TS 22.127] Clause 10.3 (§10 “Security and Privacy requirements”, §10.3 “Topology hiding”), to ensure use of the APIs is abstracted from network topology, providing support for load distribution policies.</td>
<td>PSA 1.0</td>
<td>Topology hiding</td>
</tr>
<tr>
<td>PSA-SYS-003</td>
<td>It SHALL be possible to provide a single point of access to the Applications Informational Note: Endorsed from [3GPP TS 22.127] Clause 10.3 (§10 “Security and Privacy requirements”, §10.3 “Topology hiding”), to ensure use of the APIs is abstracted from network topology, providing support for load distribution policies.</td>
<td>PSA 1.0</td>
<td>Topology hiding</td>
</tr>
</tbody>
</table>

Table 3: High-Level System Requirements
Appendix A. Change History (Informative)

A.1 Approved Version History

<table>
<thead>
<tr>
<th>Reference</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OMA-RD-Parlay_Service_Access-V1_0</td>
<td>27 Apr 2010</td>
<td>Approved by TP: OMA-TP-2010-0132R02-INP_PSA_V1_0_RRP_for_Final_Approval</td>
</tr>
</tbody>
</table>
Appendix B. Use Cases

This appendix provides high-level use cases for the PSA enabler.

B.1 Travel support and information service

This use case is adopted from 3GPP TS 22.127 v8.1.0, appendix A.1 [3GPP TS 22.127].

B.1.1 Short 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.

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.

B.1.2 Market benefits

The service provider is able to offer context-aware applications to end-users. Application developers can dispose of programmatic interfaces to access service provider enablers.

B.2 Third Party Call Web Service

This use case is adopted from [3GPP TS 29.199-02], section 4.
B.2.1 Short Description

Figure 1 shows a scenario using the Third Party Call Web Service to handle third party call functions. The application invokes a Web Service to retrieve stock quotes and a Parlay X Interface to initiate a third party call between a broker and his client.

In the scenario, whenever a particular stock quote reaches a threshold value (1) and (2), the client application invokes a third party call between one or more brokers and their corresponding customers to decide actions to be taken. After invocation (3) by the application, the Third Party Call Web Service invokes a Parlay API operation (4) using the Parlay/OSA SCS-CC (Call control) interface. This SCS handles the invocation and sends a message (5) to an MSC to set-up a call between user A and user B.

In an alternative scenario, the Parlay API interaction involving steps (4) and (5) could be replaced with a direct interaction between the Third Party Call Web Service and the Mobile network.

![Figure 3: Third party call scenario](image)

B.2.2 Market benefits

Application developers no longer need to learn and use specific protocols to access Call Control functions provided by network elements (specifically operations to initiate a call from applications), which requires a high degree of network expertise. Invoking standard abstract programmatic interfaces to gain access to call control capabilities obviates the need for advanced telecommunication skills.