Architecture Requirements

Approved Version 1.0 – 02 Feb 2007

Open Mobile Alliance

OMA-RD-Architecture-V1_0_2-20070202-A

Contents

Tables

1. Scope (Informative)

This document describes the requirements on the OMA Service Environment [**Error! Reference source not found.**]. The requirements in this document have been gathered from a number of different sources, and amalgamated to a common format. They have not always been designed from use cases formally designed according to the template in this document.

2. References

2.1 Normative References

[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

[LIBERTY] "Liberty Glossary v2.0", Liberty Alliance Project,
URL:http://www.projectliberty.org/

[OMA-DICT] "Dictionary for OMA Specifications", OMA-ORG-Dictionary-V2_5, Open Mobile Alliance
URL:http://www.openmobilealliance.org/

[RFC2828] "Internet Security Glossary". R.Shirey. May, 2000.
URL:http://www.ietf.org/rfc/rfc2828.txt

3. Terminology and Conventions

3.1 Conventions

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

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

3.2 Definitions

Address	For the purposes of this discussion, address refers to a URI
Authentication Assertion	See [LIBERTY].
Circle of Trust	See [LIBERTY].
Component	Hardware or software that is part of a functional unit
De-federate	See [LIBERTY].
Federate	See [LIBERTY].
Function	A specific purpose of an entity, or its characteristic action
Identity	See [LIBERTY].
Identity Provider	See [LIBERTY].
Principal	See [LIBERTY].
Pseudonym	See [LIBERTY].
Service Composability	The capability to assemble enablers or services in various combinations to produce new enablers or services.
Service Life Cycle	The process a service goes through from idea, to creation, to introduction in the service provider environment, to retirement (when a service is removed from the service provider environment).
Service Monitoring	The ability to retrieve information at each component or resource at runtime.
Single Log-Out (SLO)	See [LIBERTY].
Single Sign-On (SSO)	See [LIBERTY].
Trust	The extent to which someone who relies on a system can have confidence that the system meets its specifications, i.e., that the system does what it claims to do and does not perform unwanted functions. [source: RFC2828]

3.3 Abbreviations

O&M	Operations and Management
OMA	Open Mobile Alliance
OSE	OMA Service Environment
QoS	Quality of Service
SLO	Single Log-out
SSO	Single Sign-On
WAP	Wireless Applications Protocol

4. Introduction (Informative)

The OMA Service Environment (OSE) is foreseen to consist of a number of different components, to be outlined in the OMA Service Environment architecture. It will also describe the interfaces to be used between those components. Service enablers developed according to OMA specifications will be required to conform to these specifications (e.g. use interfaces as defined in the specification).

This means that all service enablers defined by OMA (current and future) are in principle system elements of the architecture, according to the definition in the requirements template. Here, we are however constraining ourselves to the systems elements which will have to be defined as part of the OMA Service Environment specification, and these are discussed in section 6.3.

5. Use Cases (Informative)

Not Applicable.

6. Requirements (Normative)

6.1 High-Level Functional Requirements

We recognize some of the requirements in this section are testable and some are measurable. All of the requirements are verifiable.

Label	Description	Release Version
HLF-01	The OMA Service Environment MUST enable deployment and use of OMA service enablers to allow for a wide variety of business models.	OSE V1.0, OSPE V1.0
HLF-02	The OMA Service Environment MUST enable the use and deployment of any service enabler by any authorized actor.	OSE V1.0, OSPE V1.0
HLF-03	The OMA Service Environment MUST facilitate the creation and deployment of services using OMA-defined service enablers	OSPE V1.0
HLF-04	The OMA Service Environment SHOULD enable the definition of components in such a way that functional overlaps between OMA enablers are minimized.	OSE V1.0
HLF-05	The OMA Service Environment MUST provide interfaces towards backend systems (e.g. charging, accounting, payment, provisioning, Operations & Management, etc.).	OSE V1.0, CHARGING V1.0, OSPE V1.0
HLF-06	The OMA Service Environment SHOULD support the integration of service enablers, support systems and/or data sources that are not specified within the OMA.	OSE V1.0
HLF-07	The OMA Service Environment MUST support end user mobility in a multi-domain environment, so that the access to or usage of the service does not appear to be affected.	OSE V1.0, GSSM V1.0
HLF-08	Using components developed according to the OMA Service Environment MUST NOT contradict or prevent any requirements imposed by legislation.	OSE V1.0
HLF-09	The Service Environment MUST provide for extensibility for future service enablers and compatibility between these service enablers.	OSE V1.0
HLF-10	The Service Environment MUST provide for the integration of existing service enablers defined by OMA with each other and with existing systems.	OSE V1.0
HLF-11	The OMA Service Environment MUST identify and define a set of functions that are common to most, if not all, use cases, and the ways these functions can be exposed and shared. Where such functions have been defined all OMA-specified enablers MUST use them.	Future release of OSE
HLF-12	The OMA Service Environment MUST be valid for any kind of service (e.g. messaging, WAP, location, “IN”-like services, corporate services, etc.	OSE V1.0
HLF-13	The OMA Service Environment MUST be suitable for services focused on any kind of users or segments, including pre-paid, post-paid, corporate users, mass market, etc.	GSSM V1.0, CHARGING V1.0
HLF-14	The Service Environment SHOULD enable component reusability.	OSE V1.0
HLF-15	If authorized by a Principal, service enablers, services, service providers or other actors MUST be able to interact with other service enablers, services, or service providers on the behalf of the Principal. For example, the OMA Service Environment MUST support the mechanisms to allow a Principal to delegate consent to an Identity Provider, allowing that Identity Provider to authorize federation of that Principal’s identity at multiple Service Providers.	Future release of OSE
HLF-16	When authorized, Principals MUST be able to set policies (e.g. charging policies and privacy policies) on any request (including discovery).	PEEM V1.0, GPM V1.0

HLF-17	The OMA Service Environment SHOULD support options for handling authentication, charging and/or storage of user profiles.	SEC_CF V1.0, OWSER NI V1.0, CHARGING V1.0, GSSM V1.0, OSPE V1.0
HLF-18	The OMA Service Environment MUST NOT assume network connections are permanent or long-lived.	OSE V1.0

Table 1: High-Level Functional Requirements

6.1.1 Security

Label	Description	Release Version
SEC-01	The OMA Service Environment MUST provide mechanisms for authentication of principals, and authorization of these principals for using resources within and across service provider domains.	SEC_CF V1.0, OWSER NI V1.0, PEEM V1.0
SEC-02	The OMA Service Environment MUST enable a Principal to authorize a service enabler or service provider to execute actions on its behalf.	Future release of OSE
SEC-03	The OMA Service Environment SHOULD NOT disallow different trust models for brokered authentication assertions or for single authentication assertions.	OSE V1.0
SEC-04	The OMA Service Environment MUST allow optimisations if a requestor and responder are in the same domain i.e. trust domain).	OSE V1.0
SEC-05	The OMA Service Environment MUST enable single sign-on and single log-out to span enablers in a single domain or across multiple Service Provider domains. One-time authentication or a SSO MUST remain valid throughout a continuous session	OWSER NI V1.0
SEC-06	The OMA Service Environment MUST support setting various strengths of security policies and SHOULD support a way for service providers to define and communicate authorization policies for enablers.	SEC_CF V1.0
SEC-07	The OMA Service Environment SHOULD support a way to negotiate security settings between service providers.	SEC_CF V1.0
SEC-08	The OMA Service Environment SHOULD provide a set of security functions (including methods and data models), which are common to all enablers and can be re-used by existing enablers and in the design of new enablers.	SEC_CF V1.0
SEC-09	The OMA Service Environment MUST provide secure and confidential access to services and associated exchanges within and across networks and domains e.g. through methods such as encryption, integrity protection, non-repudiation, authentication (both mutual and one-way) and authorization.	SEC_CF V1.0
SEC-10	The OMA Service Environment MUST be able to control access to enablers, irrespective of the network technology and domain of origin of the party attempting to access the enabler.	OSE V1.0 and PEEM V1.0
SEC-11	The OMA Service Environment MUST support a mechanism to federate and de-federate identity information across Service Provider domains.	OWSER 1.x
SEC-12	The OMA Service Environment MUST provide mechanisms that ensure protection against security threats.	SEC_CF V1.0
SEC-13	The OMA Service Environment MUST allow a Service Provider to request authentication confirmation from an Identity Provider either on behalf of itself or other Service Providers.	OWSER NI 1.0
SEC-14	The OMA Service Environment MUST provide an interface to the charging enabler.	CHARGING V1.0

Table 2: High-Level Functional Requirements – Security Items

6.1.2 Charging

Label	Description	Release Version
CH-01	The OMA Service Environment MUST NOT preclude any charging models between different actors.	OSE V1.0

Table 3: High-Level Functional Requirements – Charging Items

6.1.3 Administration and Configuration

Label	Description	Release Version
OAM-01	The OMA Service Environment SHOULD provide for the simplification of the services and service enablers life-cycle management by avoiding manual processes, need of integration due to lack of standards, etc.	**OSPE V1.0**
OAM-02	Subject to authorization by the Service Provider, the OMA Service Environment MUST enable entities (e.g. enterprises) other than the service provider to enable download of applications to devices, manage the application's service life cycle and manage devices according to the OMA Device Management requirements.	DM WSI V1.0
OAM-03	The OMA Service Environment MUST enable the communication of service monitoring data (e.g. performance measurements) between actors.	Future release of OSE
OAM-04	The OMA Service Environment SHOULD enable easy administration and configuration of users and services.	GSSM V1.0, OSPE V1.0
OAM-05	The execution or use of access and authorization functions SHOULD NOT impact the performance of services.	Future release of OSE
OAM-06	The OMA Service Environment SHOULD provide functions for the management of trust between the actors in the OMA environment.	OWSER NI V1.0
OAM-07	The OMA Service Environment MUST provide a mechanism by which device and network information can be communicated to an authorized third-party (with respect to the information holder) in a manageable way. This mechanism MUST allow for the automated discovery of new devices and new characteristics in existing devices.	DM WSI V1.0
OAM-08	The OMA Service Environment MUST provide a mechanism to enable third-parties to obtain an identification for an end-user who uses a particular device to access authorized third-party applications.	OWSER NI V1.0
OAM-09	The OMA Service Environment MUST provide a mechanism to allow third-parties to discover the device(s) currently used by an end-user, if registered on a network (e.g. where to send a notification to the employee).	DM WSI V1.0
OAM-10	The OMA Service Environment MUST provide a mechanism for an authorized third-party to discover the conditions for using a service enabler exposed by a particular service provider in a dynamic manner.	PIOSE V1.0
OAM-11	The OMA Service Environment MUST support a mechanism for service providers and other authorized actors to enforce the conditions for use of a service enabler.	OSE V1.0, PEEM V1.0
OAM-12	The OMA Service Environment MUST have a single logical point that handles subscriber and subscription information.	GSSM V1.0

Table 4: High-Level Functional Requirements – Administration and Configuration Items

6.1.4 Usability

Label	Description	Release Version

USE-01	The OMA Service Environment MUST provide the means to simplify end-user access to and use of a service.	OSE V1.0

Table 5: High-Level Functional Requirements – Usability Items

6.1.5 Interoperability

Label	Description	Release Version
IOP-01	The OMA Service Environment MUST define the data flows and interfaces between applications and enablers, and between enablers. These are the interfaces where interoperability is required.	All ERELDs
IOP-02	The OMA Service Environment MUST NOT mandate any specific deployments.	OSE V1.0
IOP-03	The OMA Service Environment MUST support simplified (e.g., plug-in) and automated integration for enablers with each other.	OSE V1.0
IOP-04	The OMA Service Environment MUST provide common mechanisms for Provisioning of services, service enablers and user parameters	OSPE V1.0 and GSSM V1.0
IOP-05	The OMA Service Environment SHOULD provide a mechanism to manage and use policies (e.g. access policies, charging polices, service level agreements, etc.).	PEEM V1.0

Table 6: High-Level Functional Requirements – Interoperability Items

6.1.6 Privacy

Label	Description	Release Version
PRV-01	The OMA Service Environment MUST provide a means to manage and enforce end-user privacy.	GPM V1.0
PRV-02	The OMA Service Environment MUST support the use of pseudonyms for the communication of Principal's identities between Service Providers (to enable traceability without disclosing the Principal's identity).	OWSER NI V1.0

Table 7: High-Level Functional Requirements – Privacy Items

6.2 High-Level System Requirements

See previous sections.

6.3 System Elements

Label	Description	Release Version
SE-01	The Service Environment SHOULD NOT preclude the deployment of service enablers in high-availability, high-uptime, scalable environments (e.g. By requiring implementation in ways which disable the use of the functions of this environment).	OSE V1.0
SE-02	The Service Environment MUST allow applications to make use of multiple enablers to create services (e.g. service composability).	OSE V1.0
SE-03	The Service Environment SHOULD enable the definition of components in such a way that reuse of components (including specified data formats) is encouraged.	OSE V1.0
SE-04	The Service Environment MUST support the ability to simultaneously operate multiple versions (i.e. multiple instances, defined according to different releases of the OMA specifications) of an interface or API.	OSE V1.0
SE-05	The Service Environment MUST provide mechanisms to control the service quality of resources.	PIOSE V1.0

SE-06	The specification of a Service Enabler MUST be done in such a way that allows for scalable implementations.	All ERELDs

Table 8: High-Level System Requirements - Systems Elements

6.3.1 General requirements on enabler interfaces

Label	Description	Release Version
GEN-01	The interfaces to a Service Enabler MUST NOT constrain the functions of the enabler to a single domain.	OSE V1.0
GEN-02	When a Service Enabler is defined by OMA a standardized interface MUST be defined for the Service Enabler.	OSE V1.0

Table 9: High-Level System Requirements - General Requirements on Enabler Interfaces

6.3.2 Common Directory / Registry

Label	Description	Release Version
CDR-01	The OMA Service Environment MUST have a single logical access point (e.g. Common Directory) to handle user data.	OWSER V1.0, OSPE V1.0

Table 10: High-Level System Requirements - Common Directory/Registry

6.3.2.1 Interfaces to Common Directory / Registry

Label	Description	Release Version
CDI-01	The OMA Service Environment MUST support Service Registration.	OSPE V1.0
CDI-02	The OMA Service Environment MUST support Service Discovery.	GSSM V1.0
CDI-03	The OMA Service Environment MUST support Discovery of an interface of a Service Enabler.	OSPE V1.0
CDI-04	The OMA Service Environment MUST support Registration of an interface of a Service Enabler.	OSPE V1.0
CDI-05	Within the OMA Service Environment it MUST be possible to register, discover, and retrieve information (e.g. a service enabler's address) using a resource identifier (e.g. a user identifier).	OSPE V1.0, GSSM V1.0

Table 11: High-Level System Requirements - Interfaces to Common Directory/Registry

6.3.3 Network interfaces

Label	Description	Release Version
NI-01	The OMA Service Environment MUST define a common interface for the operations and management (O&M) of enabler implementations or applications (including service monitoring and end-to-end service delivery).	Future release of OSE

Table 12: High-Level System Requirements - Network Interfaces

Appendix A. Change History (Informative)

A.1 Approved Version History

Reference	Date	Description
OMA-RD_Architecture_V1_0	21 Oct 2003	Initial document to address the basic starting point Ref TP Doc# OMA-TP-2003-0591-ARCH-RD
OMA-RD-Architecture-V1_0_1	03 Oct 2006	Editorial fixes (2006 template) and Minor CR OMA-ARC-2006-0289R01-CR_Applying_agreed_OSEv2_RD_CRs_to_V1
OMA-RD-Architecture-V1_0_2	06 Dec 2006	Implement: - OMA-ARC-2006-0369-CR_copy_RD_V2_agreed_changes_to_V1 - OMA-ARC-2006-0393-CR_OSEV1_RD_remove_old_reference - OMA-ARC-2006-0407-CR_OSE_V1_RD_changes_to_release_version_column
OMA-RD-Architecture-V1_0_2	02 Feb 2007	Implement: - OMA-REQ-2007-0010-CR_Class_2_Changes_OSE_V1_0_2_RD - Changed relevant occurances of “2006” to “2007”

A.2 Draft/Candidate Version 1.0 History

Document Identifier	Date	Sections	Description
n/a	n/a	n/a	n/a