# OMA Global Service Architecture Overview

Approved Version 1.1 – 01 Mar 2011

**Open Mobile Alliance**

OMA-OD-Global_Service_Architecture–V1_1-20110301-A

# Contents

# Figures

# Tables

# 1. Scope

This document describes the OMA Global Service Architecture (OGSA) that is a service architectural view of OMA Enablers leveraging OSE (OMA Service Environment). The main scope of OGSA is to support new (and/or revised) Enabler specifications clarifying how they fit with the OSE. For this reason, when creating a new (or revised) Enabler, OGSA will:

- identify the dependencies between the being-defined (or revised) Enabler and other OMA Enablers
- compile which interfaces the being-defined (or revised) Enabler exposes;

How the relevant OMA WG will specify the being-defined (or revised) Enabler is out of scope of the OGSA work.

Influencing other SDOs is out of scope of the OGSA work: in case overlaps with other SDOs specifications should come out, these will be managed as in OMA process.

Material for a specific enabler will only be included in this document for enablers where the Architecture Document has reached Candidate or Approved status.

# 2. References

## 2.1 Normative References


**[OSE]** "OMA Service Environment", Open Mobile Alliance™, URL:http://www.openmobilealliance.org/

**[RFC2119]** "Key words for use in RFCs to Indicate Requirement Levels", S. Bradner, March 1997, URL:http://www.ietf.org/rfc/rfc2119.txt



**[RFC2119]** "Key words for use in RFCs to Indicate Requirement Levels", S. Bradner, March 1997, URL:http://www.ietf.org/rfc/rfc2119.txt


## 2.2 Informative References


**[OMA-AC_MO_WP]** "White Paper on Provisioning Objects", Open Mobile Alliance™, OMA-WP-AC_MO, URL: http://www.openmobilealliance.org/

**[OMA-BCAST_AD]** "Mobile Broadcast Services Architecture", Open Mobile Alliance™, OMA-AD-BCAST-V1_0, URL: http://www.openmobilealliance.org/

**[OMA-BPS_ERP]** "Browser Protocol Stack", Open Mobile Alliance™, OMA-Browser_Protocol_Stack-V2_1, URL: http://www.openmobilealliance.org/

**[OMA-CAB-AD]** "Converged Address Book Architecture", Open Mobile Alliance™, OMA-AD-CAB-V1_0, URL: http://www.openmobilealliance.org/

**[OMA-CBCS-AD]** "Categorization Based Content Screening Architecture", Open Mobile Alliance™, OMA-AD-CBCS_V1_0, URL: http://www.openmobilealliance.org/

**[OMA-CBUS_AD]** "Condition Based URIs Selection Architecture",Open Mobile Alliance™, OMA-AD-CBUS-V1_0, URL: http://www.openmobilealliance.org/

**[OMA-CHRG_AD]** "Charging Architecture" Open Mobile Alliance™, OMA-AD-Charging-V1_1, URL: http://www.openmobilealliance.org/

**[OMA-CHRG_Data]** "Charging Data", Open Mobile Alliance™, OMA-DDS-Charging_Data-V1_0, URL: http://www.openmobilealliance.org/

**[OMA-CHWS]** "White Paper on Charging Work Split", Open Mobile Alliance™, OMA-WP-Charging-Worksplit-V1_0-20050315-A, URL: http://www.openmobilealliance.org/

**[OMA-CMI_AD]** "Content Management Interface",Open Mobile Alliance™, OMA-RD-CMI-V1_0, URL: http://www.openmobilealliance.org/

**[OMA-CMR_AD]** "Customized Multimedia Ringing Architecture", Open Mobile Alliance™, OMA-AD-CMR-V1_0, URL: http://www.openmobilealliance.org/

**[OMA-ConnMO_AD]** "Connectivity Management Objects Architecture", Open Mobile Alliance™, OMA-AD-ConnMO-V1_0, URL: http://www.openmobilealliance.org/

**[OMA-CP_AD]** "Provisioning Architecture Overview", Open Mobile Alliance™, OMA-TS-WAP_ProvArch-V1_1, URL: http://www.openmobilealliance.org/

**[OMA-CPM-AD]** "Converged IP Messaging Architecture", Open Mobile Alliance™, OMA-AD-CPM-V1_0, URL: http://www.openmobilealliance.org/

**[OMA-CSCSF_AD]** "Client Side Content Screening Framework", Open Mobile Alliance™, OMA-AD-Client_Side_CS_FW-V1_0, URL: http://www.openmobilealliance.org/

**[OMA-DCD-AD]** "Dynamic Content Delivery Architecture", Open Mobile Alliance™, OMA-AD-DCD-V1_0, URL: http://www.openmobilealliance.org/

**[OMA-DCMO_AD]** "DCMO Architecture", Open Mobile Alliance™, OMA-AD-DCMO-V1_0, URL: http://www.openmobilealliance.org/

**[OMA-DMSC-AD]** "DM Smart Card Architecture", Open Mobile Alliance™, OMA-AD-DM_SC-V1_0, URL: http://www.openmobilealliance.org/

**[OMA-DiagMon_AD]** "DM DiagMon Architecture", Open Mobile Alliance™, OMA-AD-DiagMon-V1_0, URL: http://www.openmobilealliance.org/

**[OMA-DLOTA-AD]** "Download Over the Air Architecture", Open Mobile Alliance™, OMA-AD-DLOTA-V2_0, URL: http://www.openmobilealliance.org/

**[OMA-DM_AD]** "Device Management Architecture", Open Mobile Alliance™, OMA-AD-DM-V1_3, URL: http://www.openmobilealliance.org/

**[OMA-DMSched-AD]** "DM Scheduling Architecture", Open Mobile Alliance™, OMA-AD-DM_Scheduling-V1_0, URL: http://www.openmobilealliance.org/

**[OMA-DPE_AD]** "Device Profiles Evolution Architecture", Open Mobile Alliance™, OMA-AD-DPE-V1_0, URL: http://www.openmobilealliance.org/

**[OMA-DO_WP]** "OMA Data Objects Whitepaper", Open Mobile Alliance™, OMA-WP-Data_Object-20080916-A, URL: http://www.openmobilealliance.org/

**[OMA-DRM_AD]** "DRM Architecture", Open Mobile Alliance™, OMA-AD-DRM-V2_1, URL: http://www.openmobilealliance.org/

**[OMA-DS-AD]** "DS (Data Synchronization) 2.0 Architecture",Open Mobile Alliance™, OMA-AD-DS-V2_0, URL: http://www.openmobilealliance.org/

**[OMA-EMN_ERP]** "E-Mail Notification", Open Mobile Alliance™, OMA-ERP-EMN-V1_0, URL: http://www.openmobilealliance.org/

**[OMA-EFI_ERP]** "External Functionality Interface", Open Mobile Alliance™, OMA-EFI-V1_1, URL: http://www.openmobilealliance.org/

**[OMA-FUMO_AD]** "Firmware Update Management Object Architecture", Open Mobile Alliance™, OMA-AD-FUMO-V1_0, URL: http://www.openmobilealliance.org/

**[OMA-GPM-AD]** "Global Permissions Management Architecture", Open Mobile Alliance™, OMA-AD-GPM-V1_0, URL: http://www.openmobilealliance.org/

**[OMA-GS_AD]** "Game Services Architecture", Open Mobile Alliance™, OMA-AD-Game-Services-Architecture-V1_0, URL: http://www.openmobilealliance.org/

**[OMA-GSSM-AD]** "General Service Subscription Management Architecture", Open Mobile Alliance™, OMA-AD-GSSM-V1_0, URL: http://www.openmobilealliance.org/

**[OMA-IdM_RD]** "Identity Management Framework Requirements", Open Mobile Alliance™, OMA-RD-Identity-Management-Framework-V1_0, URL: http://www.openmobilealliance.org/

**[OMA-IGA_AD]** "In-Game Advertising Architecture", Open Mobile Alliance™, OMA-AD-IGA-V1_0, URL: http://www.openmobilealliance.org/

**[OMA-IMSinOMA-AD]** "Utilization of IMS capabilities Architecture", Open Mobile Alliance™, OMA-AD-IMS-V1_0, URL: http://www.openmobilealliance.org/

**[OMA-IMPS-AD]** "IMPS (Instant Messaging and Presence Services) Architecture", Open Mobile Alliance™, OMA-AD-IMPS-V1_3, URL: http://www.openmobilealliance.org/

**[OMA-IMPS_WP]** "White Paper on Implementation Guidelines for IMPS 1.3", Open Mobile Alliance™, OMA-WP-IMPS_V1_3_IMPL-20090505-C, URL: http://www.openmobilealliance.org/

**[OMA-IGC_RD]** "In-Game Communications", Open Mobile Alliance™, OMA-RD-In-Game-Communications-V1_0, URL: http://www.openmobilealliance.org/

**[OMA-LAWMO-AD]** "LAWMO (Lock And Wipe Management Object) Architecture", Open Mobile Alliance™, OMA-AD-LAWMO-V1_0, URL: http://www.openmobilealliance.org/

**[OMA-LFC-AD]** "Look and Feel Customization Architecture", Open Mobile Alliance™, OMA-AD-LFC-V1_0, URL: http://www.openmobilealliance.org/

**[OMA-LOC_RD]** "Location Enabler Release Requirements", Open Mobile Alliance™, OMA-RD-LER-V1_0, URL: http://www.openmobilealliance.org/

**[OMA-LOCSIP-AD]** "Location in SIP/IP core Architecture", Open Mobile Alliance™, OMA-AD-LOCSIP-V1_0, URL: http://www.openmobilealliance.org/

**[OMA-MC_AD]** "Mobile Codes Architecture", Open Mobile Alliance™, OMA-AD-MC-V1_0, URL:

http://www.openmobilealliance.org/

**[OMA-MEM_AD]** "Mobile Email Architecture", Open Mobile Alliance™, OMA-AD-Mobile_Email-V1_0, URL: http://www.openmobilealliance.org/

**[OMA-MGE_WP]** "Mobile Gaming Evolution White Paper", Open Mobile Alliance™, OMA-WP-MGPC-20080610-A, URL: http://www.openmobilealliance.org/

**[OMA-MLP-TS]** "Mobile Location Protocol 3.3", Open Mobile Alliance™, OMA-TS-MLP-V3_3, URL: http://www.openmobilealliance.org/

**[OMA-MLS-AD]** "Mobile Location Service Architecture", Open Mobile Alliance™, OMA-AD-MLS-V1_2, URL: http://www.openmobilealliance.org/

**[OMA-MMMD_AD]** "OMA Multimodal and Multi-device Enabler Architecture", Open Mobile Alliance™, OMA-AD-MMMD-V1_0, URL: http://www.openmobilealliance.org/

**[OMA-MMS_AD]** "MMS Architecture", Open Mobile Alliance™, OMA-AD-MMS-V1_3, URL: http://www.openmobilealliance.org/

**[OMA-MobAd_AD]** "Mobile Advertising Architecture", Open Mobile Alliance™, OMA-AD-Mobile_Advertising-V1_0, URL: http://www.openmobilealliance.org/

**[OMA-MSI_WP]** "White Paper on Interworking of Messaging Architecture", Open Mobile Alliance™, OMA-WP-MsgSvc_Intw_Arch-20070501-A, URL: http://www.openmobilealliance.org/

**[OMA-NGSI-AD]** "Next Generation Service Interfaces Architecture", Open Mobile Alliance™, OMA-AD-NGSI-V1_0, URL: http://www.openmobilealliance.org/

**[OMA-OBKG-ERP]** "On-board Key Generation and Key Enrollment[1]", Open Mobile Alliance™, OMA-ERP-OBKG-V1_0, URL: http://www.openmobilealliance.org/

**[OMA-OCSPMP-ERP]** "Online Certificate Status Protocol Mobile Profile[2]", Open Mobile Alliance™, OMA-ERP-OCSP_MP-V1_0, URL: http://www.openmobilealliance.org/

**[OMA-OSE]** "OMA Service Environment", Open Mobile Alliance™, URL: http://www.openmobilealliance.org/

**[OMA-OCSP_MP-ERP]** "Online Certificate Status Protocol Mobile Profile[3]", Open Mobile Alliance™, OMA-ERP-OCSP_MP-V1_0, URL: http://www.openmobilealliance.org/

**[OMA-OSPE_AD]** "Open Service Provider Environment", Open Mobile Alliance™, OMA-AD-OSPE-V1_0, URL: http://www.openmobilealliance.org/

**[OMA-OWSER_AD]** "OMA Web Services Enabler (OWSER): Overview", Open Mobile Alliance™, OMA-AD-OWSER_Overview-V1_1, URL: http://www.openmobilealliance.org/

**[OMA-OWSER_NI_AD]** "OMA Web Services Network Identity Architecture", Open Mobile Alliance™, OMA-AD-OWSER_NI-V1_0, URL: http://www.openmobilealliance.org/

**[OMA-PAL_AD]** "Presence Access Layer (PAL) - Architecture", Open Mobile Alliance™, OMA-AD-PAL-V1_0, URL: http://www.openmobilealliance.org/

**[OMA-PEEM_AD]** "Policy Evaluation, Enforcement and Management Architecture", Open Mobile Alliance™, OMA-AD-Policy_Evaluation_Enforcement_Management-V1_0, URL: http://www.openmobilealliance.org/

**[OMA-PSA_AD]** "Parlay Service Access", Open Mobile Alliance™, OMA-AD-Parlay_Service_Access-V1_0, URL: http://www.openmobilealliance.org/

**[OMA-PIOSE_AD]** "Parlay in OSE Architecture", Open Mobile Alliance™, OMA-AD-PIOSE-V1_0, URL: http://www.openmobilealliance.org/

**[OMA-POC_AD]** "Push to talk Over Cellular (PoC) - Architecture", Open Mobile Alliance™, OMA-AD-PoC-V2_0, URL: http://www.openmobilealliance.org/

**[OMA-Presence-AD]** "Presence SIMPLE Architecture", Open Mobile Alliance™, OMA-AD-Presence_SIMPLE-V2_0, URL:

[1] This enabler does not contain a specific AD.

[2] This enabler does not contain a specific AD.

[3] This enabler does not contain a specific AD.

http://www.openmobilealliance.org/

**[OMA-PRIV_RD]** "Privacy Requirements for Mobile Services", Open Mobile Alliance™, OMA-RD-Privacy-V1_0_1, URL: http://www.openmobilealliance.org/

**[OMA-PUSH-AD]** "Push Architecture", Open Mobile Alliance™, OMA-AD-Push-V2_2, URL: http://www.openmobilealliance.org/

**[OMA-PUSH-AD_next]** "Push Architecture", Open Mobile Alliance™, OMA-AD-Push-V2_3, URL: http://www.openmobilealliance.org/

**[OMA-REST_ERP]** "RESTful bindings for Parlay X Web Services", Open Mobile Alliance™, OMA-ERP-ParlayREST-V1_0, URL: http://www.openmobilealliance.org/

**[OMA-RME_AD]** "Rich Media Environment Architecture", Open Mobile Alliance™, OMA-AD-RME-V1_0, URL: http://www.openmobilealliance.org/

**[OMA-SCE_AD]** "Secure Content Exchange Architecture", Open Mobile Alliance™, OMA-AD-SCE-V1_0, URL: http://www.openmobilealliance.org/

**[OMA-SEC_CF_AD]** "Security Common Functions Architecture", Open Mobile Alliance™, OMA-AD-SEC_CF-V1_0, URL: http://www.openmobilealliance.org/

**[OMA-SCIM-AD]** "Secure Content Identification Mechanism Architecture", Open Mobile Alliance™, OMA-AD-SCIDM-V1_0, URL: http://www.openmobilealliance.org/

**[OMA-SCOMO-AD]** "SCOMO (Software Component Management Object) Architecture", Open Mobile Alliance™, OMA-AD-SCOMO-V1_0, URL: http://www.openmobilealliance.org/

**[OMA-SIP-PUSH-AD]** "Push using SIP Architecture", Open Mobile Alliance™, OMA-AD-SIP_Push-V1_0, URL: http://www.openmobilealliance.org/

**[OMA-SUPL-AD]** "Secure User Plane Location Architecture", Open Mobile Alliance™, OMA-AD-SUPL-V3_0, URL: http://www.openmobilealliance.org/

**[OMA-SVG-TS]** "Scalable Vector Graphics (SVG) for the Mobile Domain"[4], Open Mobile Alliance™, OMA-TS-SVG_Mobile-V1_0, URL: http://www.openmobilealliance.org/

**[OMA-SCWS_AD]** "Smartcard Web Server Enabler Architecture", Open Mobile Alliance™, OMA-AD-Smartcard_Web_Server-V1_0, URL: http://www.openmobilealliance.org/

**[OMA-SIMPLE-IM]** "Instant Messaging", Open Mobile Alliance™, OMA-ERELD-SIMPLE_IM-V1_0, URL: http://www.openmobilealliance.org/

**[OMA-SMIL_RD]** "Mobile Domain SMIL Requirements", Open Mobile Alliance™, OMA-RD-MobileDomainSMIL-V1_0, URL: http://www.openmobilealliance.org/

**[OMA-SRM_AD]** "OMA Secure Removable Media Architecture", Open Mobile Alliance™, OMA-AD-SRM-V1_0, URL: http://www.openmobilealliance.org/

**[OMA-SRM_AD_next]** "OMA Secure Removable Media Architecture", Open Mobile Alliance™, OMA-AD-SRM-V1_1, URL: http://www.openmobilealliance.org/

**[OMA-STI-AD]** "Architecture of the Environment using the Standard Transcoding Interface", Open Mobile Alliance™, OMA-AD-STI-V1_0, URL: http://www.openmobilealliance.org/

**[OMA-UAPROF-ERP]** "User Agent Profile"[5], Open Mobile Alliance™, OMA-ERP-UAProf-V2_0_1, URL: http://www.openmobilealliance.org/

**[OMA-URI-Schemes-ERP]** "URI Schemes for the Mobile Applications Environment[6]", Open Mobile Alliance™, OMA-ERP-URI_Schemes-V1_0, URL: http://www.openmobilealliance.org/

**[OMA-vObject-ERP]** "vObject Minimum Interoperability Profile", Open Mobile Alliance™, OMA-ERP-vObject-V1_0, URL: http://www.openmobilealliance.org/

[4] This enabler does not contain a specific AD.

[5] This enabler does not contain a specific AD.

[6] This enabler does not contain a specific AD.

**[OMA-WAP_AD]** "Wireless Application Protocol Architecture Specification", Open Mobile Alliance™, OMA-AD-WAP_210_WAPArch-V1_0, URL: http://www.openmobilealliance.org/

**[OMA-WAP-BF]** "WAP Billing Framework Version 1.0", Open Mobile Alliance™, OMA-WBF-v1_0, URL: http://www.openmobilealliance.org/

**[OMA-WPBR_RD]** "WAP Proxy-Based Redirect", Open Mobile Alliance™, OMA-RD_WAPproxyBasedRedirect-V1_0, URL: http://www.openmobilealliance.org/

**[OMA-WPDNS-ERP]** "Wireless Profiled DNS (Domain Name System)[7]", Open Mobile Alliance™, OMA-ERP-DNS-V1_0, URL: http://www.openmobilealliance.org/

**[OMA-WPKI_ERP]** "Wireless Public Key Infrastructure", Open Mobile Alliance™, OMA-WPKI-V1_0, URL: http://www.openmobilealliance.org/

**[OMA-XDM_AD]** "XML Document Management Architecture", Open Mobile Alliance™, OMA-AD-XDM-V2_0, URL: http://www.openmobilealliance.org/

**[OMA-XDM_AD_next]** "XML Document Management Architecture", Open Mobile Alliance™, OMA-AD-XDM-V2_1, URL: http://www.openmobilealliance.org/

**[RFC3261]** "SIP: Session Initiation Protocol", J. Rosenberg et al, June 2002, URL:http://www.ietf.org/rfc/rfc3261.txt


[7] This enabler does not contain a specific AD.

# 3. Terminology and Conventions (Normative)

## 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 are informative, unless they are explicitly indicated to be normative.

## 3.2 Definitions

| | |
|---|---|
| **OGSA Suite** | An arbitrary grouping of enablers as a cataloguing or representational convention. |
| **OGSA View** | A representation of the interfaces specified and exposed by a specific Enabler and/or its components. |
| **Service architectural view** | A term representing the combined architecture for the portfolio of offerings made available by a service provider accessible over. |

## 3.3 Abbreviations

| | |
|---|---|
| **3GPP** | 3rd Generation Partnership Project |
| **ACMO** | Application Characteristics/Management Object |
| **AD** | Architecture Document |
| **ADRR** | Architecture Document Review Report |
| **API** | Application Programming Interface |
| **ASP** | Applications Service Provider |
| **BCAST** | Mobile Broadcast Services |
| **BSS** | Business Support System |
| **CAB** | Converged Address Book |
| **CBCS** | Categorization Based Content Screening |
| **CBUS** | Condition Based URIs Selection |
| **CHRG** | Charging |
| **CMI** | Content Management Interface |
| **CMR** | Customised Multimedia Ringing |
| **ConnMO** | Connectivity Management Object |
| **CP** | Client Provisioning |
| **CPM** | Converged IP Messaging |
| **CR** | Change Request |
| **CSCSF** | Client Side Content Screening Framework |
| **DCD** | Dynamic Content Delivery |
| **DCMO** | Device Capability Management Object |
| **DiagMon** | Diagnostics and Monitoring |
| **DLOTA** | Download Over The Air |
| **DM** | Device Management |
| **DNS** | Domain Name System |
| **DPE** | Device Profiles Evolution |
| **DRM** | Digital Rights Management |

| | |
|---|---|
| **DS** | Data Synchronization |
| **EFI** | External Functionality Interface |
| **EMN** | E-Mail Notification |
| **FUMO** | Firmware Update/Management Object |
| **GPM** | Global Permissions Management |
| **GS-CSI** | Games Services Client Server Interface |
| **GSSM** | General Service Subscription Management |
| **HTTP** | Hypertext Transfer Protocol |
| **IETF** | Internet Engineering Taskforce |
| **IM** | Instant Messaging |
| **IMF** | Identity Management Framework |
| **IMPS** | Instant Messaging Presence Service |
| **IMS** | IP Multimedia Subsystem |
| **IMSinOMA** | Utilization of IMS Capabilities in OMA |
| **IP** | Internet Protocol |
| **LAWMO** | Lock And Wipe Management Object |
| **LFC** | Look and Feel Customization |
| **LOCSIP** | Location in SIP/IP Core |
| **MEM** | Mobile E-Mail |
| **MLP** | Mobile Location Protocol |
| **MLS** | Mobile Location Services |
| **MMMD** | Multi-modal Multi-device |
| **MMS** | Multimedia Messaging Service |
| **MobAd** | Mobile Advertising |
| **MSRP** | Message Session Relay Protocol |
| **NI** | Network Identity |
| **NGSI** | Next Generation Service Interfaces |
| **OASIS** | Organization for the Advancement of Structured Information Standards |
| **OBKG** | On-Board Key Generation |
| **OCM** | OGSA Change Management |
| **OCSP** | Online Certificate Status Protocol Mobile Profile |
| **OGSA** | OMA Global Service Architecture |
| **OMA** | Open Mobile Alliance |
| **OSE** | OMA Service Environment |
| **OSS** | Operations Support System |
| **OWSER** | OMA Mobile Web Services |
| **OWSER-NI** | OWSER Network Identity |
| **PAL** | Presence Access Layer |
| **PEEM** | Policy Evaluation, Enforcement, and Management |
| **PIOSE** | Parlay In OSE |

| | |
|---|---|
| **POC** | Push-to-talk Over Cellular |
| **PSA** | Parlay Service Access |
| **REL** | Release Planning and Management committee |
| **RLS** | Resource List Server |
| **RME** | Rich Media Environment |
| **RTCP** | Real Time Control Protocol |
| **RTP** | Real Time Transport Protocol |
| **SC** | Device Management Smart Card |
| **SCE** | Secure Content Exchange |
| **Sched** | Device Management Scheduling |
| **SCIDM** | Secure Content Identification Mechanism |
| **SCOMO** | Software Component Management Object |
| **SCWS** | Smart Card Web Server |
| **SDO** | Standards Development Organization |
| **SDP** | Session Description Protocol |
| **SEC_CF** | Applicaation Layer Security Common Functions |
| **SIMPLE** | SIP for Instant Messaging and Presence Leveraging Extensions |
| **SIMPLE IM** | SIMPLE - Instant Messaging |
| **SIP** | Session Initiation Protocol |
| **SRM** | Secure Removable Module |
| **STI** | Standard Transcoding Interface |
| **SUPL** | Secure User Plane Location |
| **SVG** | Scalable Vector Graphics |
| **TPP** | Third Party Pays |
| **UAProf** | User Agent Profile |
| **URI** | Uniform Resource Identifier |
| **URI** | OMA URI Schemes |
| **VAS** | Value Added Service |
| **WAP** | Wireless Application Protocol |
| **WG** | Working Group |
| **WID** | Work Item Description |
| **WPKI** | Wireless Public Key Infrastructure |
| **WSBPEL** | Web Services Business Process Execution Language |
| **WSI** | Web Services IF for Device Management |
| **XCAP** | XML Configuration Access Protocol |
| **XDM** | XML Document Management |
| **XDMC** | XML Document Management Client |
| **XDMS** | XML Document Management Server |
| **XML** | Extensible Markup Language |

# 4. Introduction

## 4.1 Objectives

The OGSA defines an overall service architectural view of OMA Enablers leveraging OSE, such that when creating a new or revised Enabler, a WG may identify the context of the Enabler being defined.

The OGSA

- positions the OMA enablers in OGSA Suite(s),
- facilitates the justification for and representation for Enablers (not just individually but in a wider context), and helps operators and external entities understand and leverage OMA Enablers,
- represents a re-usable set of enablers and exposed interfaces,
- illustrates modularity.

## 4.2 Version 1.0

Version 1.0 of OGSA contains an architectural view of the following OMA Enablers:

- Categorization based Content Screening [OMA-CBCS-AD]
- Charging [OMA-CHRG_AD]
- Dynamic Content Delivery [OMA-DCD-AD]
- Policy Evaluation, Enforcement, and Management [OMA-PEEM_AD]
- XML Document Management [OMA-XDM_AD]

# 5. Generic View Diagram

## 5.1 Description

### 5.1.1 OGSA Suites and Enablers

Showing OMA enablers and their dependencies results in a complex and large picture. Figure 1 Figure 1below illustrates how such a picture might look like.

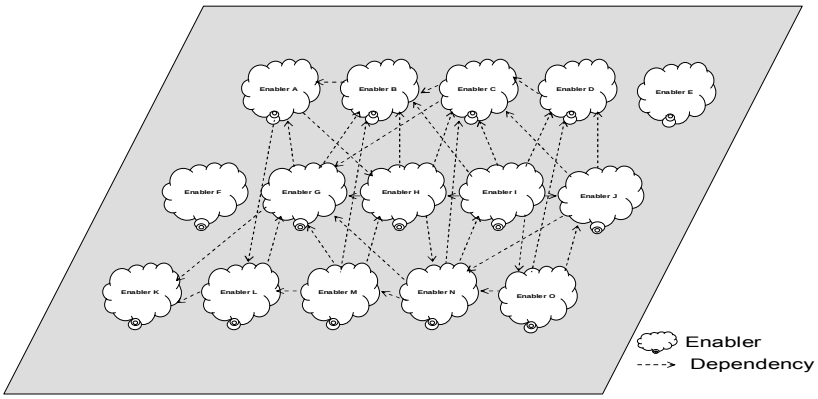



**Figure 1: Representation of the OMA Enablers and their possible dependencies**

The term “suite” is used to represent an arbitrary grouping of enablers as a cataloguing or representational convention.In the Service Architecture View, multiple suites may be identified, and some enablers may be included in more than one suite.

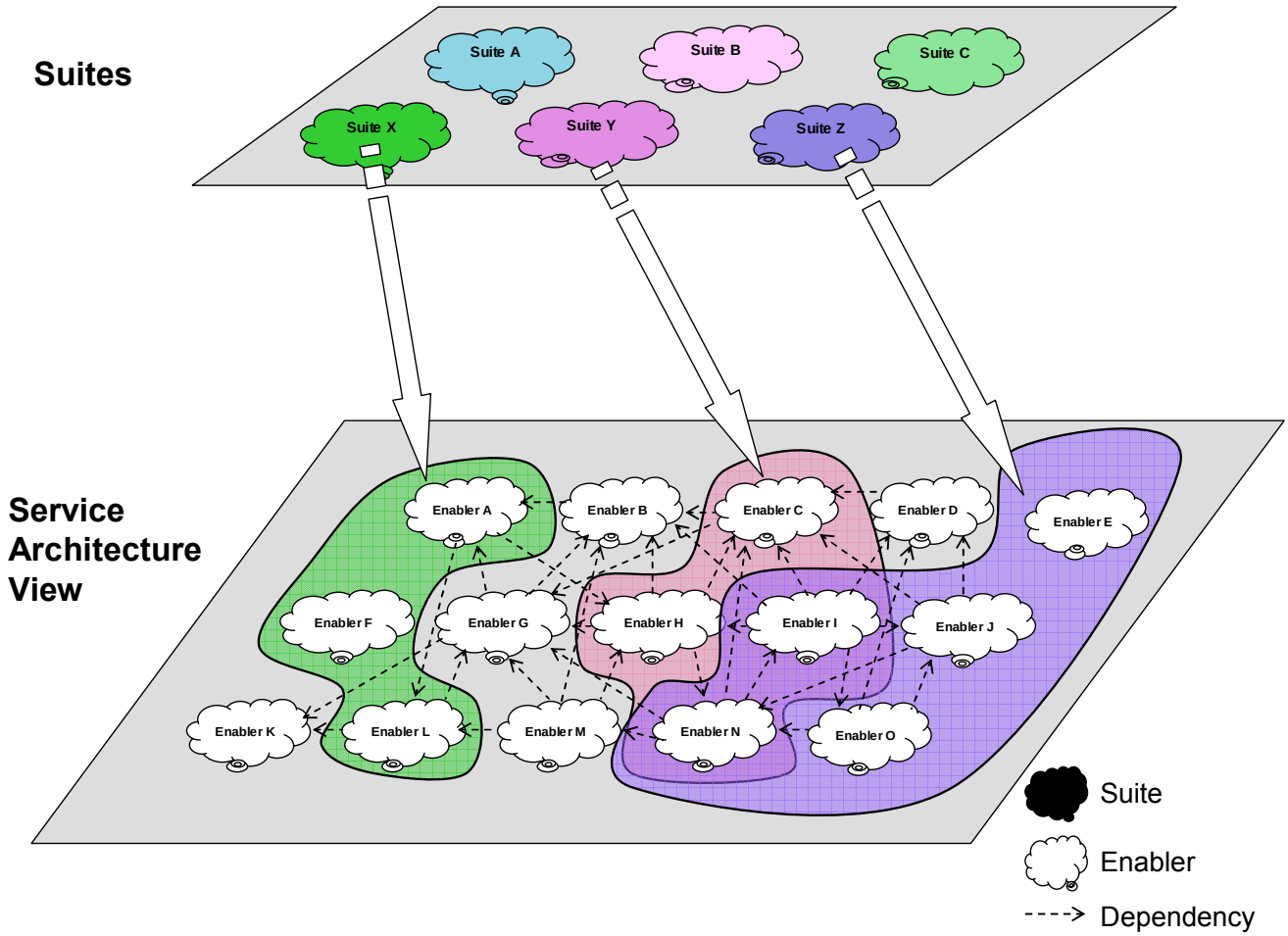



**Figure 2: OGSA Suites mapping to multiple Enablers**

In Figure 2, three OGSA Suites examples are shown:

- Suite X: contains Enablers A, F and L
- Suite Y: contains Enablers C, H, I and N
- Suite Z: contains Enablers E, I, J, N and O

As may be seen from the example, multiple OGSA Suites may be defined. A Enabler may be represented in multiple OGSA Suites, and in the above example, Enablers I and N are used by OGSA Suites Y and Z.

## 5.1.2 Using OGSA Suites

The creation of a Service Architecture View through the suites concept may assist in helping to review and compare the architectures of related enablers when updating existing or creating new enablers.

The following sections provide informative examples of how existing and new enablers may benefit from suites.

## 5.1.3 Existing Enablers

There are existing Enablers in OMA, where the duplication or overlap of functions or components of other enablers has introduced silos into the OMA and complicates implementations and deployments.

To help understand the use of OGSA Suites when evolving existing Enablers, consider (for example), Enabler C (see Figure 2: ) being further developed to add new functionality. When considering the new functionality for Enabler C, firstly the OGSA Suite(s) to which it is associated is reviewed as part of Enabler C's development.

As Enabler C is in OGSA Suite Y, then the functions of the architectures of Enablers H, I and N are required to be considered and taken into account (as well as possibly others). In the event that an Enabler is in multiple OGSA Suites, the functions of the architectures of the Enablers in those OGSA Suites also require to be taken into account. As a consequence of reviewing the related functions of the architectures within OGSA Suite Y, the proposed development of Enabler C may result in Enabler C adopting parts of the functionality of the architectures already defined in Enablers H, I and/or N, or its development being influenced by them. Additionally, enablers in other suites may also be considered as part of this evaluation.

### 5.1.4 New Enablers

New enablers define the architectures needed to support their requirements. Some enablers may not be aware of, or may even not take into account, existing functions or components of existing enablers for the new enabler. This may lead to silos.

The new Enabler will be assigned to an OGSA Suite once the RD is approved as Candidate.The working group can then carefully consider re-using/extending the Enablers in the same OGSA Suite(s), instead of creating new ones. Additionally, enablers in other suites may also be considered as part of this evaluation.

To help understand the use of OGSA Suites when creating new Enablers, consider (for example) Enabler D (see Figure 2: ) being created. When considering the new functionality for Enabler D, the OGSA Suite(s) to which it may be associated are reviewed as part of Enabler D's development.

After initial analysis, let's assume that Enabler D is assigned to OGSA Suite Z, and consequently the functions of the architectures of Enablers E, I, J, N and O are required to be considered and taken into account. As a consequence of reviewing the related functions of the architectures within OGSA Suite Z, the proposed development of Enabler D may result in Enabler D adopting parts of the functions of the architectures/functionality already of the architectures defined in Enablers E, I, J, N and/or O, or its development being influenced by them.

## 5.2 OGSA and OGSA view in OSE

The OGSA suites in the context of the OMA Service Environment (OSE) [OMA-OSE] are depicted inFigure 3.

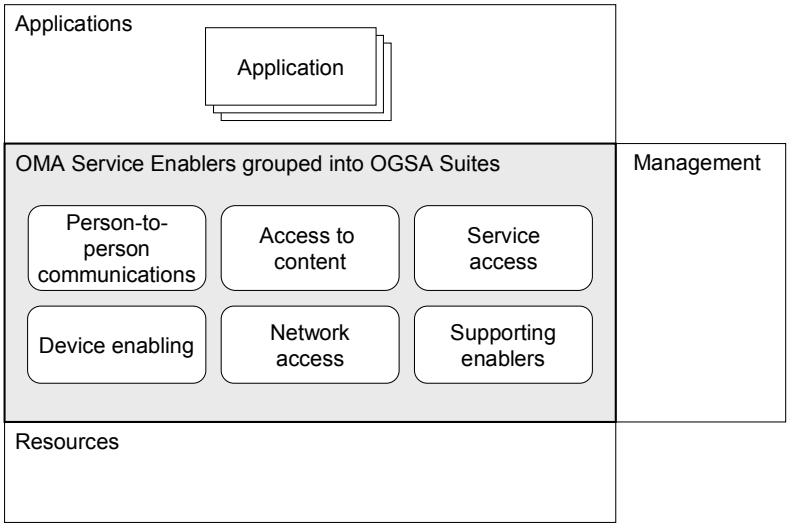



**Figure 3: OGSA Suites in the context of OSE**

The OMA Services Enablers are grouped into OGSA Suites.

Applications are a primary means for initiating and consuming an Enabler. See also [OMA-OSE].

Resources provide capabilities and exposes functionality provided by service providers, operators' networks, terminals, etc that may be used by Enablers developed in OMA. See also [OMA-OSE].

Management includes various business support functions for services like subscriber management, software life cycle management and/or contains backend resources (e.g. BSS or OSS).

## 5.3 Dependencies (Normative)

OGSA is dependent on all Enablers identified in section 4.2.

## 5.4 Modelling the generic view diagram (Normative)

In order to facilitate the reuse a simple intuitive diagram depicting OGSA View is introduced. OGSA View MUST describe and give a graphical overview of the components of the enabler and the I0 interfaces, which expose enabler functionality.

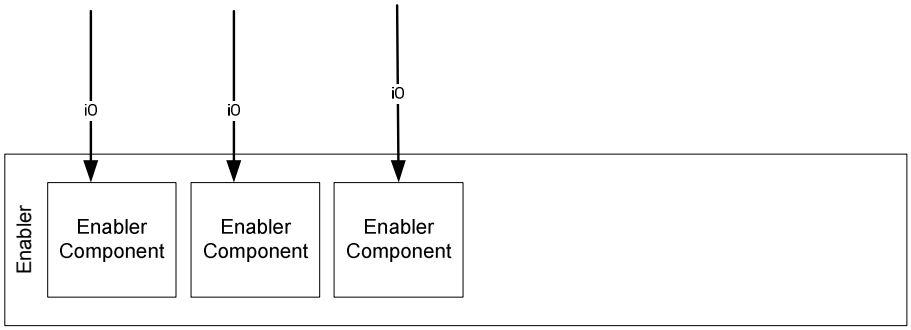



**Figure 4: OGSA View**

# 6. Description of selected Enablers in OGSA Suites

## 6.1 Person-to-person communications

The person-to-person communications OGSA Suite represents messaging and other communications means in their different forms that facilitate or encourage communication between users.

### 6.1.1 Enablers in this OGSA Suite

The Enablers in the person-to-person communications OGSA Suite are:

- Converged IP Messaging [OMA-CPM-AD]
- Instant Messaging Presence Service [OMA-Presence-AD]
- Mobile Email [OMA-MEM_AD]
- Multimedia Messaging Service [OMA-MMS_AD]
- Push to talk over cellular [OMA-POC_AD]
- SIMPLE Instant Messaging [OMA-SIMPLE-IM]
- Customised Multimedia Ringing [OMA-CMR_AD]

The following Enablers in early AD development stage belong to this OGSA Suite:

- Customised Multimedia Ringing [OMA-CMR_AD]

Figure 5 below gives a graphical overview of the Enablers belonging to this OGSA Suite.

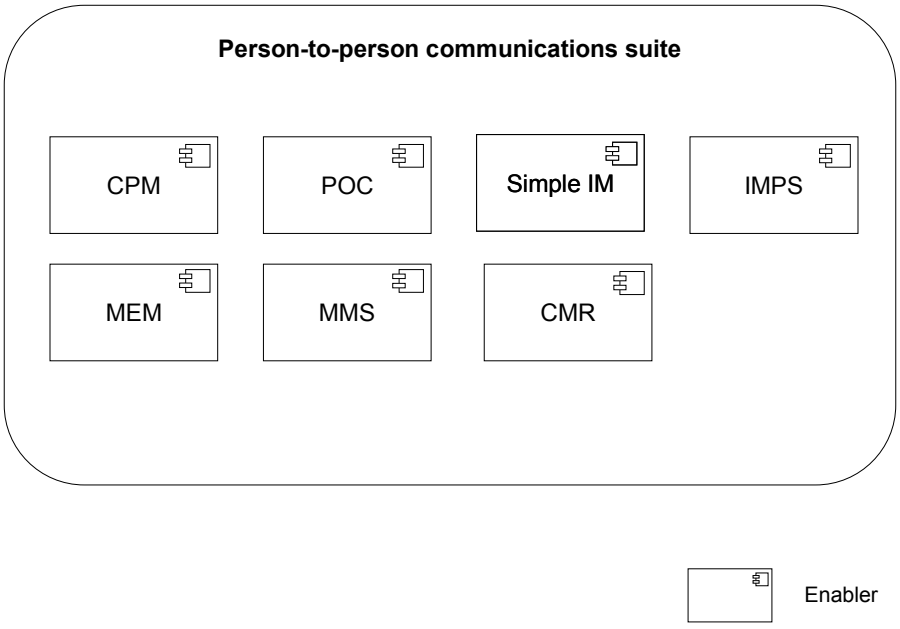



**Figure 5: Enablers of the person-to-person communications OGSA Suite**

### 6.1.2 Dependencies on other Enablers

The Enablers in this OGSA Suite have dependencies on the following other Enablers, taking into account are dependencies explicitly specified in the respective ADs of the Enablers, as well as mappings to data structures defined by the Enablers (e.g. Charging data elements).

- Browsing [OMA-WAP_AD] [8]
- Charging [OMA-CHRG_AD]
- Client Provisioning [OMA-CP_AD]
- Data Synchronisation [OMA-DS-AD] [9]
- Device Management [OMA-DM_AD]
- Digital Rights Management [OMA-DRM_AD]
- Email Notification [OMA-EMN_ERP]
- Location in SIP/IP Core [OMA-LOCSIP-AD]
- Mobile Location Service [OMA-MLS-AD]
- Presence SIMPLE [OMA-Presence-AD]
- Push [OMA-PUSH-AD]
- Push using SIP [OMA-SIP-PUSH-AD]
- Standard Transcoding Interface [OMA-STI-AD]
- User Agent Profile [OMA-UAPROF-ERP]
- Utilization of IMS capabilities [OMA-IMSinOMA-AD]
- XML Document Management [OMA-XDM_AD]

Table 1: depicts how the Enablers of this OGSA Suite are dependent on other Enablers.

| | Relationship with | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Enabler** | Browsing | CHRG | CP | DM | DRM | DS | EMN | IMSinOMA | LOCSIP | MLS | Presence | Push | SIPPush | STI | UAProf |
| CPM | | x | | x | | x | | x | | | x | x | | | |
| IMPS | | | | | | | | | | | | | | | |
| MEM | | | x | x | | | x | | | | | x | x | x | x |
| MMS | x | x | x | x | x | | | | | | | | | x | x |
| CMR | | x | | | | | | | x | x | x | | | | |

**Table 1: Dependencies of the Enablers in the person-to-person communications OGSA Suite on other Enablers**

### 6.1.3 Description of selected Enablers in this OGSA Suite

[8] The AD of Browser_Protocol_Stack-V2_1 references the WAP Arch (see OMA-ERELD-Browser_Protocol_Stack-V2_1)

[9] OMA DS is the successor of SyncML, since SyncML was renamed OMA DS in release 1.1.2.

### 6.1.3.1 CMR Enabler V1_0

The OGSA View for CMR is based on the following specific document [OMA-DCD-AD].

The Customized Multimedia Ringing (CMR) Enabler enhances a CMR End User's experience through presenting the customised multimedia resources instead of the traditional ring back tone or ringing tone according to a specified event, e.g. the establishment of a call, the arrival of a message or mail.

The CMR enabler consists of the following two functional entities:

- The **CMR Server** implements the network side of the CMR Enabler
- The **CMR Client** resides in the CMR End User's Device.

#### 6.1.3.1.1 CMR OGSA View (Normative)

Figure 6: CMR OGSA View below gives a graphical overview of the functional entities of the CMR Enabler and the interfaces, which expose CMR functionality followed by a description in Table 2: Interfaces exposing CMR functionality.

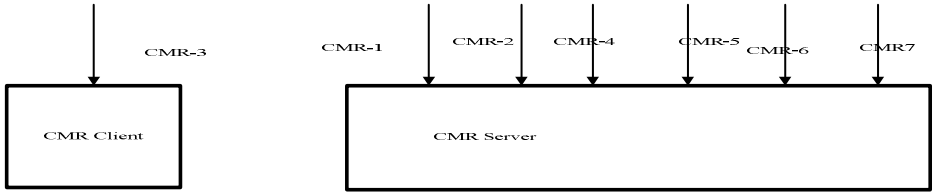



**Figure 6: CMR OGSA View**

| Functional entities | Functionality provided | Via interface | Protocol used |
|---|---|---|---|
| CMR Client | • Send the call/session requests to the CMR Client, the requests may contain CMR specific information, e.g. calling party's media information, URI of CMR Resources,<br>• Receive the responses from the CMR Client | CMR-3 | |
| CMR Server | Interface is used by the CMR Management Client to send service management requests initiated by a CMR Subscriber to the CMR Server and receive the responses from the CMR Server. The supported functionalities of this Interface include:<br>• Personal Resource Library management e.g. purchase/copy(including on-line and off-line copy)/delete of the CMR Resources related to a specific CMR Subscriber<br>• Preference management e.g. query/create/modify/delete the Preference Settings related to a specific CMR Subscriber | CMR-1 | |

| Functional entities | Functionality provided | Via interface | Protocol used |
|---|---|---|---|
| | Interface is used to:<br>• Send the call/session requests, the requests may contain CMR Client's media capabilities, filtering information and other information<br>• Receive the responses from the CMR Server, optionally containing the URI of CMR Resource<br>• Send CMR presentation control (e.g. stop) requests and receive the responses<br>• Send on-line copy requests and receive the responses | CMR-2 | |
| | Interface is used to:<br>• Request the CMR Service (e.g. start/stop a CMR Subscriber's resources presentation to a CMR End User)<br>• Receive the response of the request | CMR-4 | |
| | Interface is used by the CMR Portal to perform the CMR Resource metadata management. | CMR-5 | |
| | Interface is used by the CMR Portal to perform the CMR service management, including:<br>• CMR subscriber' Preference Settings and CMR Personal Resource Library management by CMR Subscriber<br>• CMR service management by SP | CMR-6 | |
| | Interface is used by the CMR Portal to:<br>Request and deliver the service report, including CMR Resource metadata management and CMR service management report etc. | CMR-7 | |

**Table 2: Interfaces exposing CMR functionality**

### 6.1.3.2 MEM Enabler V1_0

The OGSA View for MEM is based on the following specific document [OMA-DCD-AD].

The Mobile Email (MEM) Enabler supports efficient access to email from a mobile device. Email may be personal email provided by an email service provider or corporate email.

The MEM enabler consists of the following three functional entities:

- The MEM Client component, responsible for implementing the mobile email client-side functionality
- The MEM Server component, responsible for implementing the server-side functionality of the OMA MEM Enabler
- The Outband Notification Function component implements the Out-Band Notification functionality of the OMA MEM Enabler.

#### 6.1.3.2.1 MEM OGSA View (Normative)

Figure 7 below gives a graphical overview of the functional entities of the MEM Enabler and the interfaces, which expose MEM functionality followed by a description in Table 3.

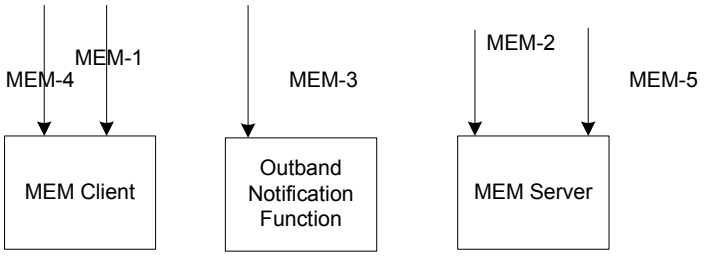



**Figure 7: CMR OGSA View**

| Functional entities | Functionality provided | Via interface | Protocol used |
|---|---|---|---|
| MEM Client | Client interface to interact with the MEM Server | MEM-1 | MEM |
| | Out-band Notification interface for the MEM Client to receive server to client notifications | MEM-4 | |
| MEM Server | Interface is used by the CMR Management Client to send service management requests initiated by a CMR Subscriber to the CMR Server and receive the responses from the CMR Server. The supported functionalities of this Interface include:<br>• Personal Resource Library management e.g. purchase/copy(including on-line and off-line copy)/delete of the CMR Resources related to a specific CMR Subscriber<br>• Preference management e.g. query/create/modify/delete the Preference Settings related to a specific CMR Subscriber | MEM-2 | |

| Functional entities | Functionality provided | Via interface | Protocol used |
|---|---|---|---|
| | Interface is used to:<br>• Send the call/session requests, the requests may contain CMR Client's media capabilities, filtering information and other information<br>• Receive the responses from the CMR Server, optionally containing the URI of CMR Resource<br>• Send CMR presentation control (e.g. stop) requests and receive the responses<br>• Send on-line copy requests and receive the responses | MEM-5 | |
| Outband Notification Function | Out-band Notification interface for the MEM Server to generate server to client notifications | MEM-3 | |

**Table 3: Interfaces exposing MEM functionality**

# 6.2 Access to content

The access to content OGSA Suite enables access to digital content through multiple terminals so that the terminals become entertainment devices, by providing architectures and functionalities enabling users to subscribe to, and/or be able to receive multimedia content.

## 6.2.1 Enablers in this OGSA Suite

The Enablers in the access to content OGSA Suite are:

- Browser Protocol Stack [OMA-BPS_ERP][10]
- Browsing [OMA-WAP_AD] [11]
- Digital Rights Management [OMA-DRM_AD]
- Dynamic Content Delivery [OMA-DCD-AD]
- Games Services Client Server Interface [OMA-GS_AD]
- Mobile Advertising [OMA-MobAd_AD]
- Mobile Broadcast Services [OMA-BCAST_AD]
- Multi-modal Multi-device [OMA-MMMD_AD]
- Rich Media Environment [OMA-RME_AD]
- Scalable Vector Graphics Mobile Domain [OMA-SVG-TS]
- Secure Content Exchange [OMA-SCE_AD]
- Secure Removable Media [OMA-SRM_AD]

[10] The AD of Browser_Protocol_Stack-V2_1 references the WAP Arch (see OMA-ERELD-Browser_Protocol_Stack-V2_1)

[11] The AD of Browser Conformance for Interoperability references the WAP Arch (see OMA-ERELD-Browsing-V2_3)

The following Enablers in early AD development stage belong to this OGSA Suite:

- In-Game Advertising [OMA-IGA_AD]
- Mobile Codes [OMA-MC_AD]
- Secure Removable Media (next version 1.1) [OMA-SRM_AD_next]

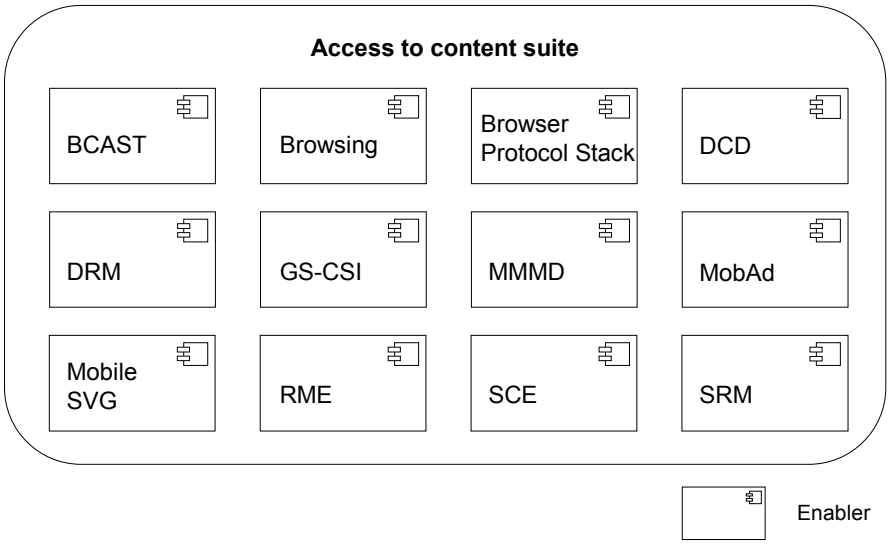



**Figure 8: Enablers of the access to content OGSA Suite**

## 6.2.2 Dependencies on other Enablers

The Enablers in this OGSA Suite have dependencies on the following other Enablers, taking into account dependencies explicitly specified in the respective ADs of the Enablers, as well as mappings to data structures defined by the Enablers (e.g. Charging data elements).

- Application Layer Security Common Functions [OMA-SEC_CF_AD]
- Browsing [OMA-WAP_AD] [12]
- Categorisation Based Content Screening [OMA-CBCS-AD]
- Charging [OMA-CHRG_AD]
- Client Provisioning [OMA-CP_AD]
- Client Side Content Screening Framework [OMA-CSCSF_AD]
- Dynamic Content Delivery [OMA-DCD-AD]
- Device Management [OMA-DM_AD]
- Device Profiles Evolution [OMA-DPE_AD]
- Digital Rights Management [OMA-DRM_AD]
- Mobile Broadcast Services [OMA-BCAST_AD]
- Mobile Location Protocol [OMA-MLP-TS]

[12] The AD of Browser Conformance for Interoperability references the WAP Arch (see OMA-ERELD-Browsing-V2_3)

- Mobile Location Services [OMA-MLS-AD]
- Online Certificate Status Protocol [OMA-OCSPMP-ERP]
- Presence SIMPLE [OMA-Presence-AD]
- Push [OMA-PUSH-AD]
- Push using SIP [OMA-SIP-PUSH-AD]
- Secure Content Exchange [OMA-SCE_AD]
- User Agent Profile [OMA-UAPROF-ERP]
- URI Schemes for the Mobile Applications Environment [OMA-URI-Schemes-ERP]

Table 4: depicts how the Enablers of this OGSA Suite are dependent on other Enablers.

| | Relationship with | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Enabler** | BCAST | Browsing | CBCS | CHRG | CP | CSCSF | DCD | DM | DPE | DRM | MLP | MLS | OCSP | Presence | Push | SCE | SEC_CF | SIPPush | UAProf | URI |
| BCAST | | | | x | | | | x | | x | x | | | | | | | | | |
| Browser Protocol Stack | | | | | | | | | | | | | | | | | | | | |
| Browsing | | | | | | | | | | | | | | | | | | | | |
| DCD | x | x | x | x | | x | | x | x | x | | x | | x | x | | | x | x | |
| DRM | | | | | | | | | | | | | | | | | | | | |
| GS-CSI | | | | | | | | | | | | | | | | | | | | |
| MMMD | | | | | | | | | | | | | | | | | | | | |
| MobAd | x | | | | | | x | | | | | | | | | | | | | |
| Mobile SVG | | | | | | | | | | | | | | | | | | | | |
| RME | x | x | | | | | | | | x | | | | | x | | | | x | |
| SCE | | | | | | | | | | x | | | x | | | | | | | |
| SRM 1.0 | | | | | | | | | | x | | | | | | x | | | | |

**Table 4: Dependencies of the Enablers in the access to content OGSA Suite on other Enablers**

## 6.2.3 Description of selected Enablers in this OGSA Suite

### 6.2.3.1 DCD Enabler V1_0

The OGSA View for DCD is based on the following specific document [OMA-DCD-AD].

The Dynamic Content Delivery (DCD) Enabler defines a common mechanism to enable periodic delivery of personalised or customized content either on a one-to-one (point-to-point) or one-to-many (broadcast) basis. The delivery of DCD Content may be based on the subscription and preferences of a user, operator or service provider. As a complementary delivery mechanism to the existing mechanisms, e.g. browsing, messaging, etc., it will reuse as much existing technology as possible, while providing the added benefits of delivery control management, and an enhanced user experience. The content delivery will support various network technologies (i.e. network types and/or bearers), and may operate autonomously in the background.

The DCD Enabler includes the following features:

- A generic Client framework that allows automated registration of DCD enabled applications;
- The ability to allow customization of the delivery of content by the DCD client in the broadcast scenario;
- The asynchronous delivery of content utilizing both point-to-point and broadcast bearers;
- Content delivery and subscription based notification mechanisms between DCD Client and DCD Server for both point-to-point and broadcast bearers;
- DCD envelope mechanism that allows DCD application and content interoperability between DCD Client and DCD Server.

The DCD Enabler consists of the following functional entities:

- **DCD Client (DCDC):** DCD Client resides in the mobile terminal and is used to communicate with the DCD Server. Three different logical functions can be differentiated inside this entity. The Subscription and Administration function (Client component), in charge of handling the exchange of service management information with the DCD Server. The Content Reception and Storage Management function, in charge of handling the content reception from the server. Finally, the Client Application Interaction Function that provides the necessary functions to make possible the interaction between DCD Enabler supported services and registered DCD Enabled Client Applications.
- **DCD Server:** DCD Server implements the application level network functionality for the DCD application. It is responsible for the fulfilment of Subscription and Administration functions in order to handling the exchange of service management information between the DCD Server and DCD Client, and between the DCD Server and the Content Provider, such as when the Content Provider handles subscriptions, as well as for the fulfilment of the Distribution and Adaptation function in order to distribute DCD Content and DCD Content notifications to the DCD Client.

The following entities are out of the scope, but may interact with the DCD Enabler:

- **DCD-Enabled Client Applications:** DCD-Enabled Client Applications are mobile-terminal-based applications, which can interact with the DCD Client in order to enable content delivery to the end user.
- **DCD Content Provider:** The DCD Content Providers interact with the DCD Server in order to serve requests for content, e.g. as any normal web server, providing channel metadata which defines the characteristics of the channels it provides, supporting one or more content publication / delivery methods, or publishing available content to the DCD Server.

#### 6.2.3.1.1 DCD OGSA View (Normative)

Figure 9 below gives a graphical overview of the functional entities of the DCD Enabler and the interfaces, which expose DCD functionality followed by a description in Table 5:.

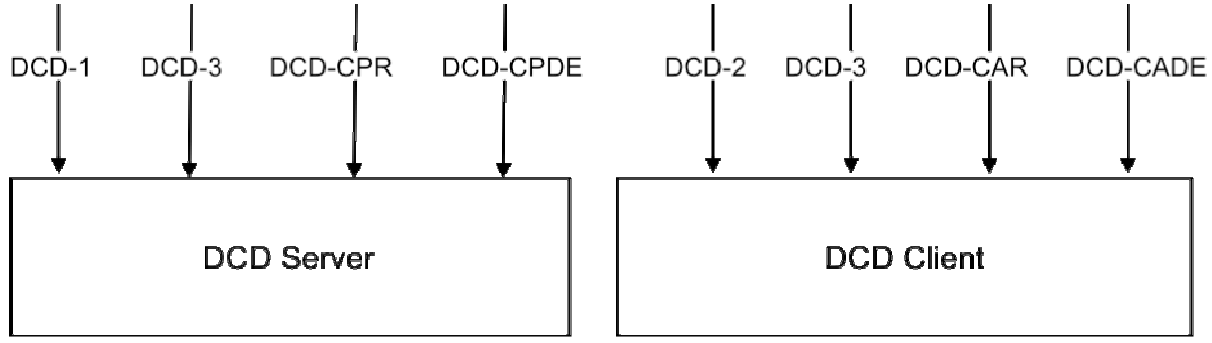



**Figure 9: DCD OGSA View**

| Functional entities | Functionality provided | Via interface | Protocol used |
|---|---|---|---|
| DCD Client (DCDC) | Channel subscription and administration functions<br>• DCD Client Activation and session management<br>• DCD-Enabled Client Application registration actions (Register, Deregister)<br>• Service administration actions, e.g. change channel delivery options, suspend / resume channel<br>• Channel Discovery actions<br>• Channel subscription actions (subscribe / unsubscribe, subscription validation for external subscriptions) | DCD-3 | |

| Functional entities | Functionality provided | Via interface | Protocol used |
|---|---|---|---|
| | • Automatic request upon notification of content availability at the DCD Server<br>• Automatic request for content upon a predefined schedule<br>• Automatic request for content upon stored content expiration<br>On-demand request for content retrieval or submission by the DCD-Enabled Client Application, e.g. upon end-user interaction or application-initiated interaction | DCD-2 | |
| | • Register / deregister of DCD-Enabled Client Application with the DCD Client (dynamically), supplying Application Profile (including the Channel Metadata) to the DCD Enabler<br>• Channel subscription actions (subscribe / unsubscribe, subscription validation for external subscriptions with DCD-Enabled Client Application)<br>Note: The mechanism is client platform specific while the data schema for this interface is defined by DCD. | DCD-CAR | |
| | • On-demand request for content retrieval or submission by the DCD-Enabled Client Application, e.g. upon end-user interaction or application-initiated interaction<br>• Providing content availability notifications and / or content to the DCD-Enabled Client Application<br>• Service administration actions, e.g. suspend / resume channel<br>• Channel Discovery actions<br>Note: The mechanism is client platform specific while the data schema for this interface is defined by DCD. | DCD-CADE | Client platform specific; |
| DCD Server | Delivers pushed notifications and / or content to the DCD Client, e.g.<br>• Notification of content availability for client-invoked retrieval via DCD-1 interface<br>• Direct delivery of content | DCD-1 | point-to-point content push interface<br>point-to-multi-point broadcast interface, e.g. HTTP, Cell Broadcast |
| | Channel subscription and administration functions<br>• Service administration actions, e.g. change channel delivery options, suspend / resume channel<br>• Channel Discovery actions<br>• Channel subscription actions (subscribe / unsubscribe, subscription validation for external subscriptions) | DCD-3 | |
| | Registration of new content channels with the DCD Server<br>Updating of content channels with the DCD Server<br>Exchange subscription related information between the DCD Content Provider and the DCD Server<br>Notification to the DCD Content Provider about subscription events from a DCD Client | DCD-CPR | |
| | Publishing of content from content Provider at the DCD Server<br>Retrieval of content from the Content Provider | DCD-CPDE | |

**Table 5: Interfaces exposing DCD functionality**

#### 6.2.3.2 MobAd Enabler V1_0

The OGSA View for MobAd is based on the following specific document [OMA-DCD-AD].

The objective of the MobAd Enabler architecture is to define network-side and device-side MobAd Enabler components, the interface(s) between them and the interface(s) exposed by those components to some entities that rely on MobAd Enabler (i.e. device-side Ad Apps as well as network-side SP Apps). The MobAd enabler consists of the following functional entities:

- The **Ad Server** performs actions grouped in the following high-level functions:
  - Ad selection function
  - Ad delivery function
  - Ad Metrics data handling function
  - User / service data management function
- The **Ad Engine** performs actions grouped in the following high-level functions:
  - Ad acquisition and delivery function
  - Ad selection function
  - Ad Metrics data handling function
  - User / service / device data handling function

##### 6.2.3.2.1 MobAd OGSA View (Normative)

Figure 10: MobAd OGSA Viewbelow gives a graphical overview of the functional entities of the MobAd enabler and the interfaces, which expose functionality to entities external to the enabler, followed by a description in Table 6: Interfaces exposing MobAd functionality

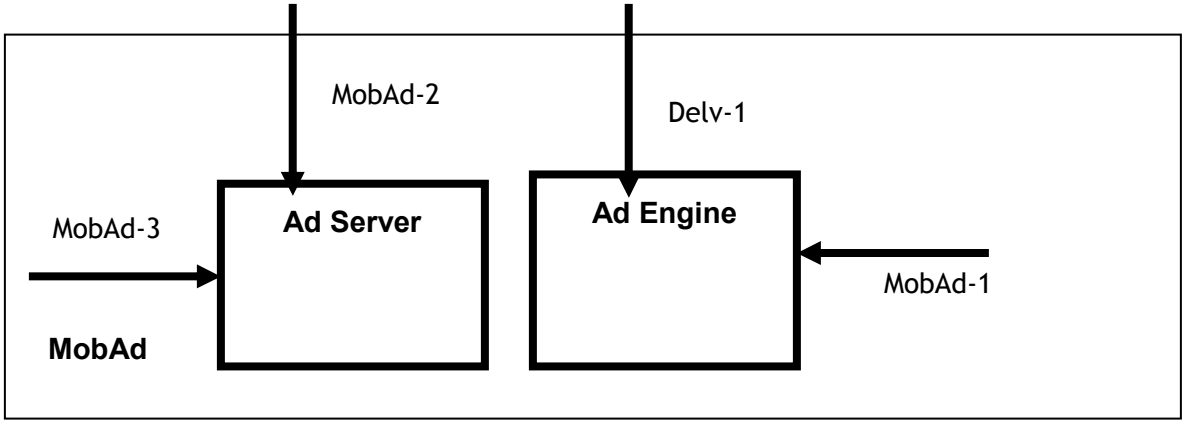



**Figure 10: MobAd OGSA View**

| Functional entities | Functionality provided | Via interface | Protocol used |
|---|---|---|---|
| Ad Server | The SP App uses this interface to request and obtain Ad(s), reference(s) to Ad(s), associated Ad(s) identifiers This interface can also be used by the Ad Server to inform the SP App that some Ad(s) (stored locally by the SP App) are supposed to be deleted. This can be achieved either by attaching Ad deletion information to an Ad Server response following an SP App request for Ad(s), or by returning such information in response to a specific request for updates on Ad's validity.<br>The message pattern supported by MobAd-2 is a request issued by SP App towards Ad Server followed by a synchronous response from Ad Server to SP App. | MobAd-2 | HTTP 1.1 |
| | Interface to request and obtain Ad(s), reference(s) to Ad(s), their associated Ad(s) ID(s) and Ad Metadata from the Ad Server, as well as to report Ad Metrics data to the Ad Server, accompanied by the associated Ad(s) ID(s).<br>This interface can also be used to inform the Ad Engine that some Ad(s) (stored locally by the Ad Engine) are supposed to be deleted. This interface may also be used by the Ad Engine to retrieve MobAd Rules and to provide notification to the Ad Server. | MobAd-3 | HTTP 1.1 |
| Ad Engine | The Ad App uses this interface to request and obtain Ads and their associated Ads identifiers from the Ad Engine, as well as to report Ad Metrics data to the Ad Engine, accompanied by the associated Ads identifiers. | MobAd-1 | May be realized/implemented using other OMA enablers or protocols to which adaptation is defined in adaptation specification. |
| | Optional interface exposed by the Ad Engine. The Ad Engine receives Ad(s) and/or Ad Metadata over this interface from the Ad Server via underlying push and/or broadcast delivery mechanisms. The Ad Server uses this interface to push either Ad(s) or notification that Ad(s) are available for retrieval.<br>The Ad Server may also use this interface to provide service notification to the Ad Engine | Delv-1 | The DELV-1 is a MobAd interface which may optionally be realized/implemented using other OMA enablers or protocols to which adaptation is defined in adaptation specification. |

**Table 6: Interfaces exposing MobAd functionality**

## 6.3 Service access

The Service access OGSA Suite includes Enablers that facilitate exposing of OMA Enablers functionality in a secure and controlled way.

Such exposure may occur towards other OMA Enablers and applications (third party or otherwise), through the Enabler's I0 interface (where present).

### 6.3.1 Enablers in this OGSA Suite

The Enablers in the Service access OGSA Suite are:

- OMA Web Services [OMA-OWSER_AD]
- OWSER Network Identity [OMA-OWSER_NI_AD]
- Parlay in OSE [OMA-PIOSE_AD]
- Parlay Service Access [OMA-PSA_AD]
- Policy Evaluation, Enforcement & Management [OMA-PEEM_AD]
- Next Generation Service Interfaces [OMA-NGSI-AD]

The following Enablers in early AD development stage belong to this OGSA Suite:

- RESTful bindings for Parlay X Web Services [OMA-REST_ERP]

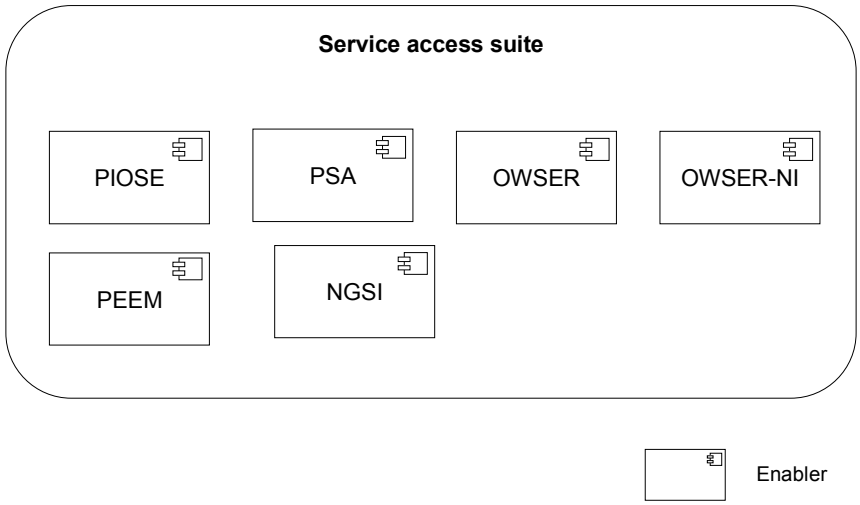



**Figure 11: Enablers of the service access OGSA Suite.**

### 6.3.2 Dependencies on other Enablers

The Enablers in this OGSA Suite have dependencies on the following other Enablers, taking into account dependencies explicitly specified in the respective ADs of the Enablers, as well as mappings to data structures defined by the Enablers (e.g. Charging data elements).

- OWSER Network Identity [OMA-OWSER_NI_AD]
- Parlay in OSE [OMA-PSA_AD]

Table 7: depicts how the Enablers of this OGSA Suite are dependent on other Enablers.

| Enabler | Relationship with | | |
|---|---|---|---|
| | OWSER | PIOSE | PSA |
| OWSER | | | |
| OWSER-NI | X | | |
| PEEM | | | |
| PIOSE | | | |
| PSA | | X | |
| NGSI | | | X |

**Table 7: Dependencies of the Enablers in the service access OGSA Suite on other Enablers**

## 6.3.3 Description of selected Enablers in this OGSA Suite

### 6.3.3.1 PEEM Enabler V1_0

The OGSA View for PEEM is based on the following specific document [OMA-PEEM_AD].

The PEEM Enabler evaluates and/or enforces policies. Policies are applied to requests to, or responses from resources or, when explicitly called by a resource.

Policies are formalisms that are used to express business, engineering or process criteria represented by a combination of policy conditions and actions.

Note that this Enabler does not specify individual policies, but rather specifies on how to express policies.

PEEM supports two options for expressing policies:

- A ruleset-based option: Each rule is evaluated as separate entity, and the combination of the results of the processing of all the rules in the ruleset determines the policy outcome (notice that a precedence mechanism may be needed). The Policy Expression Language used is the XML Common Policy schema from IETF
- A workflow-based option: The entire policy is processed as a whole, following a flowchart approach, where at each node in the graph, a rule is being processed. The Policy Expression Language used is Web Services Business Process Execution Language (WSBPEL 2.0) from OASIS.

The PEEM Enabler consists of a single functional entity:

- **Policy Evaluation and Enforcement Management (PEEM):** This entity provides the following features:
    - identifies the policies associated with the request.
    - processes the policies, i.e. goes through the following steps:
        - evaluates policies using messages received and other context information. The component may delegate to other resources where appropriate
        - executes the policy actions resulting from a positive evaluation of the policy conditions. The component may use delegation to other resources where appropriate, and
        - after completing all previous processing the PEEM Enabler
            - may return, a policy decision to a requestor. The policy processing may complete by returning a policy decision to the requesting resource or perform enforcement itself. When a policy decision is returned to a resource, that resource is in control of deciding how to handle the rendered decision.
            - may allow a request to continue to its original target destination. The policy processing completes by forwarding the original request to the destination resource (if the processing resulted into a “pass” condition) or by returning an error to the originating entity (if the processing resulted into a “fail” condition)

- provides the functions of describing, creating, updating, deleting, provisioning and viewing of policies.

#### 6.3.3.1.1 PEEM OGSA View (Normative)

Figure 12 below gives a graphical overview of the functional entities of the PEEM Enabler and the interfaces, which expose PEEM functionality, followed by a description in Table 8.

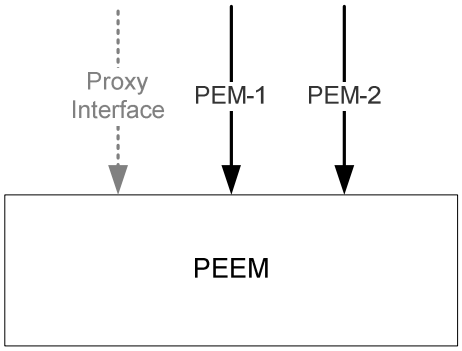



**Figure 12: PEEM OGSA View**

| Functional entities | Functionality provided | Via interface | Protocol used |
|---|---|---|---|
| PEEM | The Proxy interface is used to exchange messages compliant to the target Enablers or more generally messages compliant to combination of the target resource interface and the set of parameters that must be added to requests through that resource's interface, as required to satisfy policies that are to be processed when exposing the resource.<br>The Proxy Interface is not specified by PEEM. | Proxy Interface | Not specified |
| | The PEM-1 interface is used to make a direct request for policy processing. PEEM processes the request and may return a policy decision (the result of the policy evaluation) to the originating resource, using the same interface. Alternatively, it may also perform policy enforcement and possibly return no value to the requester. | PEM-1 | Diameter or SOAP |
| | The PEM-2 interface is used to make a request for policy management (e.g. creating, updating, deleting, and viewing policies) | PEM-2 | XCAP |

**Table 8: Interfaces exposing PEEM functionality**

### 6.3.3.2 NGSI Enabler V1_0

The OGSA View for NGSI is based on the following specific document [OMA-PEEM_AD].

- NGSI v1.0 is the standardization of functional interfaces for the following functional entities: Data Configuration and Management, Call Control and Configuration, Multimedia List Handling, Context Management, Identity Control, Service Registration and Discovery functions. NGSI v1.0 covers both new functional interfaces as well as extensions of existing PSA v1.0 [OMA-PSA] interfaces.

#### 6.3.3.2.1 NGSI OGSA View (Normative)

Figure 13: NGSI OGSA View below gives a graphical overview of the functional entities of the NGSI Enabler and the interfaces, which expose NGSI functionality, followed by a description in Table 9: Interfaces exposing NGSI functionality.

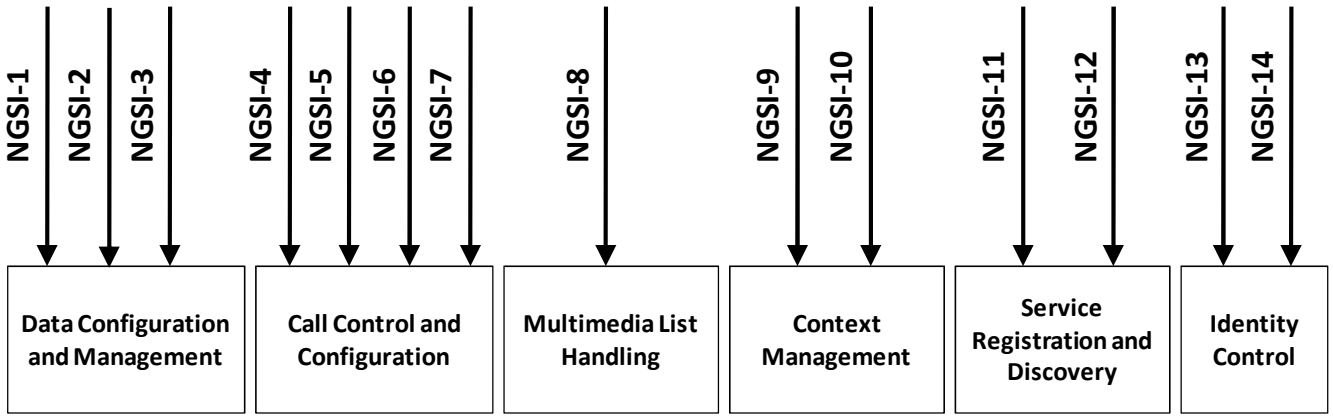



**Figure 13: NGSI OGSA View**

| Functional entities | Functionality provided | Via interface | Protocol used |
|---|---|---|---|
| The Data Configuration and Management | Generic Data Management Interface | NGSI-1 | Not specified |
| | Generic Data Change Notification Interface | NGSI-2 | Not specified |
| | Group Change Notification Interface | NGSI-3 | Not specified |
| Call Control and Configuration | Call Control Extension Interface | NGSI-4 | Not specified |
| | Call Notification Extension Interface | NGSI-5 | Not specified |
| | Call Handling Extension Interface | NGSI-6 | Not specified |
| | Multimedia Conference Extension Interface | NGSI-7 | Not specified |
| Multimedia List Handling | Multimedia List Handling Interface | NGSI-8 | Not specified |
| Context Management | Context Entity Discovery Interface | NGSI-9 | Not specified |
| | Context Information Interface | NGSI-10 | Not specified |
| Service Registration and Discovery | Service Registration Interface | NGSI-11 | Not specified |
| | Service Discovery Interface | NGSI-12 | Not specified |
| Identity Control | Identity Resolution Interface | NGSI-13 | Not specified |
| | Identity Management Interface | NGSI-14 | Not specified |

**Table 9: Interfaces exposing NGSI functionality**

# 6.4 Device enabling

The device enabling OGSA Suite consists of the OMA Enablers that provide functions and tools related to UE that may be used in various OGSA Suites for the support of services enabled by that OGSA Suite.

## 6.4.1 Enablers in this OGSA Suite

The Enablers in the device enabling OGSA Suite are:

- Client Provisioning [OMA-CP_AD]
- Connectivity Management Object [OMA-ConnMO_AD]
- Data Synchronization [OMA-DS-AD] [13]
- Device Capability Management Object [OMA-DCMO_AD]
- Device Management [OMA-DM_AD]
- Device Management Scheduling [OMA-DMSched-AD]
- Device Profiles Evolution [OMA-DPE_AD]
- Diagnostics and Monitoring [OMA-DiagMon_AD]
- Firmware Update Management Object [OMA-FUMO_AD]
- Lock And Wipe Management Object [OMA-LAWMO-AD]
- Smart Card Web Server [OMA-SCWS_AD]
- Software Component Management Object [OMA-SCOMO-AD]
- User Agent Profile [OMA-UAPROF-ERP]

The following Enablers in early AD development stage belong to this OGSA Suite:

- Device Management Smart Card [OMA-DMSC-AD]

[13] OMA DS is the successor of SyncML, since SyncML was renamed OMA DS in release 1.1.2.

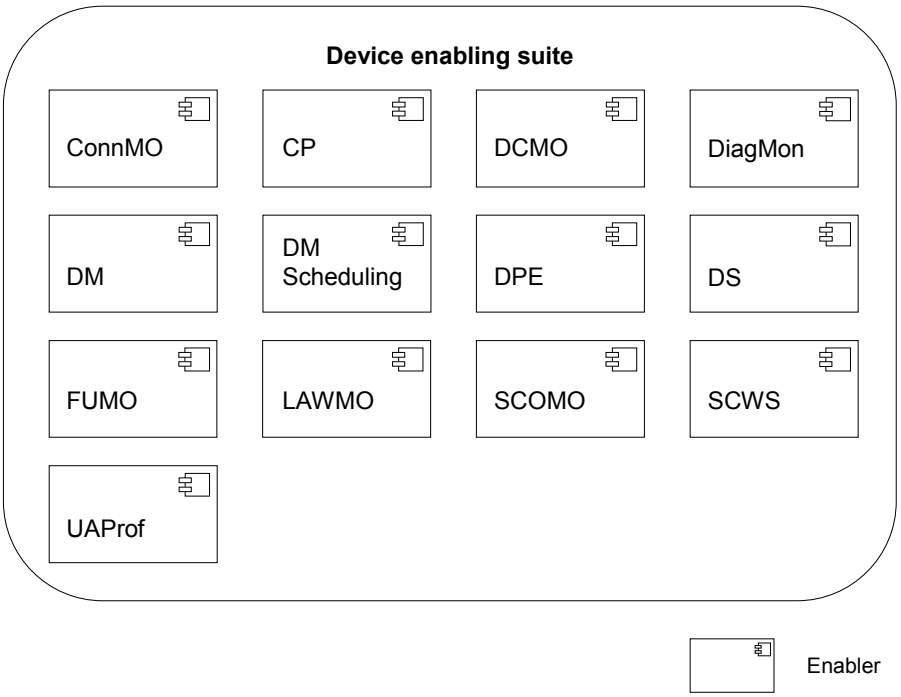



**Figure 14: Enablers of the device enabling OGSA Suite**

## 6.4.2 Dependencies on other Enablers

The Enablers in this OGSA Suite have dependencies on the following other Enablers, taking into account dependencies explicitly specified in the respective ADs of the Enablers, as well as mappings to data structures defined by the Enablers (e.g. Charging data elements).

- Application Layer Security Common Functions [OMA-SEC_CF_AD]
- Browsing [OMA-WAP_AD]
- Client Provisioning [OMA-CP_AD]
- Data Synchronisation [OMA-DS-AD]
- Device Management [OMA-DM_AD]
- Device Profiles Evolution [OMA-DPE_AD]
- Download over the air [OMA-DLOTA-AD]
- Email Notification [OMA-EMN_ERP]
- Push [OMA-PUSH-AD]
- Push using SIP [OMA-SIP-PUSH-AD]
- Smart Card Web Server [OMA-SCWS_AD]

Table 10 depicts how the Enablers of this OGSA Suite are dependent on other Enablers.

| Enabler | Relationship with | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | Browsing | CP | DLOTA | DM | DPE | DS | EMN | Push | SCWS | SEC_CF | SIPPush |
| ConnMO | | | | x | | | | | | | |
| CP | | | | | | | | | | | |
| DCMO | | | | x | x | | | | | | |
| DiagMon | | | | x | | | | | | | |
| DM | | | | | | x | | | | | x |
| DM Scheduling | | | | x | | | | | | | |
| DPE | | x | | x | | | | | | x | |
| DS | | | | x | | | x | x | | | x |
| FUMO | | | x | x | | | | | | | |
| LAWMO | | | | x | | | | | | | |
| SCOMO | | | x | x | | | | | | | |
| SCWS | x | | | | | | | | | | |
| UAProf | | | | | | | | | | | |

**Table 10: Dependencies of the Enablers in the device enabling OGSA Suite on other Enablers**

### 6.4.3 Description of selected Enablers in this OGSA Suite

To be provided in a future release.

## 6.5 Network access

The network access OGSA Suite includes Enablers that provide access to the resources in the networks and their exposed functionality.

### 6.5.1 Enablers in this OGSA Suite

The Enablers in the network access OGSA Suite are:

- Parlay in OSE [OMA-PIOSE_AD]
- Utilization of IMS capabilities [OMA-IMSinOMA-AD]

Figure 15 below gives a graphical overview of the OMA Enablers belonging to OGSA network access OGSA Suite:

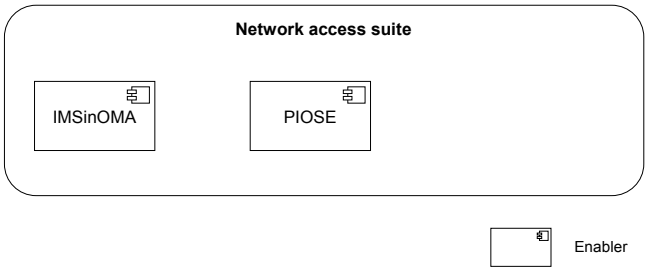



**Figure 15: Enablers of the network access OGSA Suite**

### 6.5.2 Dependencies on other Enablers

The Enablers in this OGSA Suite have no relationships to other Enablers.

### 6.5.3 Description of selected Enablers in this OGSA Suite

To be provided in a future release.

## 6.6 Supporting Enablers

The supporting Enablers are Enablers that provide functions and tools that may be used in various OGSA Suites for the support of services enabled by that OGSA Suite. These Enablers have different natures and include provisioning of parameters and services, data synchronisation, service platform common architecture, interconnections and some other horizontal activities such as security, privacy or charging etc. Supporting Enablers may be used by the above listed OGSA Suites.

### 6.6.1 Enablers in this OGSA Suite

The supporting Enablers are:

- Application Layer Security Common Functions [OMA-SEC_CF_AD]
- Categorisation Based Content Screening [OMA-CBCS-AD]
- Charging [OMA-CHRG_AD]
- Client Side Content Screening Framework [OMA-CSCSF_AD]
- Download over the air [OMA-DLOTA-AD]
- Email notification [OMA-EMN_ERP]
- External Functionality Interface [OMA-EFI_ERP]
- General Service Subscription Management [OMA-GSSM-AD]
- Global Permissions Management [OMA-GPM-AD]
- Location in SIP/IP Core [OMA-LOCSIP-AD]
- Look and Feel Customisation [OMA-LFC-AD]
- Mobile Location Protocol [OMA-MLP-TS]
- Mobile Location Services [OMA-MLS-AD]
- OMA Domain Name System [OMA-WPDNS-ERP]
- Online Certificate Status Protocol [OMA-OCSPMP-ERP]
- On-Board Key Generation and Key Enrolment [OMA-OBKG-ERP]
- Presence SIMPLE [OMA-Presence-AD]
- Push [OMA-PUSH-AD]
- Secure Content Identification Mechanism [OMA-SCIM-AD]
- Secure User Plane Location [OMA-SUPL-AD]
- SIP Push [OMA-SIP-PUSH-AD]
- Standard Transcoding Interface [OMA-STI-AD]
- URI Schemes for the Mobile Applications Environment [OMA-URI-Schemes-ERP]
- vObject [OMA-vObject-ERP]
- XML Document Management [OMA-XDM_AD]
- Wireless Public Key Infrastructure [OMA-WPKI_ERP]
- Content Management Interface [OMA-CMI_AD]
- Presence Access Layer [OMA-PAL_AD]
- Converged Address Book [OMA-CAB-AD]

The following Enablers in early AD development stage belong to this OGSA Suite:

- Condition-based URIs selection [OMA-CBUS_AD]
- Push (next version 2.3) [OMA-PUSH-AD_next]
- XML Data Management (next version 2.1) [OMA-XDM_AD_next]

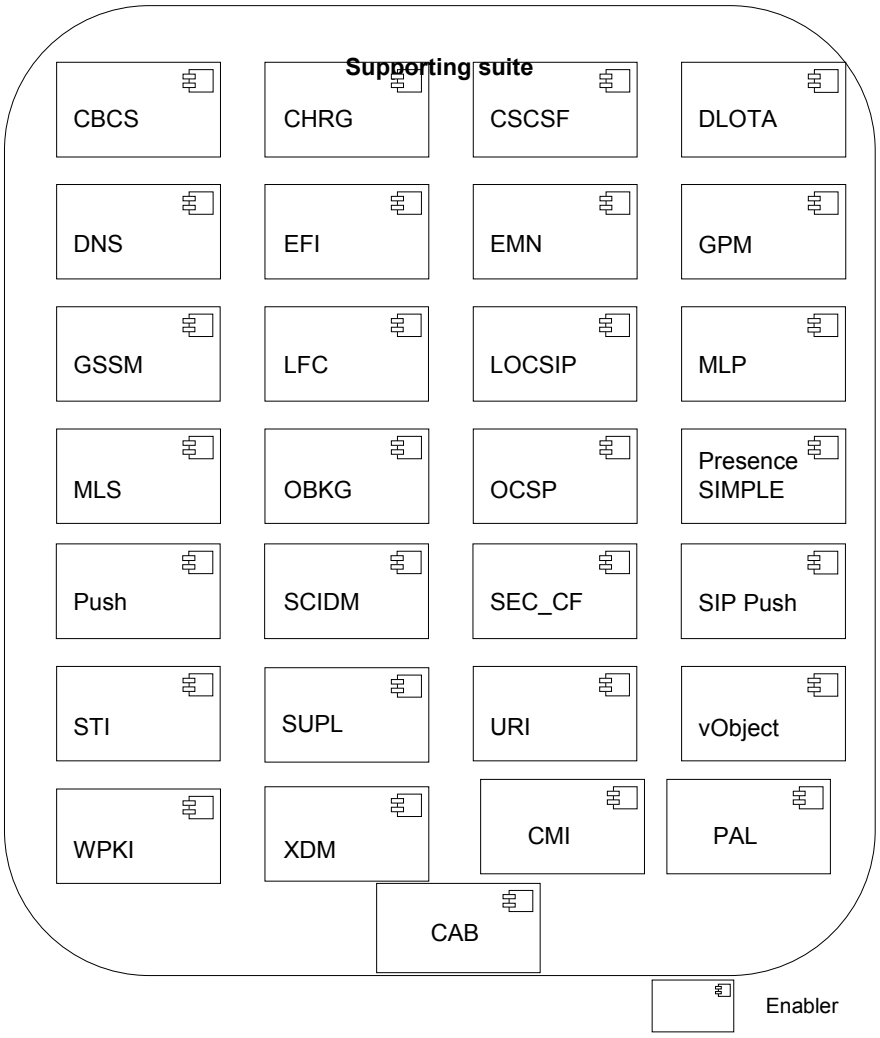



**Figure 16: Enablers of the supporting OGSA Suite**

## 6.6.2 Dependencies on other Enablers

The Enablers in this OGSA Suite have dependencies on the following other Enablers, taking into account dependencies explicitly specified in the respective ADs of the Enablers, as well as mappings to data structures defined by the Enablers (e.g. Charging data elements).

- Application Layer Security Common Functions [OMA-SEC_CF_AD]

- Browser Protocol Stack [OMA-BPS_ERP][14]
- Browsing [OMA-WAP_AD]
- Charging [OMA-CHRG_AD]
- Device Management [OMA-DM_AD]
- Download over the air [OMA-DLOTA-AD]
- Global Permissions Management [OMA-GPM-AD]
- Mobile Location Services [OMA-MLS-AD]
- OMA Web Services [OMA-OWSER_AD]
- Policy Evaluation, Enforcement & Management [OMA-PEEM_AD]
- Push [OMA-PUSH-AD]
- Push using SIP [OMA-SIP-PUSH-AD]
- User Agent Profile [OMA-UAPROF-ERP]
- Utilization of IMS capabilities [OMA-IMSinOMA-AD]
- XML Document Management [OMA-XDM_AD]

Table 11: Dependencies of the Enablers in the supporting OGSA Suite on other Enablers depicts how the Enablers of this OGSA Suite are dependent on other Enablers.

[14] The AD of Browser_Protocol_Stack-V2_1 references the WAP Arch (see OMA-ERELD-Browser_Protocol_Stack-V2_1)

| Enabler | Relationship with | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Browsing | Browser Prot Stack | CHRG | DLOTA | DM | GPM | IMSinOMA | MLS | OWSER | PEEM | Push | SEC_CF | SIPPush | UAProf | XDM |
| CBCS | | | | | | | | | | x | | | | | |
| CHRG | | | | | | | | | | | | | | | |
| CSCSF | | | | | | | | | | | | | | | |
| DLOTA | | | | | | | | | | | | | | | |
| DNS | | | | | | | | | | | | | | | |
| EFI | | | | | | | | | | | | | | | |
| EMN | | | | | | | | | | | | | | | |
| GPM | | | | | | | | | | x | | | | | |
| GSSM | | | | | | | | | | x | | | | | |
| LFC | | | | x | x | | | | | | | | | | |
| LOCSIP | | | | | | x | x | | | | | | | | x |
| MLP | | | | | | | | | | | | | | | |
| MLS | | | | | | | | | | | | | | | |
| OBKG | | | | | | | | | | | | | | | |
| OCSP | | | | | | | | | | | | | | | |
| Presence SIMPLE | | | | | x | | x | | | | | | | | x |
| Push (V2.2) | x | x | | | | | | | | | | | x | x | |
| SCIDM | | | | | | | | | | | | x | | | |
| SEC_CF | | | | | | | | | | | | | | | |
| SIP Push | | | | | | | x | | | | | | | x | |
| STI | | | x | | | | | | x | | | | | | |
| SUPL | | | | | | | | x | | | x | | x | | |
| URI | | | | | | | | | | | | | | | |
| vOBJECT IOP Profile | | | | | | | | | | | | | | | |
| WPKI | | | | | | | | | | | | | | | |
| XDM (V2.0) | | | x | | x | | x | | | | | | | | |

| Enabler | Browsing | Browser Prot Stack | CHRG | DLOTA | DM | DS | GPM | IMSinOMA |
|---|---|---|---|---|---|---|---|---|
| CAB | | | | | x | x | | |
| CBCS | | | | | | | | |
| CHRG | | | | | | | | |
| CSCSF | | | | | | | | |
| DLOTA | | | | | | | | |
| DNS | | | | | | | | |
| EFI | | | | | | | | |
| EMN | | | | | | | | |
| GPM | | | | | | | | |
| GSSM | | | | | | | | |
| LFC | | | | x | x | | | |
| LOCSIP | | | | | | | x | x |
| MLP | | | | | | | | |
| MLS | | | | | | | | |
| OBKG | | | | | | | | |
| OCSP | | | | | | | | |
| PAL | x | | | | | | | |
| Presence SIMPLE | | | | | x | | | x |
| Push (V2.2) | x | x | | | | | | |
| SCIDM | | | | | | | | |
| SEC_CF | | | | | | | | |
| SIP Push | | | | | | | | x |
| STI | | | x | | | | | |
| SUPL | | | | | | | | |
| URI | | | | | | | | |
| vOBJECT IOP Profile | | | | | | | | |

**Table 11: Dependencies of the Enablers in the supporting OGSA Suite on other Enablers**

## 6.6.3 Description of selected Enablers in this OGSA Suite

### 6.6.3.1 XDM Enabler V2_0

The OGSA View for XDM is based on the following specific document [OMA-XDM_AD].

The XDM Enabler defines a common mechanism to make user-specific, service-related information accessible to other service Enablers. XDM specifies how such information is defined in well-structured XML document, how these documents are accessed and manipulated and how consumers of the documents are notified of changes made to the documents.

The XDM Enabler includes the following features:

- A common protocol, XML Configuration Access Protocol (XCAP), by which Principals can access and manipulate service-related data stored as XML documents.
- A mechanism, SIP subscription/notification, by which Principals can be notified of changes to such documents
- A mechanism, limited XQuery, by which Principals can search service-related data stored as XML documents.

The XDM Enabler consists of the following functional entities

- **XDM Client (XDMC)**: The XDMC accesses various XDMS features as described in [OMA-XDM_AD].
- **Aggregation Proxy**: The Aggregation Proxy is the single contact point for Untrusted XDMCs to access XML documents stored in any XDMS.
- **Search Proxy**: This entity manages search requests from the XDMC to XML documents stored in any XDMS.
- **Subscription Proxy**: The Subscription Proxy is a server entity that receives subscriptions for notification of changes in XML documents stored in any XDMS
- **XDMSs**: This entity is a logical repository that manages XML documents
- **Cross-Network Proxy**: The entity is the single contact point for the XDM Enablers located in different networks to communicate over trusted connection.

#### 6.6.3.1.1 XDM OGSA View (Normative)

Figure 17: XDM OGSA View below gives a graphical overview of the functional entities of the XDM Enabler and the interfaces, which expose XDM, followed by a description in Table 12: Interfaces exposing XDM functionality.

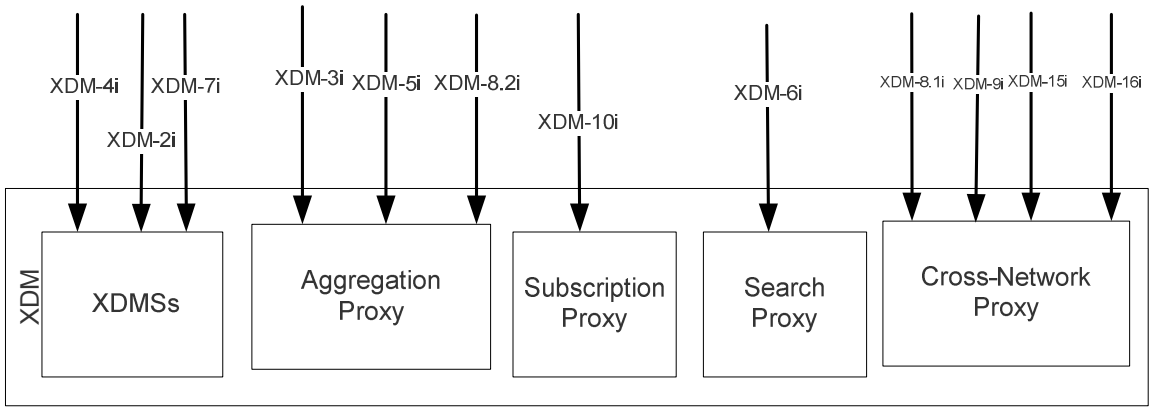



**Figure 17: XDM OGSA View**

| Functional entities | Functionality provided | Via interface | Protocol used |
|---|---|---|---|
| Aggregation Proxy | XML document management (e.g. create, modify, retrieve, delete) by routing the requests to the correct XDMS or Aggregation Proxy of Remote Network;<br>Mutual authentication (between XDMC and Aggregation Proxy);<br>Optional compression/decompression. | XDM-3i | XCAP |
| | Searching information from XML documents stored in any XDMS by routing the requests to the Search Proxy;<br>Mutual authentication (between XDMC and Aggregation Proxy);<br>Optional compression/decompression | XDM-5i | Limited XQuery over HTTP |
| | "Enabler-specific" (acting as Trusted XDMC) XML document management (e.g. create, modify, retrieve, delete) in a remote network by routing the requests to Aggregation Proxy of Remote Network | XDM-8.2i | XCAP |
| Subscription Proxy | Subscription to / notification of the modification of XML documents handled by multiple XDMSs | XDM-10i | SIP |

| Functional entities | Functionality provided | Via interface | Protocol used |
|---|---|---|---|
| Search Proxy | Searching information from XML documents stored in any XDMS | XDM-6i | Limited XQuery over HTTP |
| XDMSs | XML document management (e.g. create, modify, retrieve, delete) handled by a particular XDMS | XDM-4i | XCAP |
| | Subscription to / notification of the modification of XML documents handled by a particular XDMS | XDM-2i | SIP |
| | Forwarding of search requests for Searching information from XML | XDM-7i | Limited XQuery over HTTP |
| Cross-Network Proxy | Forwarding of requests to the Cross-Network Proxy for XML document management of XML documents (e.g. create, modify, retrieve, delete) handled by any XDMS in remote networks;<br>Receiving responses from the Cross-Network Proxy for XML document management of XML documents (e.g. create, modify, retrieve, delete) handled by any XDMS in remote networks. | XDM-8.1i | XCAP |
| | Forwarding of search requests to the Cross-Network Proxy for searches in remote domains;<br>Receiving search responses from the Cross-Network Proxy for searches in remote domains. | XDM-9i | Limited XQuery over HTTP |
| | Forwarding of requests to the Cross-Network Proxy for XML document management of XML documents (e.g. create, modify, retrieve, delete) handled by any XDMS residing in the same domain as the Cross-Network Proxy;<br>Receiving responses from the Cross-Network Proxies for XML document management of XML documents (e.g. create, modify, retrieve, delete) handled by any XDMS residing in the same domain as the Cross-Network Proxy. | XDM-15i | XCAP |
| | Forwarding of search requests to the Cross-Network Proxy for searching information from XML documents stored in any XDMS residing in the same domain as the Cross-Network Proxy;<br>Receiving search responses from the Cross-Network Proxy for the search requests. | XDM-16i | Limited XQuery over HTTP |

**Table 12: Interfaces exposing XDM functionality**

### 6.6.3.2 Charging Enabler V1_1

The OGSA View for Charging is based on the following specific document [OMA-CHRG_AD].

The Charging Enabler enables charging for various types of Chargeable Events to a subscriber's account, possibly maintained by an underlying Charging Infrastructure. It is not a Charging Infrastructure in its own right but a facilitator in the process of providing charging at the application and OMA Enabler level. It builds on existing charging architectures which have already defined models for charging.

It specifies charging interfaces CH-1 (Offline Charging) and CH-2 (Online Charging) with a high-level protocol-independent description and with detailed protocol bindings to Diameter and Web Services .

The Charging Enabler includes the following features:

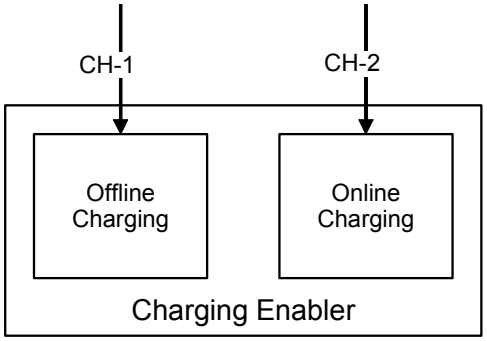
- Time and/or Volume and Subscription based
- Online and Offline charging methods (i.e. prepay and postpay payment methods),
- Mechanism for 'A' party pays
- Third-Party-Pays (TPP) capability
- Operations for refunding or depositing units to the end-user's account
- Capabilities for cost splitting of group services
- Quota Management.
- Correlation/Aggregation
- Rating
- Account Balance Management
- Event and Session Based Charging

The Charging Enabler consists of the following functional entities

- **Charging Enabler**: This entity receives charging requests via either the offline or online charging interface or both.
    - Offline charging is a process where charging information for resource usage is generated concurrently with usage of that resource. The charging information generated for offline charging does not have a real time effect on the service rendered nor does it affect service control.
    - Online charging is a charging process where charging information can affect in real time the service rendered and therefore directly interacts with the session/service control.
- **Charging Enabler User**: This entity generates Charging Events as the result of a user consuming a service and invokes and interacts with the Charging Enabler.

#### 6.6.3.2.1 Charging OGSA View (Normative)

Figure 18 below gives a graphical overview of the functional entities of the Charging Enabler and the interfaces, which expose Charging functionality followed by a description in Table 13. Please, note that the Charging Enabler User is not shown in this figure.




CH1: Diameter Accounting or Parlay X Web Services Payment API

CH2: Diameter Credit Control or Parlay X Web Services Payment API

**Figure 18: Charging OGSA View**

| Functional entities | Functionality provided | Via interface | Protocol used |
|---|---|---|---|
| Offline Charging | CH-1 is used for offline Charging Event reporting. This interface supports the following functions:<br>• The sending of Charging Events after service delivery<br>• The sending of interim Charging Events during service delivery<br>• Charging Correlation<br><br>This interface is exposed by the charging Enabler to any authorized Offline Charging requestor (authorized Charging Enabler User) | CH-1 | Diameter Accounting,<br><br>Parlay X Web Services Payment API (only event based charging) |
| Online Charging | CH-2 is used for online charging. This interface supports the following functions:<br>• Quota requests<br>• Renewed quota requests<br>• Reporting of portion of unused quota<br>• Rating<br>• Credit checking<br>• Correlation<br>• Refunding facility.<br><br>This interface is exposed by the charging Enabler to any authorized Online Charging requestor (authorized Charging Enabler User) | CH-2 | Diameter Credit Control,<br><br>Parlay X Web Services Payment API |

**Table 13: Interfaces exposing Charging functionality**

#### 6.6.3.3 CBCS Enabler V1_0

The OGSA View for CBCS is based on the following specific document [OMA-CBCS-AD].

The CBCS Enabler screens Content before delivering it to the user, based on Content Categories. The CBCS Enabler can be applied to any Content regardless of the Enabler or protocol that is used to deliver the Content.

A Content Category qualifies the Content according to a categorization scheme. The CBCS Enabler can obtain the Content Category for a given piece of Content from a Categorization Entity, from categorization meta-data in the Content itself, or by analyzing the Content.

The CBCS Enabler consists of two independent functional entities:

**Content Categorization Component:**
This entity provides following features:

- Maps Content or Content References to a set of categories
- Management of Content Categorization Rules
- Management of associations between Content References and Content Categories

**Content Screening Component:**
This entity provides following features:

- Identifies the Screening Rules associated with the incoming request for screening
- Identifies of the submitted Content and any other parameters
- Processes the Screening Rules to determine whether the Content should be categorized, modified in any way and delivered.
- Management of Screening Rules

The standardization of Content categorization schemes, Content Categories, CBCS User Profiles, Screening Rules and other Content related information, is outside the scope of the CBCS Enabler specification.

#### 6.6.3.3.1 CBCS OGSA View (Normative)

Figure 19 below gives a graphical overview of the functional entities of the CBCS Enabler and the interfaces, which expose CBCS functionality, followed by a description in Table 14.

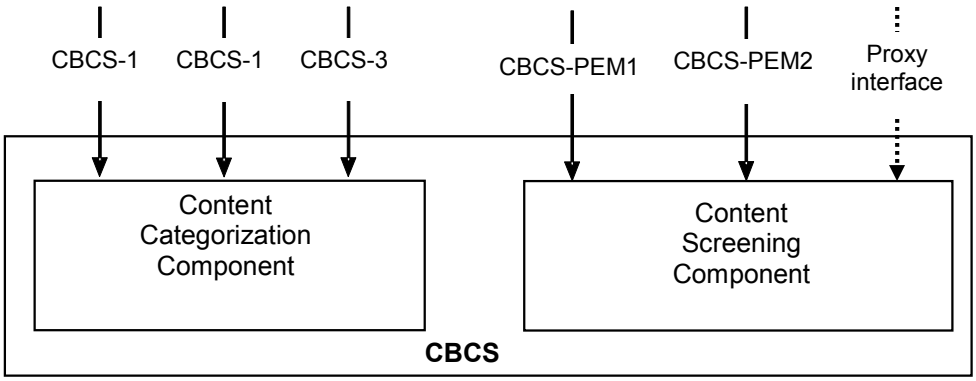



**Figure 19: CBCS OGSA View**

| Functional entities | Functionality provided | Via interface | Protocol used |
|---|---|---|---|
| Content Screening Component | While CBCS can be deployed in proxy pattern, a proxy interface is not specified by CBCS; this is because specifying such an interface depends on the protocols being proxied (e.g. Browsing, HTTP, Messaging, etc), which is out of scope for CBCS. | Proxy Interface | Not specified |
| | The CBCS interface to invoke the processing of Screening Rules is derived from CBCS.PEM-1. It is used to perform Content Screening in the callable usage pattern.<br>Input parameters in the request may include:<br>• Identification of the target principal for Content,<br>• Content or a Content reference (e.g., URI),<br>• Other information (e.g., Content metadata and categorization information)<br>• Content source (e.g. URI) and associated information<br>Output parameters in the response may include:<br>• The decision resulting from the processing of the screening rules<br>• Additional explanatory information related to the decision | CBCS.PEM-1 | Diameter or SOAP |
| | The CBCS management interface is derived from CBCS.PEM-2. It is used to create, delete, modify and view Screening Rules. | CBCS.PEM-2 | XCAP |

| Functional entities | Functionality provided | Via interface | Protocol used |
|---|---|---|---|
| Content Categorization Component | Using this interface a Resource may obtain the Content Category (or Categories) for given Content.<br>Input parameters in the request may include:<br>• the Content itself or a Content reference (e.g. URI)<br>• Content related information (e.g. Content metadata and categorization information)<br>• Content source (e.g. URI) and associated information.<br>• A request identifier.<br>Output parameters in the response may include:<br>• A set of Content Categories (i.e. zero or more)<br>• Metadata associated with the Content Categories<br>• The request identifier of the request to which this is the response. | CBCS-1 | ICAP |
| | The CBCS-2 interface is used to create, delete, modify and view Content Categorization Rules. | CBCS-2 | XCAP |
| | The CBCS-3 interface is used to associate (create, delete, modify and view) Content references (e.g., URIs or the Content itself) with Content Categories. | CBCS-3 | ICAP |

**Table 14: Interfaces exposing CBCS functionality**

#### 6.6.3.4 GPM Enabler V1_0

The OGSA View for GPM is based on the following specific document [OMA-DCD-AD].

The Global Permissions Management enabler provides generic permissions checking and permissions management, which can be used by other resources (e.g. OMA service enablers). The GPM enabler consists of a single functional entity: P**ermissions Checking and Management Component**.

This entity provides the following features:

- **Processes the Permissions Rules**, i.e. goes through the following steps:
    - Identifies the Permissions Rules associated with the Permissions Checking Request as part of the permission rule processing
    - Evaluates and Processes Permissions Rules using input arguments received from a Permissions Checking Requester (a resource that issues a Permissions Checking Request to GPM enabler) and additional information which it may acquire from other resources. As part of the processing, there could be an action to ASK (Ask for consent from Ask Target) – an action that the GPM enabler would complete prior to returning the decision to the Permissions Checking Requester.
    - Determines the decisions to return to the Permissions Checking Requester
    - Returns to the Permissions Checking Requester a decision to:
        - GRANT (grant permission to release (a subset of) the Target Attribute(s)) or
        - DENY (deny permission to release Target Attribute(s))

- **Provides the Permissions Rules management functions** to a Management Requester - a resource that issues a request for performing functions such as:
    - creating, reading, deleting, modifying of Permissions Rules
    - associating/disassociating permission rules with attributes, application feature sets, Permissions Targets

#### 6.6.3.4.1 GPM OGSA View (Normative)

Figure 20 below gives a graphical overview of the functional entities of the GPM Enabler and the interfaces, which expose GPM functionality, followed by a description in Table 15.

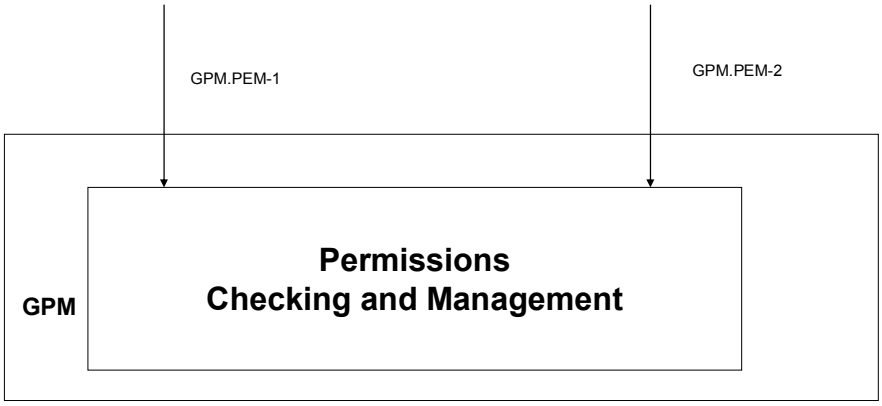



**Figure 20: GPM OGSA View**

| Functional entities | Functionality provided | Via interface | Protocol used |
|---|---|---|---|
| Permissions Checking and Management | This GPM interface exposes the permissions checking functionality and is derived from PEM-1.<br>• Input parameters in the Permission Checking request<br>1. Must include all arguments required in the evaluation of the Permissions Rules<br>1. Permissions Target identity,<br>2. Requested Permission Target Attributes,<br>3. Permission Requester identity<br>4. Target Attribute Consumer<br>2. May include<br>1. The intended use of the Target Attributes (i.e. use that will be made of this information by the application, e.g. to access and modify a Target Attribute, or sharing medical data with doctors but not students)<br>2. User profile information, application specific data, and other relevant GPM Context information (e.g. time of day, number of requests per unit time or other information coming from OMA enablers)<br>• Output parameters in the Permission Checking response<br>3. Must include<br>1. decision rendered by the evaluation of Permissions Rules for each attribute<br>4. May include<br>1. If DENY Reason of the decision | GPM.PEM-1 | Diameter or SOAP |
| | This GPM interface exposes the permissions rules management functionality and is derived from PEM-2. It is used to create, read, delete, read, and modify Permission Rules. | GPM.PEM-2 | XCAP |

**Table 15 : Interfaces exposing GPM functionality**

### 6.6.3.5 GSSM Enabler V1_0

The OGSA View for GSSM is based on the following specific document [OMA-DCD-AD].

The GSSM enabler allows an authorized principal to setup, terminate, change, query subscriptions by actions such as subscribing and unsubscribing to services, registering authorized user(s) for using the service, and setting subscription preferences and/or service usage constraints for associated users(s). The GSSM enabler consists of the following functional entities:

- **Subscription Validation Component**:

- Provides subscription validation function (to check if the service subscription is valid) to the Subscription Validation Requestor. Provides validation criteria management function to the Validation Criteria Management Requestor;

- **Subscription Profile Component:**
  - Provides data access functions (i.e. only read) for subscription profile data
- **Subscription Management Component:**
  - Performs subscription management operations (e.g. subscribing to a service, unsubscribing from a service, change an existing subscription).

#### 6.6.3.5.1 GSSM OGSA View (Normative)

Figure 21: GSSM OGSA View below gives a graphical overview of the functional entities of the GSSM Enabler and the interfaces, which expose GSSM functionality, followed by a description in Table 16.

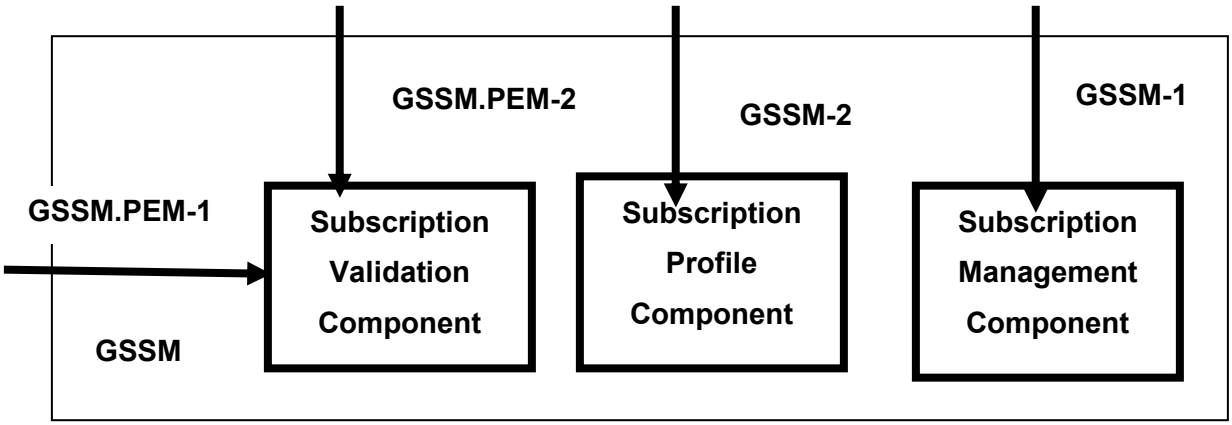



**Figure 21: GSSM OGSA View**

| Functional entities | Functionality provided | Via interface | Protocol used |
|---|---|---|---|
| Subscription Validation Component | The GSSM subscription validation interface is derived from PEM-1. It is used to perform subscription validation in the callable usage pattern. | GSSM.PEM-1 | Diameter or SOAP |
| | This interface is derived from PEM-2 and allows Validation Criteria Management Requestor to manage Validation Criteria, i.e. create, read, delete and modify Validation Criteria. | GSSM.PEM-2 | XCAP |
| Subscription Profile Component | This interface allows read access to subscription profiles (e.g. subscription status) in ways that are data-type independent | GSSM-2 | |
| Subscription Management Component | GSSM subscription management interface that provides subscription management functions | GSSM-1 | |

**Table 16: Interfaces exposing GSSM functionality**

### 6.6.3.6 PUSH Enabler V2_2

The OGSA View for PUSH is based on the following specific document [OMA-DCD-AD].

The PUSH Enabler enables a service to push content to mobile devices.

The PUSH enabler consists of the following two functional entities:

- The Push Proxy Gateway (*PPG*) is the entity that does most of the work in the Push framework. Its responsibilities include acting as an access point for content pushes from Push Intiators to Push Clients, and everything associated therewith (authentication, address resolution, etc).
- The Push Client is the entity that receives Push content from the PPG. Its responsibilities include acting as a service access point for OMA enabler user agents or applications that directly use Push services.

#### 6.6.3.6.1 PUSH OGSA View (Normative)

Figure 22: PUSH OGSA View below gives a graphical overview of the functional entities of the PUSH Enabler and the interfaces, which expose PUSH functionality followed by a description in Table 17: Interfaces exposing PUSH functionality.

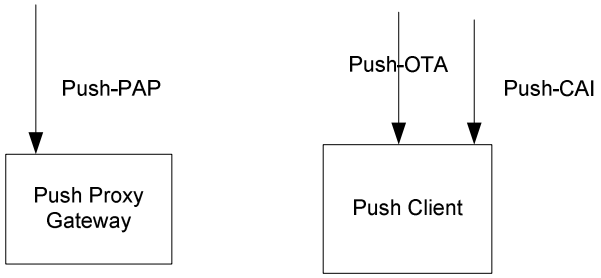



**Figure 22: PUSH OGSA View**

| Functional entities | Functionality provided | Via interface | Protocol used |
|---|---|---|---|
| PUSH Client | The interface, via which the PPG and Push Client interact using one of the Push-OTA protocol variants | Push-OTA | |
| | The interface, via which the Push Client exposes Push services to Push-enabled applications | Push-CAI | |
| Push Proxy Gateway | The interface, via which the PPG exposes Push services to the Push Initiator | Push-PAP | |

**Table 17: Interfaces exposing PUSH functionality**

### 6.6.3.7 CMI Enabler V1_0

The OGSA View for CMI is based on the following specific document [OMA-DCD-AD].

The CMI Enabler provides mechanisms for the management of content by Content Providers and Service Providers. The CMI enabler consists of the following two functional entities:

The CMC (Content Management Component) provides the following high level functional capabilities:

- New content and associated metadata upload
- Processing of uploaded content and metadata. Processing can include validation of content.
- Update of previously uploaded content and associated metadata
- Removal of content and associated metadata
- Management of content status, e.g. availability for use in services
- Management of content items individually or in bulk (multiple content items).
- Content upload from CMI Component to CMI interface-using entity, e.g. for user-generated content (this functionality is deferred for future version).

The BPC (Business Process Component) provides the following high level functional capabilities:

- SLA establishment;
- CMI enabler policy enforcement, e.g. CMI interface security requirements, limitations on CMI interface operation rates;
- Service discovery and/or notifications of available features related to CMI content;
- Content item purchase operations;
- Delivery of reports related to content, e.g. purchase, usage, upload, either on-demand (synchronous) or on a triggered/scheduled basis (asynchronous);

#### 6.6.3.7.1 CMI OGSA View (Normative)

Figure 23: CMI OGSA View below gives a graphical overview of the functional entities of the CMI Enabler and the interfaces, which expose CMI functionality followed by a description in Table 18: Interfaces exposing CMI functionality.

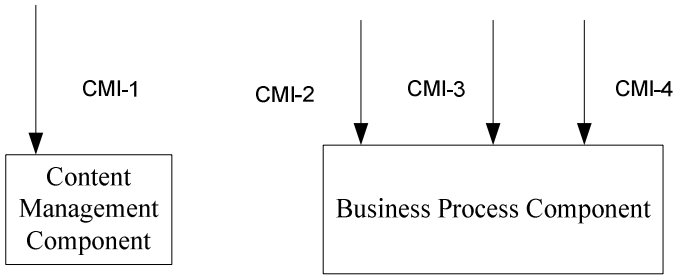



**Figure 23: CMI OGSA View**

| Functional entities | Functionality provided | Via interface | Protocol used |
|---|---|---|---|
| BPC | The interface is exposed by the Business Process Component (BPC) and provides establishment and management of operations in support of specific services. | CMI-2 | |
| | Interface is exposed by the Business Process Component and provides user access control functionalities. Some of these capabilities are related to a specific content item or a collection of content items for a particular user. | CMI-3 | |
| | The interface is exposed by the CMI Component and provides the following functionalities:<br>• Delivery of content usage reports, including any metrics about CMI, e.g. interaction time | CMI-4 | |
| CMC | Interface is exposed by the Content Management Component (CMC) to support upload and management of content and its associated metadata. Metadata in the CMI context is any information about the content (e.g. who created the content, what category it belongs to, etc.). | CMI-1 | |

**Table 18: Interfaces exposing CMI functionality**

### 6.6.3.8 PAL Enabler V1_0

The OGSA View for PAL is based on the following specific document [OMA-XDM_AD].

The PAL Enabler provides a series of interfaces for accessing and making use of presence information on behalf of one or more interested individuals or entities. Access to presence information on behalf of an observer is based on a contextually aware perspective or view. The presence view/perspective is resolved by the PAL Enabler relative to a presence capable application or service and potentially other factors including a requestor identity.

The PAL Enabler consists of the following functional entities

- PAL Client supports the following functions:
  - Requests to receive Presence Context;
  - Requests to receive Presence Aspects relative to a specified Presence Context ;
  - Requests to suspend or resume delivery of Presence Aspect notifications associated with a Presence Context; and,
  - Receives a pre-defined action as a result of a detected value change corresponding to a Presence Trigger.
- PAL Server provides support the following functions:
  - Authorizes requesting PAL Clients;
  - Evaluates and applies policy to support the consolidation of Presence Information by a PAL Server, on behalf of a PAL Client;
  - Establishes and reports Presence Context based on Presence Aware Services, on behalf of PAL Clients;
  - Subscribes to receive Presence Information as a Watcher or Watcher Information Subscriber;
  - Functions as an HSA in the context of the PAL Enabler;
  - Manipulates (i.e. retrieves, forwards, and/or shares) PAL Profiles as an XDM Agent;
  - Subscribes to receive notification of changes to PAL Profiles, as an XDM Agent;
  - Provides views of Presence Information utilizing Presence Aspects for PAL Clients, based on interoperable rules associated with an applicable Presence Context;

- Monitors, and detects Presence Aspect value changes associated with an applicable Presence Context, and executes predefined actions corresponding to a Presence Trigger; and,
- Accepts requests for suspending or resuming the delivery of Presence Aspects associated with a Presence Context (i.e. suspending or resuming notifications corresponding to Presence Triggers applicable to a given Presence Context).

#### 6.6.3.8.1 PAL OGSA View (Normative)

Figure 24: PAL OGSA View below gives a graphical overview of the functional entities of the PAL Enabler and the interfaces, which expose PAL functionality, followed by a description in Table 19: Interfaces exposing PAL functionality.

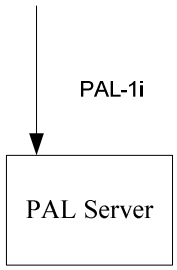



**Figure 24: PAL OGSA View**

| Functional entities | Functionality provided | Via interface | Protocol used |
|---|---|---|---|

**Table 19: Interfaces exposing PAL functionality**

### 6.6.3.9 SEC_CF Enabler V1_1

The OGSA View for Security Common Functions is based on the following specific document [OMA-PEEM_AD].

SEC_CF aims to provide security functionality for OMA Enablers.

SEC_CF defines functional entities such as security gateways and key management centres that can be integrated into other OMA functional entities.

#### 6.6.3.9.1 SEC_CF OGSA View (Normative)

Figure 25: SEC CF OGSA View below gives a graphical overview of the functional entities of the SEC-CF Enabler and the interfaces, which expose SEC_CF functionality, followed by a description in Table 20: Interfaces exposing SEC-CF functionality.

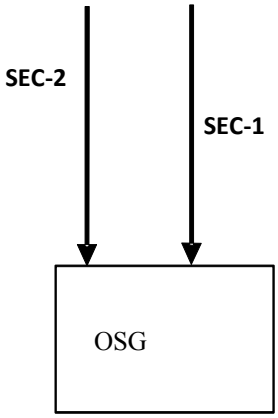



**Figure 25: SEC CF OGSA View**

| Functional entities | Functionality provided | Via interface | Protocol used |
|---|---|---|---|
| OSG | Security services for this interface are implemented at the transport and application layers | SEC-1 | TLS<br>HTTP Digest<br>PSK-TLS<br>DTLS or IPSec<br>Open-ID |
| | This interface can be used for distributed enabler deployments where the security agent connects to a requesting resource in a visited domain via the home OSG | SEC-2 | TLS<br>IPSec |

**Table 20: Interfaces exposing SEC-CF functionality**

### 6.6.3.10 CAB Enabler V1_0

The OGSA View for CAB is based on the following specific document [OMA-PEEM_AD].

CAB enabler provides the following functions:

- Address Book Synchronization Function
- Contact Status Function
- Contact Subscription Function
- CAB Interworking Function
- Contact Share Function

#### 6.6.3.10.1 CAB OGSA View (Normative)

Figure 26: CAB OGSA View below gives a graphical overview of the functional entities of the CAB Enabler and the interfaces, which expose CAB functionality, followed by a description in Table 21: Interfaces exposing CAB functionality.

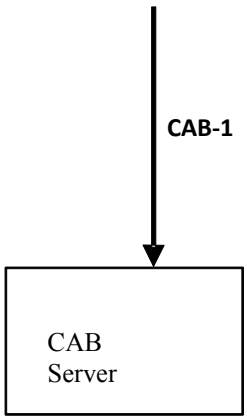



**Figure 26: CAB OGSA View**

| Functional entities | Functionality provided | Via interface | Protocol used |
|---|---|---|---|
| CAB Server | Supported functionalities exposed by this interface include:<br>• CAB data synchronization requests and responses;<br>Request and receive CAB server information such as CAB Server credentials | CAB-1 | DS |

**Table 21: Interfaces exposing CAB functionality**

# Appendix A. Change History

## A.1 Approved Version 1.1 History

| Reference | Date | Description |
|---|---|---|
| OMA-OD-Global_Service_Architecture-V1_1-20110301-A | 01 Mar 2011 | Status changed to Approved by TP:<br>OMA-TP-2011-0077-INP_OGSA_V1_1_RRP_for_Final_Approval |

# Appendix B. Enablers not included in this release

OGSA Suites only include current, normative OMA Enabler Releases. For this reason, White Papers, Historic Enabler Releases, Data Schemas and Releases that contain only Requirements for which neither Architecture nor Technical Specification exists are not included in OGSA Suites.

The following releases have not been included in OGSA Suites as they fall in one of the categories above:

- Games Services [OMA-GS_AD] (Historic Release)
- Charging Data [OMA-CHRG_Data] (Data Schema)
- Charging Worksplit Whitepaper [OMA-CHWS] (White Paper)
- Identity Management Framework [OMA-IdM_RD] (Requirements Only)
- IMPS V1.3 Implementation Guidelines [OMA-IMPS_WP] (White Paper)
- In-Game Communications [OMA-IGC_RD] (Requirements Only)
- Location [OMA-LOC_RD] (Requirements Only)
- Messaging Services Interworking [OMA-MSI_WP] (White Paper)
- Mobile Domain SMIL [OMA-SMIL_RD] (Requirements Only)
- Mobile Gaming Evolution [OMA-MGE_WP] (White Paper)
- OMA Data Objects [OMA-DO_WP] (White Paper)
- OMA Service Environment [OMA-OSE] (Reference Release that provides an architectural framework for all OMA Enablers, but does not constitute a particular Enabler architecture)
- Open Service Provider Environment [OMA-OSPE_AD] (Reference Release)
- Privacy Requirements for Mobile Services [OMA-PRIV_RD] (Requirements Only)
- WAP Billing Framework [OMA-WAP-BF] (Historic Release)
- White Paper on Provisioning Objects [OMA-AC_MO_WP] (White Paper)
- WAP Proxy-Based Redirect [OMA-WPBR_RD] (Requirements Only)