Utilization of IMS capabilities Architecture

Approved Version 1.0 – 9 Aug 2005

Open Mobile Alliance

OMA-AD-IMS-V1_0-20050809-A

Contents

Figures

Tables

1. Scope (Informative)

Within the framework of the OMA Service Environment (OSE) [OSE], this Architecture Document (AD) identifies a set of capabilities within the IP Multimedia Subsystem (IMS) as defined by 3GPP and 3GPP2 that can be utilized for the OMA service enabler implementations.

The scope of the IMS in OMA AD is to show, for OMA enablers realised on IMS, how they should use IMS and how they should interface with IMS in a consistent way. Furthermore, the AD describes interoperability and/or interworking of OMA enablers realized on IMS with other OMA enablers (either IMS realized or not).

Although targeted at implementers of OMA enablers, the information contained in this AD is also targeted at OMA working groups that are developing service enablers that may be realized using IMS capabilities.

This AD describes how OMA service enabler implementations interface with an underlying IP Multimedia Subsystem (as specified by 3GPP/3GPP2) in order to ensure interoperability.

This document provides guidance and support for the implementation of service enablers utilizing IMS capabilities in order to meet the requirements given in the corresponding Requirements Document, ref. [IMS in OMA RD].

2. References

2.1 Normative References

[IMS in OMA RD]	"Requirements for the utilization of IMS capabilities" OMA-RD_IMSinOMA URL: http://www.openmobilealliance.org
[3GPP TS 23.228]	3GPP TS 23.228, IP Multimedia Subsystem (IMS); Stage 2 URL: http://www.3gpp.org/ftp/Specs/
[3GPP TS 23.141]	3GPP TS 23.141, Presence service; Architecture and functional description; Stage 2 URL: http://www.3gpp.org/ftp/Specs/
[3GPP TS 24.229]	3GPP TS 24.229, IP Multimedia Call Control Protocol based on SIP and SDP; Stage 3 URL: http://www.3gpp.org/ftp/Specs/
[3GPP TS 32.225]	Telecommunication management; Charging management; Charging data description for the IP Multimedia Subsystem (IMS) URL: http://www.3gpp.org/ftp/Specs/
[3GPP TS 32.260]	Telecommunication management; Charging management; IP Multimedia Subsystem (IMS) charging; (Release 6) URL: http://www.3gpp.org/ftp/Specs/
[3GPP2 X.S0013-002]	All-IP Core Network Multimedia Domain, IP Multimedia Subsystem - Stage-2 URL: http://www.3gpp2.org/Public_html/specs/
[3GPP2 X.S0013-004]	3GPP2 X.P0013.4 IP Multimedia Call Control Protocol based on SIP & SDP; Stage-3 URL: http://www.3gpp2.org/Public_html/specs/
[3GPP2 X.P0013.7]	IP Multimedia Subsystem Charging Architecture and Stage-2 Description URL: http://www.3gpp2.org/Public_html/specs/
[RFC2119]	"Key words for use in RFCs to Indicate Requirement Levels". S. Bradner. March 1997. URL:http://www.ietf.org/rfc/rfc2119.txt
[OMADICT]	Open Mobile Alliance Dictionary" OMA-Dictionary-V2_1 URL:http://www.openmobilealliance.org/
[IOPPROC]	"OMA Interoperability Policy and Process", Version 1.1, Open Mobile Alliance™, OMA-IOP-Process-V1_1 URL:http://www.openmobilealliance.org/
[POC RD]	"Push to Talk over Cellular Requirements Version 1.0" OMA-RD-PoC-V1_0 URL:http://www.openmobilealliance.org/
[POC AD]	"Push to Talk over Cellular Requirements Version 1.0" OMA-AD-PoC-V1_0 URL:http://www.openmobilealliance.org/
[PAG RD]	"Presence Requirements Version 1.0" OMA-RD-PAG-V1_0 URL:http://www.openmobilealliance.org/
[PAG AD]	"Stage 2 - Presence using SIMPLE Draft Version 1.0" OMA-AD-PAG-V1_0 URL:http://www.openmobilealliance.org/
[IM RD]	"Instant Messaging Requirements" OMA-RD-IM-V1_0 URL:http://www.openmobilealliance.org/
[IM AD]	"Instant Messaging using SIMPLE-Architecture" OMA-AD-IM_SIMPLE-V1_0 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

[ARCHREVIEW] "OMA Architecture Review process" OMA-ARCH_Review_Process-V1_0_0
URL:http://www.openmobilealliance.org/

[ARCHPRINC] "OMA Architectural principles" OMA-ArchitecturePrinciples-V1_2
URL:http://www.openmobilealliance.org/

2.2 Informative References

[3GPP TS 22.141] 3GPP TS 22.141, Presence service; Stage 1
URL: http://www.3gpp.org/ftp/Specs/

[3GPP TS 22.228] 3GPP TS 22.228, Service requirements for the IP Multimedia Core Network Subsystem; Stage 1
URL: http://www.3gpp.org/ftp/Specs/

[3GPP TS 22.250] 3GPP TS 22.250, IP Multimedia Subsystem (IMS) Group Management; Stage 1
URL: http://www.3gpp.org/ftp/Specs/

[3GPP TS 22.340] 3GPP TS 22.340, IP Multimedia Subsystem (IMS) messaging; Stage 1
URL: http://www.3gpp.org/ftp/Specs/

[3GPP TS 23.002] 3GPP TS 23.002, Network Architecture
URL: http://www.3gpp.org/ftp/Specs/

[3GPP TS 24.141] 3GPP TS 24.141, Presence service using the IP Multimedia (IM) Core Network (CN) Subsystem; Stage 3
URL: http://www.3gpp.org/ftp/Specs/

[3GPP TS 26.236] 3GPP TS 26.236, Packet switched conversational multimedia applications: Transport protocols
URL: http://www.3gpp.org/ftp/Specs/

[3GPP TS 29.328] 3GPP TS 29.328, IP Multimedia (IM) Subsystem Sh interface; Signalling flows and message contents
URL: http://www.3gpp.org/ftp/Specs/

[3GPP TS 29.329] 3GPP TS 29.329, Sh Interface based on the Diameter protocol; Protocol details
URL: http://www.3gpp.org/ftp/Specs/

[3GPP TS 32.200] 3GPP TS 32.200, Telecommunication management; Charging management; Charging principles
URL: http://www.3gpp.org/ftp/Specs/

[3GPP TS 32.240] 3GPP TS 32.240, Charging management; Charging architecture and principles (Release 6)
URL: http://www.3gpp.org/ftp/Specs/

[3GPP TS 32.296] 3GPP TS 32.296, Telecommunication management; Charging management; Online Charging System (OCS): Applications and interfaces (Release 6)
URL: http://www.3gpp.org/ftp/Specs/

[3GPP TS 32.299] 3GPP TS 32.299, Telecommunication management; Charging management; Diameter Charging Application (Release 6)
URL: http://www.3gpp.org/ftp/Specs/

[3GPP TS 33.203] 3GPP TS 33.203, 3G security; Access security for IP-based services
URL: http://www.3gpp.org/ftp/Specs/

[3GPP TS 33.210] 3GPP TS 33.210, 3G Security; Network Domain Security; IP network layer security

[3GPP2 S.R0037-0]	IP Network Architecture Model for cdma2000® Spread Spectrum Systems URL: http://www.3gpp2.org/Public_html/specs/
[3GPP2 X.P0013.0]	Multi-Media Domain Overview URL: http://www.3gpp2.org/Public_html/specs/
[3GPP2 X.S0013-003]	All-IP Core Network Multimedia Domain, IP Multimedia (IMS) session handling; IP Multimedia (IM) call model; Stage 2 URL: http://www.3gpp2.org/Public_html/specs/
[3GPP2 X.S0013-004]	All-IP Core Network Multimedia Domain, IP Multimedia Call Control Protocol based on SIP and SDP; Stage-3 URL: http://www.3gpp2.org/Public_html/specs/
[3GPP2 X.S0013-005]	All-IP Core Network Multimedia Domain, IP Multimedia Subsystem Cx Interface; Signaling flows and message contents URL: http://www.3gpp2.org/Public_html/specs/
[3GPP2 X.S0013-006]	All-IP Core Network Multimedia Domain, Cx Interface based on the Diameter protocol; Protocol details URL: http://www.3gpp2.org/Public_html/specs/
[3GPP2 X.S0013-007]	All-IP Core Network Multimedia Domain, IP Multimedia Subsystem – Charging Architecture URL: http://www.3gpp2.org/Public_html/specs/
[3GPP2 X.S0013-008]	All-IP Core Network Multimedia Domain, IP Mulimedia Subsystem – Accounting Information Flows and Protocol URL: http://www.3gpp2.org/Public_html/specs/ URL: http://www.3gpp.org/ftp/Specs/
[3GPP2 X.S0013-010]	All-IP Core Network Multimedia Domain, IP Mulimedia Subsystem Sh interface; Signaling flows and message contents – Stage 2 URL: http://www.3gpp2.org/Public_html/specs/
[3GPP2 X.S0013-011]	All-IP Core Network Multimedia Domain, Sh interface based on Diameter Protocols, Protocol Details – Stage 3 URL: http://www.3gpp2.org/Public_html/specs/
[TIA-835]	TIA/IS-835, Release C; CDMA200 Wireless IP Network Standard URL: http://www.tiaonline.org/standards/
[OSE]	"OMA Service Environment", OMA-SERVICE_ENVIRONMENT-V1_0 URL:http://www.openmobilealliance.org/
[TIA-41]	TIA/IS-41, Revision D, Cellular Radiotelecommunications Intersystem Operations URL: http://www.tiaonline.org/standards/
[RFC2617]	HTTP Authentication: Basic and Digest Access Authentication URL:http://www.ietf.org/rfc/rfc2617.txt
[RFC 3310]	Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA) URL:http://www.ietf.org/rfc/rfc3310.txt
[RFC 3329]	Security Mechanism Agreement for the Session Initiation Protocol (SIP) URL:http://www.ietf.org/rfc/rfc3329.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

Collaborative Context Model	An extension of the Context Model. It expands on the Context Model by describing the interactions (collaborations) between the entities of this architecture and external entities (e.g. entities in other architectures).
Contextual Item	A logical entity in an architecture
Context Model	A model that identifies all contextual items relevant to understanding architecture.
Interface	See [OMA DICT].
Reference Point	See [OMA DICT].
System	An organized assembly of functional entities designed to perform a specific function or set of functions.
Enabler Implementation	See OMA Service Environment (OSE) [OSE]
IMS Common Capability	The IMS Common Capability that does not interact directly with the upper layer (i.e. service enablers), but provides support to both service capabilities, supporting capabilities. The common capabilities provide capabilities on which the other capabilities are built, e.g. security, authentication.
IMS Resource Capability Layer	The IMS Resource Capability layer provides bearers defined by parameters, and/or mechanisms needed to realise services. These are within networks and under network control.
IMS Service Capabilitiy	The IMS Service Capabilitiy is a capability that provides a service to the upper layer, i.e. OMA Service Enablers. Service capabilities can be used as building blocks for service enablers, and services.
IMS Service Capability Layer	The IMS Service Capability Layer separates applications and content, i.e. commercial services, from underlying networks. It comprises IMS Service Capabilities, IMS Supporting Capabilities and IMS Common Capabilities. The Service Capability Layer provides functionality to get services launched, charged for, and maintained in a secure environment
IMS Supporting Capability	The IMS Supporting Capability provides a capability that is in a supporting role for service capabilities. Supporting capabilities cannot be used to build services directly, but they can provide support for services built on Service Capabilities.
Service Layer	The Service Layer provides the commercial services to end-users, which make use of network functionalities represented by the IMS Service Capability Layer. It comprises platforms on which content and applications can be hosted and executed
Value Added Service (VAS)	A Value Added Service (VAS) is a telecommunication/information service that is offered in addition to and/or in conjunction with a basic telecommunication/data service.

3.3 Abbreviations

AS	Application Server
CCF	Charging Collection Function
CDR	Charging DataRecord
CN	Core Network
CSCF	Call Session Control Function

ECF	Event Charging Function
EI	Enabler Implementation
ESI	Enabler Server Implementation
ETI	Enabler Terminal Implementation
Gm	Interface between a UE and a P-CSCF.
GW	Gateway
HSS	Home Subscriber Server
IM	Instant Messaging
IMS	IP Multimedia Subsystem
ISC	IMS Service Control (Interface between a CSCF and an Application Server)
ISIM	IMS Subscriber Identity Module
Mb	Interface to IPv6 network services
MMD	Multimedia Domain
MSRP	Message Session Relay Protocol
OCS	On-line Charging System
OMA	Open Mobile Alliance
OMA	Open Mobile Alliance
OSA	Open Service Access
OSE	OMA Service Environment
P-CSCF	Proxy-CSCF
PoC	Push to talk over Cellular
QoS	Quality of Service
Rf	Interface between the CCF (Charging Collection Function) and any AS. (Rf is used also elsewhere within IMS.)
Ro	Interface between the Event Charging Function (which is part of the Online Charging System) and the AS (Ro is used also elsewhere within IMS.)
RTP	Real-time Transport Protocol
S-CSCF	Serving-CSCF
Sh	Interface between an AS (SIP-AS or OSA-CSCF) and an HSS.
SIMPLE	SIP for Instant Messaging and Presence Leveraging
SIP	Session Initiation Protocol
UE	User Equipment
UICC	Universal Identity Circuit Card
USIM	Universal Subscriber Identity Module
Ut	Interface between UE and an Application Server
XCAP	XML Configuration Access Protocol
3GPP	3rd Generation Partnership Project
3GPP2	3rd Generation Partnership Project 2

4. Introduction

4.1 General (Informative)

The IP Multimedia Subsystem (IMS) have been developed based on the widespread technical know-how of the cellular industry and internet technology to enable the realization of real-time and non real-time multimedia services in a mobile environment. IMS provides a SIP based architecture that addresses the needs of mobile operators for session management, security, mobility, QoS and charging capabilities. The use of SIP allows the mobile communication services to be combined with services in the Internet in a modular and extensible way. Currently there exists a 3GPP/3GPP2 profile of SIP, but this is interoperable with any other profile of SIP. The differences between the different profiles are only apparent between the IMS network and the IMS mobile equipment. Other interfaces between the IMS network and the service layer are based on a profile of SIP that contains no 3GPP/3GPP2 specific extensions. At the moment there are no other globally standardised SIP architectures. SIP and other protocols used in IMS are specified in IETF, but in general this document does not refer to IETF specifications directly, only to 3GPP/3GPP2 specifications.

This AD describes the use of SIP and the IMS architecture in such a way as to ensure that service enablers based on SIP are developed in an interoperable, interconnectable and consistent manner. OMA's use case and market requirement driven approach complements the standardisation achievements of 3GPP and 3GPP2 on IMS, with additional market input. As the main industry body for the development of mobile service enabler specifications, OMA has the potential to define service enablers that leverage these IMS capabilities in an interoperable and consistent way.

It is important to note that OMA and the mobile communications industry in general gain advantage from the exploitation of the existing IMS capabilities. Among these benefits are:

- The service definition process within OMA is facilitated and accelerated
- Continuity of the specification process from 3GPP/3GPP2 can be maintained by exploiting the already defined IMS architecture and focusing on service enabler specifications.
- Duplication of work between OMA and 3GPP/3GPP2 can be avoided and the same IMS architecture can be adopted.
- Improved communication and information sharing can be achieved between OMA and 3GPP/3GPP2 when the IMS terms, definitions and concepts are the same.
- Maximised reuse of IMS capabilities and network mechanisms can be made to protect the investments and efforts of the cellular industry and to reduce additional costs by leveraging current investments into IMS

For example, a Push-to-Talk service being designed by OMA will be based on SIP. In addition to the use of SIP User Agents and Proxy servers, some auxiliary capabilities are required in order to create a satisfactory service. There are some areas of the IMS architecture that already exist, that should be re-used when designing the Push-to-Talk service, rather than duplicating effort by creating a similar architecture for Push-to-Talk.

Moreover, when implementing other services like Instant Messaging (IM) or Presence besed on SIP, there is the possibility to reuse functionalities defined for other services (eg PoC) and easily integrate all these services.

Therefore, the architecture specified in this AD aims at ensuring the interoperability between OMA service enablers and an underlying IMS network. Furthermore, a consistent use of the IMS architecture when creating services shall be guaranteed.

IMS provides an architectural solution for the usage of SIP in 3GPP and 3GPP2 networks. IMS addresses some specific solutions as defined in section 6. However, these specific solutions can be addressed in other methods depending on the specific needs of the Operator. The decision of the Operator to meet their needs outside of IMS specific solution shall not prevent the Operator from utilizing OMA developed service enablers that use the SIP protocol. When developing OMA service enablers it can be assumed that the underlying network provides the same functionality as IMS. Further, OMA may work on service enablers that take advantage of SIP as a protocol but do not require IMS.

4.2 Target Audience (Informative)

The target audience for this document includes but is not limited to the following:

- The Working Group(s) that will create specifications based on this subject matter
- Working Groups that need to understand the architecture of this subject matter
- Architecture Working Group (e.g. during Architecture Reviews as defined in [ARCHREVIEW], to determine compliance of [ARCHPRINC], etc.)
- Interoperability Working Group (e.g. for early analysis of interoperability requirements)
- Security Working Group

4.3 Split of work on IMS between OMA and 3GPP/ 3GPP2 (Normative)

The split of work between 3GPP, 3GPP2 and OMA is governed by the "Co-operation Framework" between the OMA and these organizations. Inter-organizational cooperation agreements have also been defined for this purpose. This AD defines the work split between OMA and 3GPP/3GPP2 in OSE terms by identifying IMS interfaces as OSE I2 interfaces. The detailed work split SHALL be enabler dependent, and it is not only an architectural but also an inter-organization cooperation issue, as the case of MMS has shown, and therefore out of the scope of this AD.

Fragmentation of specifications SHOULD be avoided by ensuring that details of the SIP signalling protocol related to IMS are kept under the control of 3GPP/3GPP2. Whilst IMS is based on IETF protocols, OMA SHOULD conveys possible new IMS requirements to 3GPP and 3GPP2.

4.4 Use Cases (Informative)

The use cases that apply for this AD are described in the corresponding Requirements document [IMS in OMA RD].

4.5 Requirements (Informative)

This AD is based on the requirements specified in [IMS in OMA RD].

Requirement ID/Number (Section in IMS in OMA RD)	**Phase Met (IMSinOMA AD Implementation Phases)**	**Section(s)**
6.1 #1 Functional split	1.0	5.2, 5.3 and 6.9
6.1 #2 Interfaces	1.0	5.2, 6.5 and 6.9
6.1.1 #3 Security	1.0	6.6, 6.7 and 6.8.5
6.1.2#4 Charging	1.0	6.6, 6.7 and 6.8.4
6.1.3	NA	NA
6.1.4	NA	NA
6.1.5#5 Interoperability: - interface with the IMS	1.0	5.2, 6.5 and 6.9
6.1.5#6 Interoperability: - use IMS capabilities	1.0	6.6, 6.7 and 6.9
6.1.5#7 Interoperability: - exploit IMS resources	1.0	6.8, 6.9
6.1.5#8 Interoperability with non-IMS networks	1.0	5.2, 5.3 and 6.4

Requirement ID/Number (Section in IMS in OMA RD)	Phase Met (IMSinOMA AD Implementation Phases)	Section(s)
6.1.6#9 Privacy	1.0	6.6, 6.7 and 6.8.7
6.1.7#10 Identity	1.0	6.6, 6.7 and 6.8.7
6.1.8#11 Interoperator interconnect	1.0	6.6, 6.7 and 6.8.4
6.2#12 Enabler usage of IMS network capabilities	1.0	6.6, 6.7 and 6.9
6.2#13 Enabler interfaces with IMS	1.0	5.2, 6.5 and 6.9

Table 1: Requirements met by the IMS in OMA Architecture

4.6 Planned Phases (Normative)

The first release of IMS specifications in 3GPP was specified in the 3GPP Release 5. 3GPP2 has also adopted the Release 5 part of their Multimedia Domain (MMD) specifications. IMS has been further enhanced in 3GPP Release 6 to include additional features like e.g. presence and group management.

The first Phase 1.0 of the IMS in OMA architecture SHALL be complient with IMS as specified by 3GPP in 3GPP Rel-5 or Rel-6 and as specified by 3GPP2 in the corresponding releases.

Any later phase of the IMS in OMA architecture is for further study.

5. Context Model

This chapter specifies how IMS is related to OSE and how IMS fits into the OSE context and how OMA enablers shall interface with IMS within the contex of OSE.

5.1 OSE and IMS (Informative)

5.1.1 The OMA Service Environment (OSE)

The OSE Context as specified by OMA, ref. [OSE], is a conceptual and structured environment that includes OMA enablers, interfaces to applications that make use of OMA enablers, interfaces to Service Providers' Execution Environment (e.g. software life cycle management) and the interfaces to invoke and use underlying capabilities and resources for enabler implementations. The use of IMS capabilities as one such a group of resources and capabilities is described in this document.

5.1.2 The IP Multimedia Subsystem (IMS/MMD)

The IP Multimedia Subsystem (IMS) is a Session Initiation Protocol (SIP) based IP multimedia infrastructure that provides a complete architecture and framework for providing multimedia services. This includes but is not limitd to security functions (e.g. authentication, authorization), routing, charging, and default codecs. Thus, IMS provides a platform for globally interoperable IP multimedia services - especially in the mobile environment.

5.1.3 IMS in OSE

The IMS Service Provisioning Architecture standardized by 3GPP/3GPP2, allows applications, i.e. commercial services, to access capabilities of the IMS. It comprises options for service provisioning, namely SIP-Application Server and OSA Gateway. IMS provides service-enabling functions and IP transport and is therefore relevant to the OMA Service Environment (OSE), which is being developed by OMA.

Applications may use OMA enablers or may use IMS functions directly or both. The OSE does not consider applications that use IMS directly. However, such applications, like any others, can also use the capabilities of OSE.

In the OSE, OMA enabler implementations may make use of IMS capabilities, e.g. charging, authentication, service management, etc. IMS related applications/enablers can use OSE capabilities in addition to IMS capabilities.

5.2 Context Diagram (Normative)

Figure 5.1 shows the conceptual OSE architecture including its three categories of interfaces, I0, I1 and I2 [OSE]. It further depicts the IMS interfaces (as well as non-IMS) in the context of OSE I2 interface category.

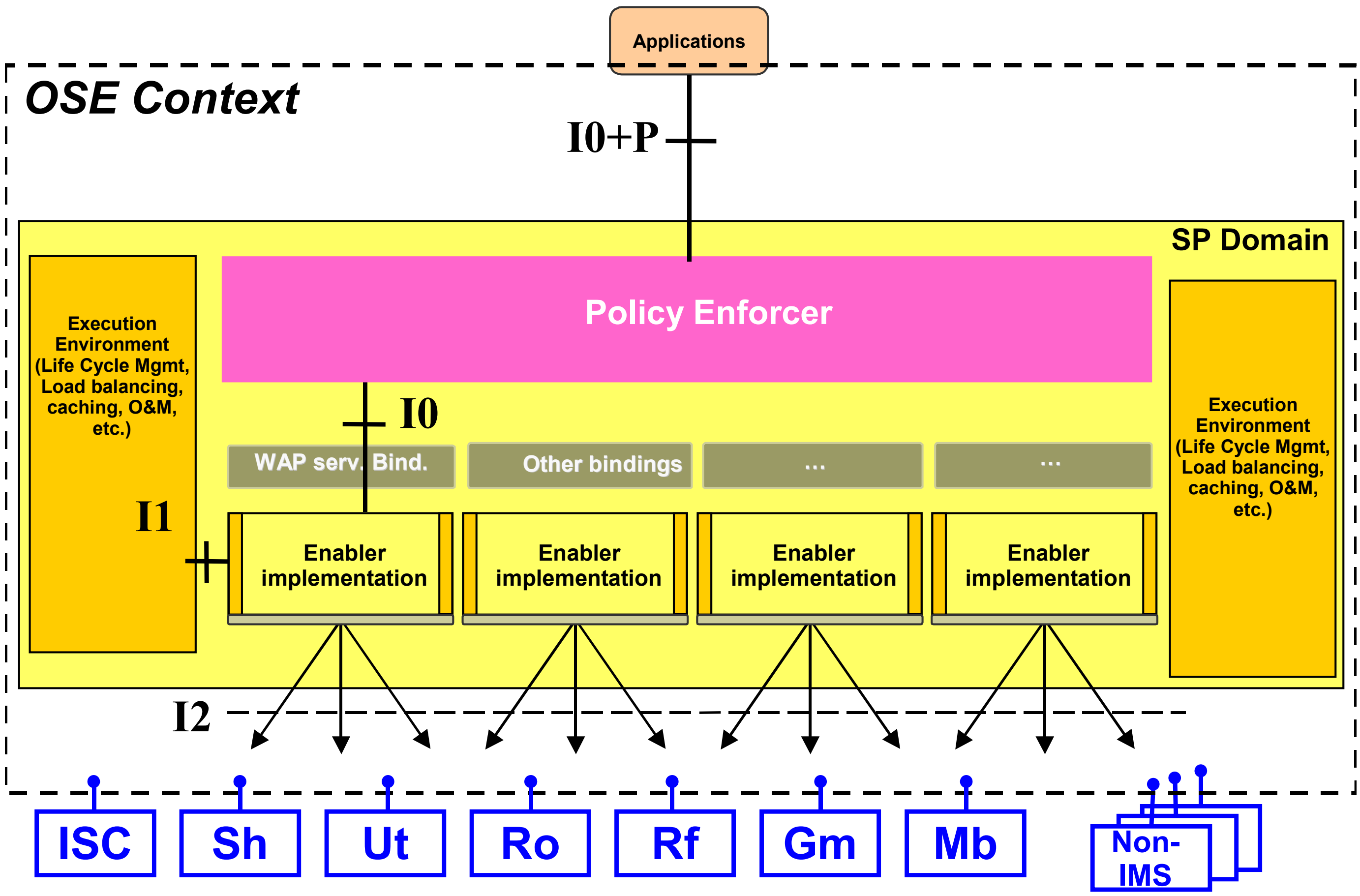

Figure 5.1 IMS interfaces in the context of OSE

The OMA Service Environment in Figure 5.1 contains enablers, which are used by applications using the I0 and I0+p interfaces. The enablers are connected via the I1 interface to the Service Provider Execution Environment (e.g. software life cycle management) and via the I2 interfaces to underlying resources and capabilities, e.g., IMS or non-IMS networks. The set of IMS interfaces that correspond to I2 are described in chapter 6. The I2 type of interfaces to the IMS as shown in the figure represent a wide variety of functionalities and capabilities that are standardized by 3GPP and 3GPP2.

The only IMS interfaces an OMA enabler MAY use are the following: ISC, Sh, Ut, Ro, Rf, Gm and Mb. The interfaces are further described in chapter 6.

5.3 OSE and IMS services (Normative)

Figure 5.1 above shows IMS and its standardized interfaces in the context of OSE. In addition, it should be noted that 3GPP/3GGP2 have standardised IMS services that also work on top of the IMS core. Several of these IMS services are currently being integrated in the OMA framework, like presence and messaging, while others do not have a corresponding OMA enabler so far, like conferencing. Figure 5.2 shows IMS services that are on the same enabler level as the OMA enablers and connected to the IMS core network using IMS interfaces standardised in 3GPP/3GPP2. Some applications or non-OMA enablers may use IMS capabilities and interfaces directly, but such IMS usage is out of the scope of OMA.

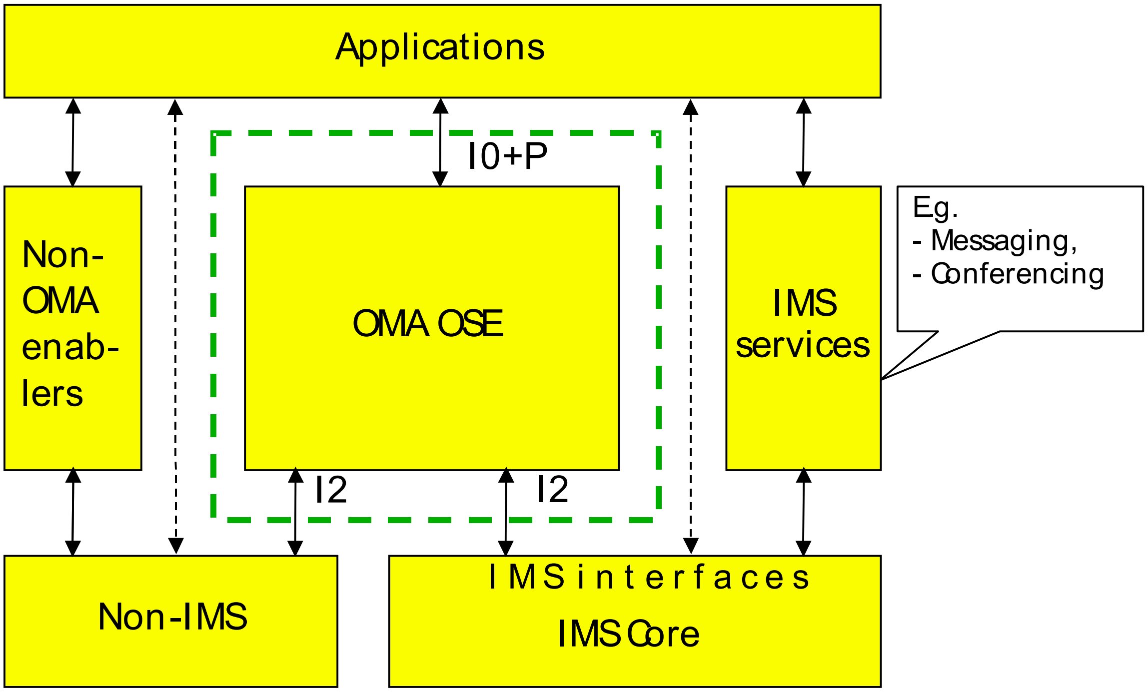

Figure 5.2; OSE and 3GPP/3GPP2 IMS services

The IMS services have been suitable candidates for OMA enablers, in order to provide capabilities that are not in the set of existing OMA enablers. One part of the development work to integrate IMS service capabilities in OSE is to identify or develop I0 type of interfaces for these services/enablers, where applicable and when necessary. The IMS services of course already support interfaces with the IMS core.

As an example it is noted that currently there is no OMA enabler for the IMS conferencing capability, but in principle e.g. an OMA conference enabler could adopt the IMS conference service as an OMA enabler. Figure 5.3 shows the relationship between such a hyphothetical "Conference enabler", linked to other OMA enablers via I0 type of interfaces and to the IMS core network via I2 type of interfaces.

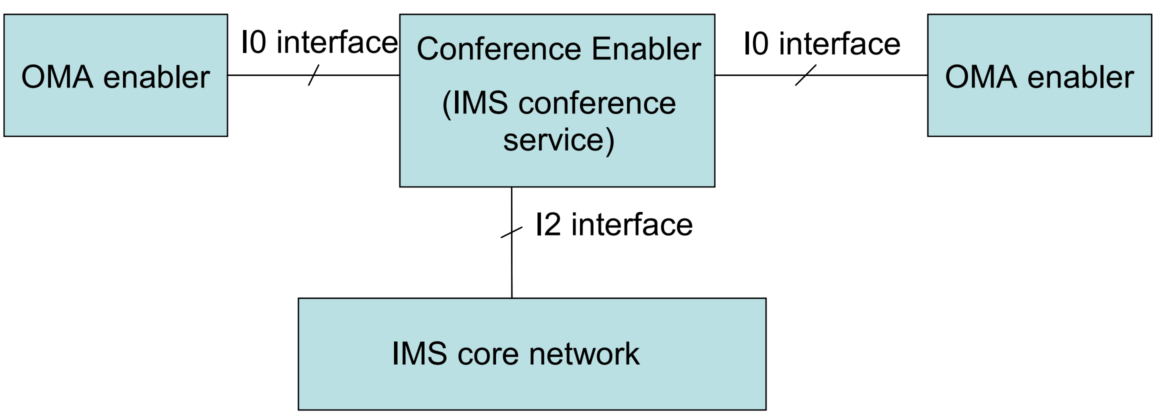

Figure 5.3; Example of a possible "Conference enabler" reusing the IMS conference service

For example, an OMA game enabler may use the OMA conference enabler (via an I0 interface) in order to establish a multi-party game session.

It is not in the scope of this AD to identify or define IMS services to become OMA enablers– the way to develop new OMA enablers is to follow the usual OMA process – first agree a work item and identify a working group to work on the specification of the enabler and so on. However, those IMS resources (services and capabilities) that are identified in this AD and are usable in the OSE SHALL be used by OMA working groups developing new OMA enabler specifications. The IMS resources are accessed by OMA enablers via the I2 interface that is further clarified below.

5.4 Clarification of I0 and I2 interfaces in OSE and IMS (Normative)

It is a basic assumption that IMS is an underlying 'SIP control' network defined outside OMA. From OMA point of view IMS looks simply like a set of 'assumptions'. For instance, if an OMA enabler (e.g. PoC server) is connected to an 3GPP/3GPP2 IMS core network, then the enabler SHALL assume that certain capabilities will be provided by the underlying 3GPP/3GPP2 IMS core network, e.g:

charging

authentication

compression

routing

Therefore these capabilities do not need to be worked on by OMA. Each OMA enabler SHALL assume that they are present in the underlying IMS core network.

If one OMA enabler wishes to talk to another OMA enabler using SIP then, as far as OMA specifications are concerned, it does so by relying on the routing capability of the underlying 3GPP/3GPP2 IMS core network. The OMA enabler simply routes a SIP request to the 3GPP/3GPP2 IMS core network, which routes it towards the correct OMA enabler.

The routing capability is therefore provided by an I2 type of interface, as shown in Figure 5.4. Logically however, according to the OSE model, the OMA enablers are talking SIP to each other across an I0 interface. When the OMA enablers happen to run on top of IMS, they may actually use I2 interfaces to realise that I0 interface (see the blue arrows in fig. 5.4). OMA enablers using SIP need an underlying mechanism to transport SIP and provide other capabilities. IMS is one way to provide this and it does so using I2 type of interfaces.

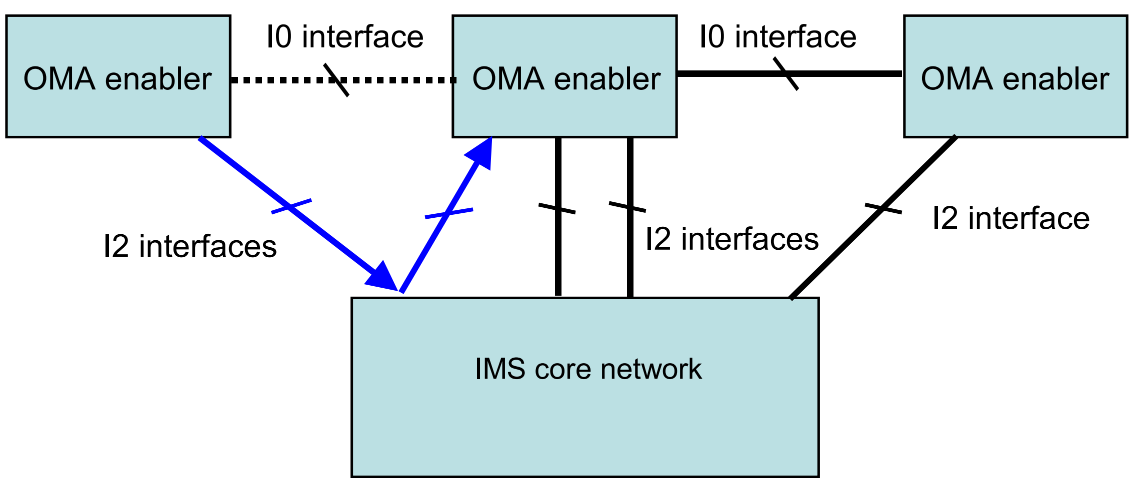

Figure 5.4: OMA Enablers communicationg with each other via the 3GPP/3GPP2 IMS core network

The advantage of this situation is that for each SIP-based OMA enabler, OMA can specify the service-specific details of the OMA enabler without having to think about the common capabilities. For example, if PoC requires routing or compression/decompression of signalling messages, the PoC server itself doesn't have to do this, but can depend on the IMS Core to do it. Also any future OMA enabler can rely on the compression capability of the 3GPP/3GPP2 IMS core network in a similar way.

So OMA concentrates on what it is supposed to provide and does not have to concern itself with the underlying network.

This AD describes what capabilities are provided by the 3GPP/3GPP2 IMS core network and what the OMA enablers need to implement in order to consistently use those capabilities. The 3GPP/3GPP2 IMS core capabilities SHALL be provided via I2 type of interfaces, which are specified as normative IMS interfaces that offer a standard way to use IMS in OMA when so desired.

5.5 Context Collaboration Model (Normative)

The enabler’s usage of IMS interfaces SHALL be specified by OMA, but the actual protocols of the interfaces are under the responsibility of 3GPP/3GPP2.

6. Architectural Model

6.1 Introduction (Informative)

The IP Multimedia Subsystem (IMS) is a Session Initiation Protocol (SIP) based IP multimedia infrastructure that provides a fully standardized complete architecture and framework for providing multimedia services. IMS provides the architecture for the usage of SIP, rather than something different from IETF SIP. In addition to this the IMS architecture is not limited to SIP based interfaces, but it also addresses additional functionalities that complete the necessary requirements for service delivery e.g. bearer control, security and charging issues by defining the IMS charging framework with complete protocol set and interfaces. Even though the IMS Service Provisioning Architecture is designed and optimized for the 3GPP/3GPP2 mobile environment, it is the only generally standardized SIP platform to build services on.

The first release of IMS specifications was defined in the 3GPP Release 5; see ref. [3GPP TS23.002, Rel-5] and ref. [3GPP TS 23.228, Rel-5]. 3GPP2 has also adopted the Release 5 as part of their Multimedia Domain (MMD) specifications, see ref. [3GGP2 X.P0013.0] and ref. [3GPP2 X.P0013.2]. 3GPP2 MMD comprises the IMS and the core network packet data subsystem, which in the 3GPP terms would mean the IMS and the packet switched domain. 3GPP have developed enhancements to IMS/MMD, which are specified in the 3GPP Release 6 set of specifications.

The OMA Service Environment (OSE), which is being established by OMA, allows commercial services to be built using OMA enablers. The general relations between OSE and IMS are described in chapter 5.

IMS contains network capability providing IP transport and IMS is also a source of service enabling functions. OMA service enablers are not end-to-end services, but capabilities that value added services are built on[1]. Therefore, the capability and resources that IMS offers to build value added services could be logically integrated in the OMA service environment.

6.2 IMS Architecture model supporting OSE (Normative)

The main components of the IMS architecture in relation to enablers are depicted in figure 6-1 together with the interfaces between IMS and the enabler implementations in the terminal and in the network. The IMS interfaces are described in chapter 6.4 and the functionalities of the main IMS elements in the figure are described in chapter 6.8.

[1] A value added service (VAS) provider (VASP) could be a network operator or a 3rd party service provider.

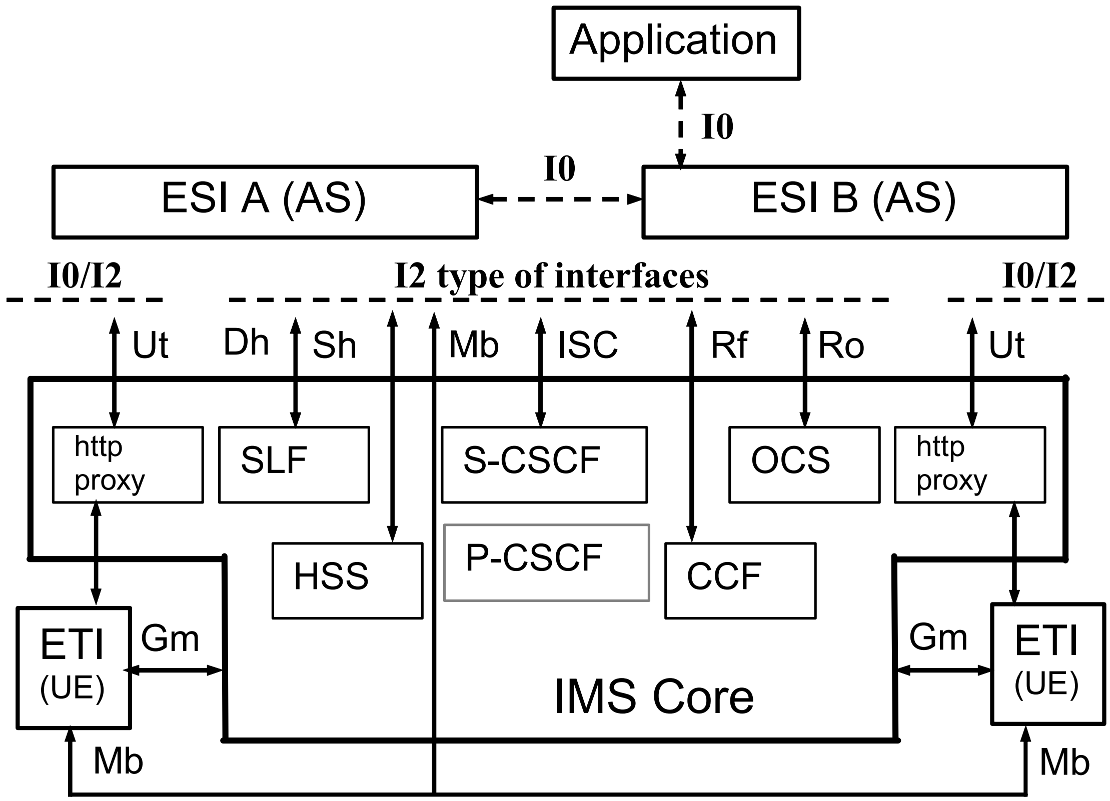

Figure 6-1: The main components of the IMS architecture in relation to enablers

The Enabler Terminal Implementation, abbreviated ETI in figure 6.1, can communicate with the Enabler Server Implementation (ESI ~ Application Servers (AS)). Any SIP-based service enabler must have at least a SIP-based interface towards endpoints. Specifically, it is the IMS core that provides the ability for these endpoints to be reached. Therefore, SIP-based service enablers SHALL interface to the IMS core, using the IMS Service Control (ISC) interface. ISC and the other interfaces between the OMA enabler implementations and the IMS are described in chapter 6.4.

If an enabler implementation is using IMS network capabilities it SHALL NOT build its own network capabilities on top of IMS.

The OMA enablers using both IMS and non-IMS network capabilities SHALL be specified in OMA with the assumption and requirement that the non-IMS networks offer the same capabilities as IMS, e.g. with regard to SIP, XCAP RTP, MSRP and other functionalities.

It is noted that the “Application server” concept as defined by 3GPP/3GPP2 is quite similar to the enabler concept defined in OMA, but they are not identical. The application server can correspond to an OMA enabler server implementation, ESI. The 3GPP/3GPP2 term “Terminal” can correspond to an OMA enabler terminal implementation, ETI, but these concepts are not identical either.

Terminals are typically used by individual end-users and can be mobile (e.g. implemented in small wireless devices or laptops), while application servers are typically fixed and are part of the network infrastructure run by the IMS operator or third party service providers.

However, whenever an OMA enabler server implementation and enabler terminal implementation interacts with IMS they SHALL follow the IMS specifications of 3GPP/3GPPP2 that apply for the application servers and terminals respectively.

6.3 IMS endpoints and protocol interfaces (Normative)

Figure 6.2 depicts IMS endpoints as described by 3GPP/3GPP2 and the protocol interfaces that IMS supports. There are two types of endpoints that can be connected to the IMS, i.e. the Enabler Terminal Implementation (ETI ~ Terminal (UE)) and the Enabler Server Implementation (ESI ~ Application Server (AS)).

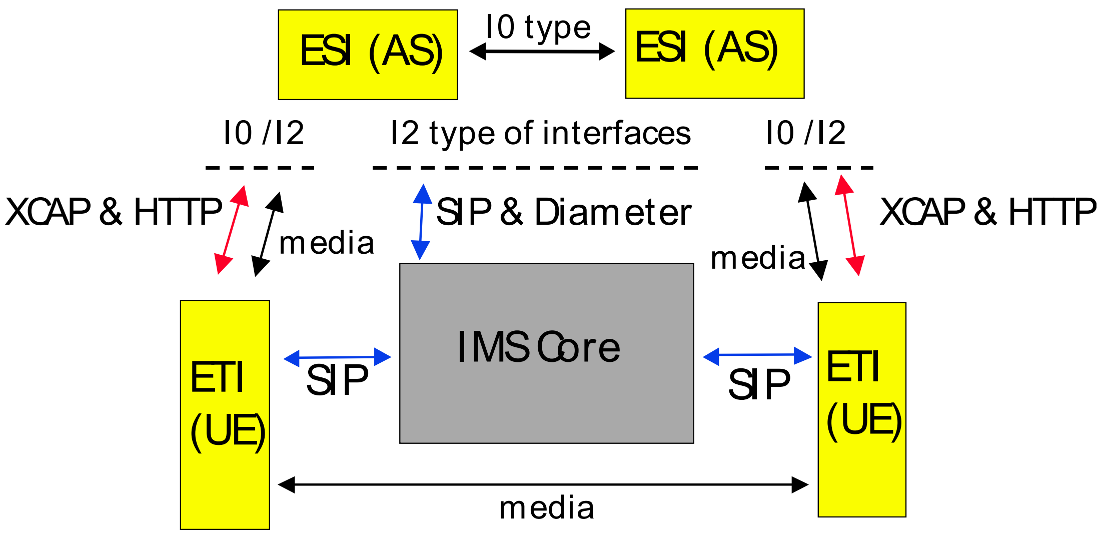

Figure 6.2: IMS protocol interfaces

IMS provides the end-points with a secure and resilient inter-domain SIP proxy server infrastructure, through which they can be reachable (registration for terminals, configuration based routing for application servers) and can use SIP methods to communicate with each other. Using SIP the endpoints are e.g. able to set up media sessions between each other. The media explicitly supported by 3GPP Release 6 and 3GGP2 Release A include but are not limited to voice, video and messaging sessions based on Message Session Relay Protocol (MSRP). In addition to SIP and the media sessions initiated by it, IMS provides a secure HTTP interface between UE the application server, i.e. between ETI and ESI in OSE terms. This interface is called Ut in IMS and further supports HTTP-based XML Configuration Access Protocol (XCAP), which allows the enabler terminal implementation (ETI) to manipulate various service related data in the enabler server implementation (ESI), such as resource lists used for presence and push to talk. The Ut interface is further described in chapter 6.4.

In general IMS can support any applications and enablers that are built using SIP, SDP, XCAP, RTP, MSRP or their extensions. The extension models and principles of these protocols are defined in the IETF, and IMS does not hinder this extensibility. The extensions to the SIP protocol that SHOULD be supported by the OMA enabler implementations are described in chapter 6.7. An enabler implementation in the terminal SHALL support IMS-specific functions like authentication and security association setup for terminals and an enabler server implementation SHALL support the ISC interface and other IMS interfaces.

6.4 IMS connectivity and signalling support for enablers (Normative)

Figure 6.3 shows a simplified view how enabler interactions in principle can be split in two layers, here named “SIP connectivity layer” and “enabler layer”. The “SIP connectivity layer” comprises the basic SIP proxy and registrar functions that allow end-to-end point connections based on addressing conventions using IMS Session Control functionality, as well as service-based routing and hop-by-hop security. IMS offers SIP infrastructure capabilities in the network and in the terminal and the “SIP connectivity layer” is common to all applications. So, “SIP connectivity layer” functionality SHALL NOT be developed for the individual OMA enablers.

The OMA service enabler realizations using IMS are specified in the enabler layer of OSE on top of the connectivity layer in the underlying network. The IMS connectivity layer looks completely transparent to the enabler layer, even though there may be a need to define some service-specific routing rules inside the IMS. Such definitions are seen to be part of the enabler configuration settings. At the enabler layer it SHALL NOT make a difference if the underlying infrastructure is IMS, or some other similar SIP network.

Similar layering exists for XCAP signalling. Below XCAP there is HTTP in the underlying network that offers transport capabilities, routing and security capabilities and addressing conventions, while XCAP on the enabler layer offers definitions of e.g. content type (or data format) and other definitions specific for a single XCAP application usage.

Figure 6.3 shows some possible interfaces between enabler implementations (I0 type of interfaces) and the enabler interfaces with the SIP connectivity layer of IMS and non-IMS SIP networks (I2 type of interfaces). The figure also shows interfaces between different implementations of the same enabler, e.g. used in a client-server configuration of the enabler.

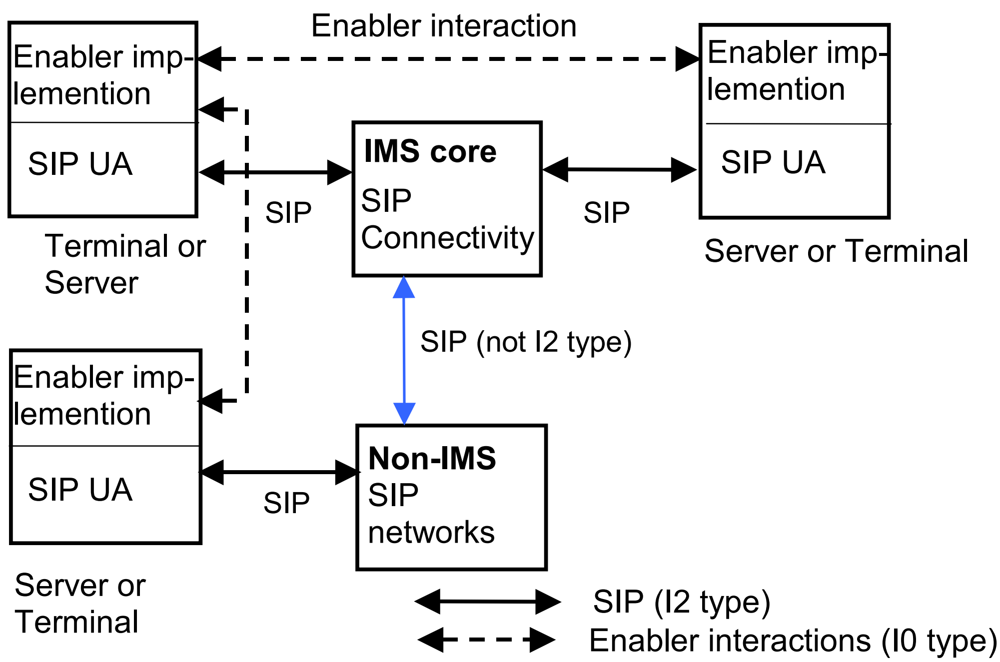

Figure 6.3: SIP interfaces for enablers

IMS can be connected to other SIP-based networks. OMA enabler implementations using IMS can therefore be connected to OMA enabler implementations that use non-IMS SIP-based networks as shown in Figure 6.3.

6.5 Interfaces to be used between enabler implementations and IMS (Normative)

Figure 6.4 depicts the interfaces that IMS provides to an OMA service enabler.

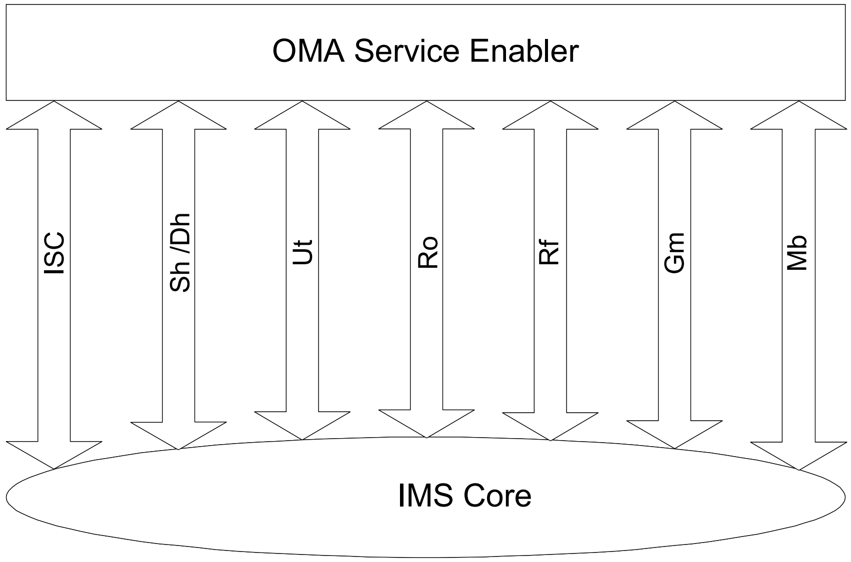

Figure 6.4: OMA service enabler interfaces to IMS core

The only IMS interfaces an OMA enabler MAY use are the following.

ISC interface

The ISC interface is between the enabler server implementation and the IMS core. The ISC interface provides the OMA service enabler with SIP/SDP call control, SIP event related subscription and notification, SIP messaging, etc. The ISC interface is based on SIP and is specified in 3GPP TS 23.228 [3GPP TS 23.228] or 3GPP2 X.P0013.2 [3GPP2 X.P0013.2].

The protocol used on the ISC interface is SIP, as specified in 3GPP TS24.229 [3GPP TS24.229] and 3GPP2 X.S0013.4 [3GGP2 X.S0013.4], respectively.

Sh interface

The Sh interface is between the enabler server implementation and HSS in the IMS core. The Sh interface provides the OMA service enabler with read and write operations of user data related to IMS. It also provides with functionality for subscription and notification of changes in the user data related to IMS. The Sh interface is specified in 3GPP TS 23.228 [3GPP TS 23.228] or 3GPP2 X.P0013.2 [3GPP2 X.P0013.2].

The protocol used on the Sh interface is DIAMETER, as described and specified in 3GPP TS29.328 [3GPP TS29.328] and 3GPP TS29.329 [3GPP TS29.328] respectively.

Dh interface

The Dh interface is between the enabler server implementation and the Service Locator Function (SLF) in IMS core. The Dh interface is quite similar to the Sh interface and is used by the enabler implementations to get the address of the HSS that handles a particular user in networks, where there are several HSS. The Dh interface is specified in 3GPP TS 23.228 [3GPP TS 23.228] or 3GPP2 X.P0013.2 [3GPP2 X.P0013.2]. The protocol used on the Dh interface is DIAMETER, as described and specified in 3GPP TS 29.328 [3GPP TS 29.328] and 3GPP TS 29.329 [3GPP TS 29.329] respectivly.

Ut interface

The Ut interface is between the enabler implementation in the terminal and the enabler server implementation. The Ut interface provides the UE with a set of operations that allow configuring user specific data in the OMA service enabler servers. The user specific data comprises, but it is not restricted to configuration management, such as configuration of presence lists and presence authorization rules. The Ut interface is specified in 3GPP TS 23.228 [3GPP TS 23.228] or 3GPP2 X.P0013.2 [3GPP2 X.P0013.2]. The protocol used on the Ut interface is being specified in 3GPP and is based on XCAP.

Ro interface

The Ro interface provides the OMA service enabler with an event based charging interface to the online charging system in the IMS core. The protocol used on the Ro interface is DIAMETER and the Ro interface is specified in 3GPP TS 32.225 [3GPP TS 32.225] and 3GPP2 X.S0013-008 [3GPP2 X.S0013-008].

Rf interface

The Rf interface provides the OMA service enabler with an interface to the off-line charging system in the IMS core. The protocol used on the Rf interface is DIAMETER and the Rf interface is specified in 3GPP TS 32.225 [3GPP TS 32.225] and 3GPP2 X.S0013-008 [3GPP2 X.S0013-008].

Gm interface

The Gm interface is between the enabler implementation in the terminal and the IMS core. The Gm interface provides the OMA service enabler with SIP/SDP call control, SIP event related subscription and notification, SIP messaging, etc. The Gm interface is specified in 3GPP TS 23.228 [3GPP TS 23.228] or 3GPP2 X.P0013.2 [3GPP2 X.P0013.2].

Mb interface

The Mb interface provides the OMA service enabler with user plane packet media streams over IP via the IMS core. The transport protocols for packet switched multimedia applications are standardized in 3GPP TS 26.236 [3GPP TS 26.236].

6.6 IMS Capabilities (Normative)

IMS offers specific solutions like:

- The mechanism for maintaining session state and providing control mechanisms for session re-direction and detection of unreachable users.
- The specified relationship between the responsibilities of the home and visited networks when the user is roaming.
- The security architecture that allows authentication of the user before the user is allowed to use network capabilities.
- The security architecture between network elements. In addition to providing security for the network elements, the security architecture provides the basis for a trust domain, which is used by certain SIP extensions. Of major importance of these extensions is the one that provides for calling/connected line identification, for which the mechanism without using trusted domains is not yet available in IETF.
- The mechanism for differential charging based on content, rather than solely on byte counts, and which allows the visited and home networks of the roaming user to agree on the charges due to each other.
- The mechanism for the policy control maintained by the network operator in the network in order to handle only the traffic that the user has contracted for and that corresponds to the application needs.
- The mechanism for ensuring that the traffic over the radio interface is kept to a minimum.
- The mechanism for provision of services by third parties, which are required by the regulatory bodies in certain geographic regions.

IMS also facilitates the easy deployment of the following:

- Generic IP transport layer media session establishment negotiation. Definitions for voice and video media exist in detail, extensibility allows defining new ones. This allows e.g. rich call and push to talk type of applications.
- Instant messaging
- Generic subscription and notification framework. A definition for the presence service exists, and extensibility allows defining new packages.

The service and support capabilities of IMS SHALL be made available to the OMA enablers via the IMS interfaces described in this AD. For instance, the ISC interface is a SIP interface with extended functionality defining how the IMS and the application servers interact with each other. IMS also offers so called “common capabilities”, which do not have direct interfaces to the enabler layer, but can be called by OMA service enablers (e.g. authentication).

IMS and the IMS capabilities in the context of OSE are described in chapter 5.

6.6.1 IMS Service Capabilities

OMA service enabler realizations using IMS SHALL use the IMS service capabilities where available.

The IMS service capabilities consist of session management, user data access, event subscription and notification, messaging, data manipulation, and conference control[2] as indicated in ref. [IMS in OMA RD] and as standardized by 3GPP/3GPP2

6.6.2 Supporting Capabilities

OMA service enabler realizations using IMS SHALL use the IMS supporting capability charging as indicated in ref. [IMS in OMA RD] and as standardized by 3GPP/3GPP2.

6.6.3 Common Capabilities

OMA service enabler realizations using IMS SHALL use the IMS internal common capabilities, like secured connections, authentication and authorization as indicated in ref. [IMS in OMA RD] and as standardized by 3GPP/3GPP2.

6.7 Special IMS Characteristics (Normative)

6.7.1 IETF 3GPP SIP extensions for 3GPP/3GPP2

IMS defines and uses several private header (P-header) extensions [RFC3455] compared to the standard SIP [RFC3261]. P-headers are used to carry information necessary for the IMS to work as a complete and secure system from the user’s, as well as from the operator’s, point of view. Together, the P-headers, the Path header [RFC3327], the Service-Route header [RFC3608], and the standard SIP headers and standard SIP functionality make various IMS-specific procedures possible, e.g. the AKA authentication ref. [RFC3310], establishment of the security associations, usage of IPsec, IMS charging, etc.

This section describes some of the SIP extensions defined by 3GPP for IMS. This is not a comprehensive list, it just shows some examples. For a complete list of the SIP capabilities and extensions used by IMS, refer to [3GPP TS 24.229] and [3GPP2 X.S0013-004].

In order to be able to utilize services built on IMS the enabler terminal implementation (ETI~UE) SHALL support the following main features in addition to SIP:

- AKA authentication within REGISTER
- security mechanism agreement for SIP within REGISTER
- IPsec based on AKA and on the security mechanism agreement for SIP

In order to connect an enabler server implementation (ESI~AS) to IMS to offer services the ESI SHALL support the following main features in addition to SIP:

- charging using the received information from IMS
- at least one of the modes: UAC, UAS and proxy
- two types of third party call control when acting as a B2BUA

[2] Editor’s Note: some of these capabilities are yet to be approved by 3GPP/3GPP2

IMS [3GPP TS 24.229] defines and uses several private header (P-header) extensions to SIP. The following P-headers are visible both in ETI and ESI (the corresponding terms UE and AS are used below):

- P-Access-Network-Info (carries information of the access network from UE to IMS and from IMS to ASes; visible only to trusted AS)
- P-Asserted-Identity
- P-Called-Party-ID (carries the target public user identity from IMS to UE). The P-Called-Party-ID header field may be seen at the AS when the AS is the called party (i.e., the destination of the session), but not in other scenarios (e.g., when the AS is just a proxy in the chain of proxies in the path towards a UE).
- P-Charging-Vector
- P-Charging-Function-Addresses

The following P-headers are visible only in UE, but not in AS:

- P-Associated-URI (carries associated URIs to the registered Public user identity from IMS to UE)
- P-Media-Authorization (carries media authorization token from IMS to UE)
- P-Preferred-Identity (carries identity preferred by the user from UE to IMS)

The following P-headers are visible in AS, but not in UE:

- P-Asserted-Identity (carries valid and authenticated Public user identity from IMS to AS)
- P-Charging-Vector (carries charging correlation information from IMS to AS)
- P-Charging-Function-Addresses (carries offline and online charging function addresses from IMS to AS)

6.8 System and Subsystem Descriptions (Normative)

6.8.1IMS Control Elements

The list is not exhaustive, as it only contains the elements applicable to this AD.

6.8.1.1 P-CSCF

P-CSCF - Proxy Call Session Control Function is the first contact point for the UE. It handles certain SIP related functions (e.g. forwarding of different SIP messages), security related functions (e.g. maintaining security association with the mobile), charging functions, SIP signalling compression/decompression. The P-CSCF can either be in the visited or in the home network. P-CSCF is specified in ref. [3GPP TS 23.228] and in ref. [3GPP2 X.S0013-002].

6.8.1.2 S-CSCF

S-CSCF - Serving CSCF performs the session control and registration services for the UE. It maintains a session state and interacts with service platforms as configured by the network operator for support of services. Within an operator’s network, different S-CSCFs may have different capabilities. The S-CSCF is located at the home network. S-CSCF is specified in ref. [3GPP TS 23.228] and in ref. [3GPP2 X.S0013-002].

6.8.2 IMS Service Elements

The list is not exhaustive, as it only contains the elements applicable to this AD.

6.8.2.1 SIP Application Server (AS)

The IMS / MMD introduces an AS - Application Server that may host and execute services. It offers value added IM services and normally resides in the user's home network. The Application Server can influence and impact the SIP session on behalf of the services and it uses the ISC interface to communicate with the IMS. In addition, AS can originate SIP requests on behalf of the UE. The AS may also terminate SIP requests. The AS defined in IMS/MMD specifications is different from conventional web AS. Details of the IMS AS can be found in in ref. [3GPP TS 23.228] and in ref. [3GPP2 X.S0013-002]. In OMA terms the AS corresponds to the enabler server implementation, ESI.

6.8.3 IMS Database Elements

The list is not exhaustive, as it only contains the elements applicable to this AD.

6.8.3.1 Home Subscriber Server (HSS)

HSS – Home Subscriber Server is the master database for a given user. It is the entity containing the subscription-related information to support the network entities actually handling sessions. The HSS is responsible storing the data for authenticating and authorizing the subscriber. The HSS is specified in ref. [3GPP TS 23.228] and in ref. [3GPP2 X.S0013-002].

6.8.4 IMS Charging Systems

The IMS charging architecture and principles, charging scenarios and charging systems are specified in [3GPP TS 32.200], [3GPP TS 32.225] , [3GPP2 X.S0013-007] and in [3GPP2 X.S0013-008].

In IMS there are separate systems for off-line and on-line charging, which are described below. 3GPP2's current release only supports off-line charging. However, the next 3GPP2 revision will include on-line charging.

6.8.4.1 Offline Charging System

The so-called Charging Collection Function, CCF, in 3GPP Release 5 and Charging Data Function, CDF, in 3GPP Release 6, are used for offline charging in IMS. An AS, i.e. an Enabler Server Implementation (ESI), or an IMS network entity SHALL report accounting information to the CCF/CDF. The CCF/CDF uses this information to construct and format Charging Data Records (CDR).

In 3GPP2, the equivalent entity for collection of charging data is the AAA for both 3GPP2 Rev-0 and Rev-A releases. (3GPP2 Rev-0 and Rev-A releases correspond to 3GPP Release 5 and Release 6 respectively.) The AAA uses accounting information to construct and format Accounting Information Records for both Rev-0 and Rev-A releases.

Offline charging SHALL be handled using the Rf reference point as specified in [3GPP TS 32.225] (Release 5), [3GPP TS 32.260] (Release 6) and [3GPP2 X.S0013-008].

The Rf reference point offers reliable transfer of Charging Information to 3GPP's CCF/CDF and 3GPP2's AAA with acknowledgement mechanisms and redundancy mechanisms. In 3GPP2 Release Rev-A and 3GPP Release 6, Rf is based on Diameter, specified in [3GPP TS 32.299] and [3GPP X.P0013-008-A], respectively.

6.8.4.2 On-line Charging System

In 3GPP systems, the IMS Online Charging System, OCS, is used for online charging. An AS, i.e. an ESI, or a S-CSCF SHALL report credit control information to the OCS using the Ro interface. This information is used for online based charging. The OCS is located at the home network of the end user terminal. The OCS functionality is defined in [3GPP TS 32.200] (Release 5) and [3GPP TS 32.296] (Release 6).

The protocol for the Ro reference point is easily extendable to include additional online charging functions. The Ro reference point supports integrity protection and authentication for the case that the AS (ESI) is outside the operator domain. In 3GPP the Ro is based on Diameter Credit Control Application, specified in [3GPP TS 32.225] (Release 5) and [3GPP TS 32.299] (Release 6). In harmonization with 3GPP's charging documentation, the equivalent Ro specifications in 3GPP2 are in the process of being specified in [3GPP2 X.P0013-008-0] and [3GPP2 X.P0013-013-A] for releases Rev-0 and Rev-A, respectively.

6.8.4.3 List of charging specifications in 3GPP Release 5 and Release 6

The 3GPP specification TS 32.200 [3GPP TS 32.200] "Charging management; Charging principles (Release 5)" describes the principles of charging and billing and TS 32.225 [3GPP TS 32.200] specifies the details of IMS Charging in 3GPP Release 5 systems.

The 3GPP specification TS 32.240 "Charging management; Charging architecture and principles (Release 6)" [3GPP TS 32.240] gives a general overview of charging in 3GPP Release 6. Some of the other specifications in Release 6 related to charging that may be relevant for OMA enablers are:

TS 32.260 IM Subsystem Charging [3GPP TS 32.260]

TS 32.296 Online Charging System (OCS) applications and interfaces [3GPP TS 32.296]

TS 32.299 Diameter Charging Application [3GPP TS 32.299]

6.8.5 IMS Security Functions

OMA enablers SHALL rely on the security mechanisms provided by IMS, as described in this section.

IMS classifies the security functions into:

1. Access Security, as specified in [3GPP TS 33.203] and [3GPP2 S.R0086]; and

2. Network Security. 3GPP specifies network security procedures in [3GPP TS 33.210]. 3GPP2 does not have a corresponding specification. However, their network security requirements are contained in S.R0086.

6.8.5.1 IMS Access Security

The IMS Access Security functions affect the IMS implementation in the UE and the network. IMS Access Security has the following charectaristics:

- Mutual authentication between the IMS subscriber and the network.
- The private user identity is used for authentication. The private user identity is stored, along with shared security parameters both on a tamperproof identity module (e.g., 3GPP's UICC, 3GPP2's RUIM) or in the terminal secure memory, and also in a server in the network..
- IMS Authentication is based on HTTP Digest Authentication using IMS-AKA as per 3GPP and 3GPP2 specifications (see [3GPP TS 24.229], [3GPP2 X.S0013-004] and [3GPP TS 33.203]).
- Users may register one or more public user identities. Upon authentication of the private user identity the network is able to verify that the public user identity or identities are valid.
- Confidentiality between the UE and the access point is specified based on SIP as defined in [3GPP TS 33.203] Release 6 (not in Release 5) and required in [3GPP2 S.R0086].
- Integrity protection over the air, between the UE and the access point is negotiated during the SIP registration. Integrity protection in the core network is specified in [3GPP 33.210] and [3GPP2 S.R0086].
- A security association agreement procedure [RFC 3329] allows negotiation of the security mechanism between the UE and the Access Point (1st hop.).

6.8.5.2 IMS Network Security

The IMS Network Security functions affect the implementation of network nodes. IMS Network Security has the following characteristics:

- Inter-domain interfaces supports confidentiality and integrity protection as per [3GPP 33.210] or [3GPP2 S.R0086].
- Intra-domain interfaces may support, at the discretion of the operator, confidentiality and/or integrity protection.

6.9 Subsystem Collaboration and enabler interactions (Normative)

This AD describes the general principles how enabler implementations SHALL use IMS.

In OSE, OMA enabler implementations SHALL make use of the IMS capabilities and interfaces described previously in the document, e.g. charging, authentication, service management. The normative detailed description of how an OMA enabler uses IMS and e.g. enabler specific IMS interface parameters SHALL fall in the scope of the AD and specifications of the enabler concerned, and SHALL NOT fall in the scope of the IMS in OMA AD.

New IMS related enabler specifications SHALL be aligned regarding the ways IMS is used and the way such usage is described and specified.

The interaction between OMA enablers SHALLcomply with OSE.

Appendix A. Change History (Informative)

A.1 Approved Version History

Reference	Date	Description
OMA-AD-IMS-V1_0-20050809-A	9 Aug 2005	Status changed to Approved by TP TP ref# OMA-TP-2005-0238R01-IMSinOMA-V1_0-for-Final-Approval.

Appendix B. Static Conformance Requirements (SCR)

B.1 Conformance Requirements Notation Details

The tables in this Appendix use the following notation:

Item: Entry in this column MUST be a valid ScrItem according to [IOPPROC].

Function: Entry in this column SHOULD be a short descriptive label to the **Item** in question.

Status: Entry in this column MUST accurately reflect the architectural status of the **Item** in question.

- **M** means the **Item** is mandatory for the class
- **O** means the **Item** is optional for the class
- **NA** means the **Item** is not applicable for the class

Requirement: Expression in the column MUST be a valid TerminalExpression according to [IOPPROC] and it MUST accurately reflect the architectural requirement of the **Item** in question.

B.2 IMS related work split OMA, 3GPP, 3GPP2

Item	Function	Reference	Status	Requirement
IMSinOMA C-001	Detailed work split on enablers	Subclause 4.3	M	
IMSinOMA C-002	Avoid fragmentation of IMS and SIP specifications	Subclause 4.3	M	
IMSinOMA C-003	Possible new IMS requirements	Subclause 4.3	M	
IMSinOMA C-004	Context collaboration model	Subclause 5.5	M	

B.3 IMS related work split inside OMA

Item	Function	Reference	Status	Requirement
IMSinOMA C-005	Detailed descriptions and IMS interface parameters	Subclause 6.9	M	
IMSinOMA C-006	Aligning new IMS related OMA enabler specifications	Subclause 6.9	M	
IMSinOMA C-007	OSE and interactions between OMA enablers	Subclause 6.9	M	

B.4 Planned phases

Item	Function	Reference	Status	Requirement
IMSinOMA C-008	Phase 1.0 of the IMSinOMA Architecture	Subclause 4.6	M	

B.5 Enablers' usage of IMS interfaces

Item	Function	Reference	Status	Requirement
IMSinOMA C-009	IMS interfaces used by enablers	Subclauses 5.2 and 6.5	M	
IMSinOMA C-010	Specified normative IMS interfaces	Subclause 5.4	M	
IMSinOMA C-011	SIP-based enabler interfaces with the IMS core network	Subclause 6.2	M	
IMSinOMA C-012	Extensions to the SIP protocol	Subclauses 6.3 and 6.7	M	

B.6 Enablers' usage of IMS resources and capabilities

Item	Function	Reference	Status	Requirement
IMSinOMA C-013	IMS resources (services and capabilities)	Subclauses 5.3 and 6.9	M	
IMSinOMA C-014	IMS capabilities like charging, authentication, compression, routing.	Subclauses 5.4, 6.6 and 6.9	M	
IMSinOMA C-015	Enabler usage of IMS network capabilities	Subclauses 6.2 and 6.6	M	

B.7 IMS and Non-IMS networks

Item	Function	Reference	Status	Requirement
IMSinOMA C-016	IMS and Non-IMS network capabilities	Subclause 6.2	M	
IMSinOMA C-017	Underlying SIP network infrastructure	Subclause 6.4	M	

B.8 Enabler Server Implementations

Item	Function	Reference	Status	Requirement
IMSinOMA	Interactions between enabler server	Subclauses 6.2	M	

C-018	implementations and IMS	and 6.3		
IMSinOMA C-019	"SIP connectivity layer" functionality	Subclause 6.4	M	
IMSinOMA C-020	Extensions to the SIP protocol	Subclause 6.7	M	

B.9 Enabler Terminal Implementations

Item	Function	Reference	Status	Requirement
IMSinOMA C-021	Interactions between enabler terminal implementations and IMS	Subclauses 6.2 and 6.3	M	
IMSinOMA C-022	"SIP connectivity layer" functionality	Subclause 6.4	M	
IMSinOMA C-023	Extensions to the SIP protocol	Subclauses 6.7	M	