OMTP

SPECIFICATION OF A SOFTWARE PLATFORM

IMS FUNCTIONAL REQUIREMENTS V2.0

.

VERSION: 2.0

STATUS: Issued

DATE OF PUBLICATION:

OWNER: OMTP LIMITED

CONTENTS

1 INTRODUCTION

1.1 DOCUMENT PURPOSE

This document defines the minimum set of requirements for IMS (IP Multimedia System) functionalities on mobile Terminals and identifies which of these functionalities shall be available for developing new IMS capable applications in the Terminal. 3GPP IMS Release 7 and related service enablers are the scope of this document.

Specifically the document contains:

– Requirements to ensure common and consistent functionality on IMS capable Terminals (e.g. requirements on SIP protocol), referencing 3GPP specifications as much as possible.

– Functional Requirements to enable easier development of consistent IMS applications in the IMS implementations within a Terminal (e.g. availability of SIP REGISTRY command for application developers)

– Functional Requirements to enable proper deployment of applications on the Terminals (e.g. application or new capability registry)

The requirements included in this document cover both basic IMS aspects and standardized service enablers (addressed as features later in this document) defined by 3GPP, OMA and other bodies. It is also acknowledged that many of them could also apply to any Terminal using non-3GPP access networks (e.g. WiFi).

1.2 SCOPE & RELATIONSHIP WITH SDOS

1.2.1 DOCUMENT SCOPE

Diagram 1 below depicts the logical relationships between different IMS components and functionalities. Please note that it is not intended to define any layered architecture in the diagram.

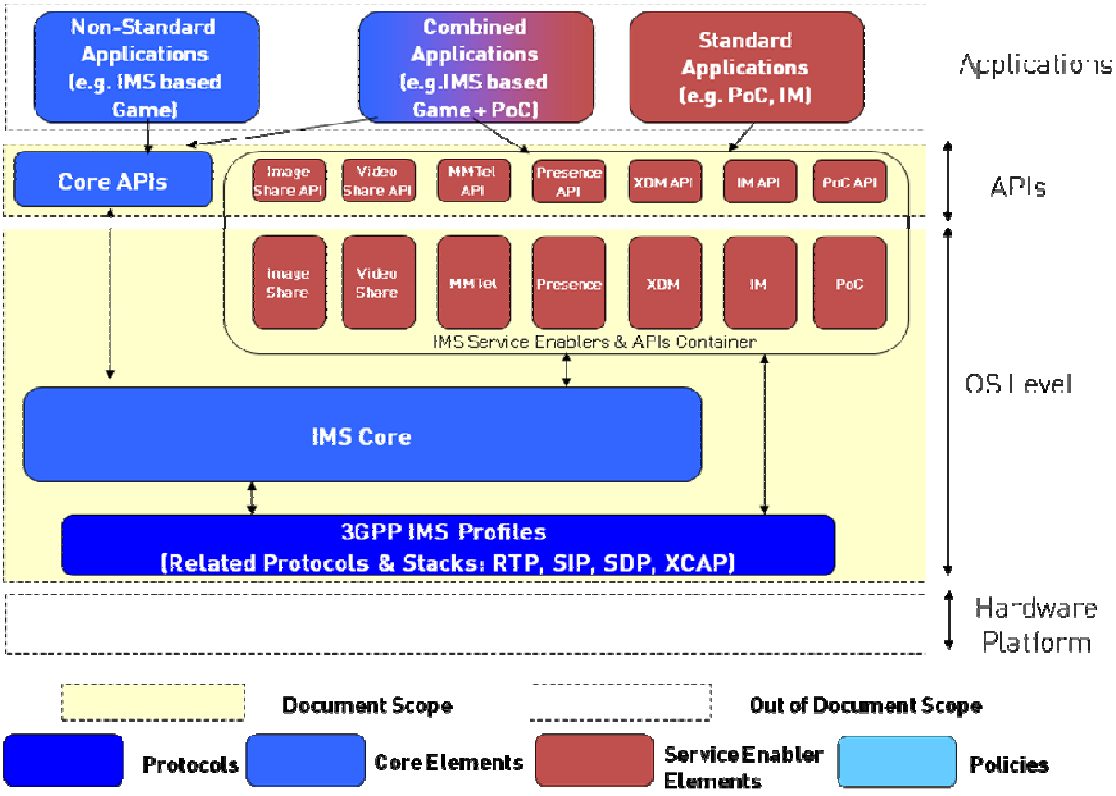

Diagram 1: IMS Logical Relationships

This model is structured in four main components

- Hardware Platform: It comprises all the hardware elements (e.g. Camera, Display, UICC) available on the Terminal.
- OS: It gathers all the software modules built on top of the hardware platform. Its main responsibility is implementing the functionality needed in order to offer mobile services.
- APIs: The APIs expose the functionality implemented in the OS Level via a programming interface that allows possible application development. Although the API layer has been represented as a single module for the sake of the simplicity it is also possible to have different API sets (e.g. Java or C++) using a single OS Level Framework.
- Applications: This block comprises all the applications available on the Terminal in order to offer a service to end-user (e.g. a game, an Instant Messaging Client…)

The IMS related modules have been included within each of these elements. These blocks are:

- OS
  - 3GPP IMS Profiles: This module gathers all the functionality related to the protocols essential in order to offer IMS Services (e.g. SIP, SDP, RTP and XCAP).
  - IMS Core: This block provides the basic IMS functionality using the capabilities of the IMS related protocols and stacks. The main target of this module is abstracting the complexity of dealing directly with the protocols by providing a set of core high level functionalities (e.g. Session Management or Authentication)
  - IMS Service Enablers: Although the functionality offered by the IMS Core abstracts protocol details, it is generic and hence not oriented to provide any concrete end-to-end service. The IMS Service Enablers offer functionality focused in a specific service (e.g. PoC, IM, presence). Therefore these enablers make the offering of end-to-end services to the users easier. The enablers are typically built using the high-level functionalities offered by the IMS Core.
- APIs:
  - Core APIs: This module comprises all the programming interfaces exposed by the IMS Core in order to develop IMS applications.
  - Service APIs: This module gathers all the APIs offered by the IMS Service Enablers for application development.
- Applications
  - Standard Applications: These applications are based exclusively on the Service Enablers functionality and therefore are intended to offer a single end-to-end service (e.g. PoC Client, Instant Messaging Client and MMTel).
  - Non-Standard Applications: These applications are built using only the IMS Core functionalities and hence provide a service not related to any standard solution (e.g. an IMS based game).
  - Combined Applications: These applications combine the functionalities offered by the Core IMS and the Service Enablers (e.g. an IMS based game that allows users to chat using PoC).

All the IMS related modules listed above comprise the IMS Framework. This document does not define any particular implementation of this framework (e.g. whether it should be a single module, an application etc.) but defines

requirements for the functionality that mobile Terminals should offer regarding IMS capabilities.

The definition of a common set of functionalities for IMS frameworks together with the services available for application developers will foster the creation of an open environment for service creation. To achieve this, the document focuses in the following parts of the framework:

- Functional Requirements: A set of requirements are defined to identify the needs and functionalities expected in IMS frameworks. The focus is put on the IMS Core capabilities and protocols as well as on the IMS service enablers. As the main target of the document is identifying a core set of requirements that facilitates interoperability, the definition of requirements for IMS applications is out of the scope.

- Application Programming Interface (API): The focus of the document is not on the detailed APIs and protocol specifications as these activities are covered by the OS providers, handset manufacturers and SDOs. However, the document provides high level definitions of the IMS Core and service functionality that should be exposed to application developers, as this is essential to guarantee a consistent environment for service creation. The definition of requirements for the IMS protocols and stacks APIs has been considered as out of the scope of this document. It is anticipated that whenever possible direct access to protocol capabilities should be avoided using the Core and Service APIs instead.

As the main focus in the short-term is achieving a consistent functionality rather than a common user experience, in this phase applications have been considered out of the document scope.

1.2.2 RELATED SDOS

The aim of the document is not defining a set of competing standards, but referring to available standards or providing inputs to them whenever needed.

There are some related SDOs considered especially relevant for the definition of Terminal functionality. These are:

- 3GPP: This document is based on 3GPP Release 7 Specification. 3GPP developed the IP Multimedia Subsystem as part of Rel-5 and Rel-6. These specifications have been adopted by 3GPP2 and TISPAN and were the basis for OMTP IMS Functional Requirements v1.0 [ref]. 3GPP also specifies conformance test specifications to validate the mobile implementations against test equipment. These specifications are used in the GCF and PTCRB process of certification of IMS clients in mobile Terminals. 3GPP R7 also specifies two service enablers on top of the core IMS capability called Combinational Services (CSI) and Multi-Media Telephony (MMTel). OMA DM Management Objects are defined by 3GPP for configuration of service enablers, IMS and PS domain bearers.

- IETF: Some of the IMS key protocols (SIP, SDP etc.) have been defined by this body.

- OMA: This organisation has defined some service enablers (presence, XDM, PoC, Instant Messaging…) on top of the core IMS capability. OMA also specifies IoT specifications and run test events to validate mobile implementations of these service enablers. These specifications are used in the GCF process of certification of IMS clients in the mobiles. OMA DM Management Objects are defined by OMA for configuration of service enablers and PS domain bearers.

- GSMA: The GSMA has been developing interoperability trials covering IMS video-sharing.

There are some platform specific activities in the Application Programming Interface area defined in the JCP. The relevant JSRs are considered as an input for OMTP. The contents of this document could also be used to identify possible gaps in these JSRs:

- JSR-180 defined a general SIP API for J2ME.

- JSR-281 is defining a framework and APIs for IMS Core on which operators and third parties could develop and offer IMS services.

- JSR-325 is defining an IMS Services framework and APIs for common Communication Enablers

1.2.3 SECURITY CONSIDERATIONS

This document defines a set of requirements for the IMS APIs that should be available to developers in the Terminal execution environments. These APIs are intended to offer applications access to both IMS Core and IMS Service Enablers functionalities.

Some of these APIs will allow applications to perform operations that may trigger billing events, access to user preferences or the disclosure of personal data. Because of this possibility, it is acknowledged that not all the APIs will be available to all the applications and that some restrictions (based on the need of explicit user consent or the level of trust of the application) could apply.

The definition of these restrictions or the mechanisms for granting access to these APIs is not in this scope of this document. The recommendation is to restrict access to APIs following the approach defined by OMTP in the Application Security Framework [1]. Therefore it is understood that successful use of these APIs are dependant on authorization levels as defined by ASF [1]. However, ASF [1] does not cover all IMS-specific security events (e.g.

changing PoC settings). Moreover, a billing event may not be obvious to a terminal.

1.3 BUSINESS RATIONALE

Although IMS is one of the most important technologies that have come out during the last few years, the standardisation efforts in this area are still very focused on the protocols and do not provide a clear idea on how an IMS Terminal should behave.

The objective of this document is to provide a more comprehensive view on what an IMS Terminal should be by aggregating all these standards in a single forum and providing a less protocol-centric point of view. Furthermore these requirements pay special attention to defining how IMS functionality should interact with the basic phone capabilities. This aspect has been identified as one of the big challenges and opportunities that this kind of Terminal offers.

Having a common set of IMS requirements should provide benefits for all mobile industry players:

- Reducing divergence in operators' IMS requirements in an early stage will not only reduce cost for mobile manufacturers and OS providers, but also avoid market fragmentation.
- Having common IMS functionality across mobile Terminals will increase the number of Terminals that can interoperate both with each other and with networks.
- The development of an application by a third party will be easier, and the applications are more likely to be compatible.
- End users will also benefit from a richer IMS framework that simplifies service creation and offers a better user experience.
- Expected use of IMS-based application/services is higher.

1.4 INTENDED AUDIENCE

The main audiences for these recommendations are:

Mobile Operators; as one of the main targets is reducing requirements fragmentation, OMTP operators should adopt or reference these recommendations within their requirements specifications.

OMTP Terminal implementers; i.e. the equipment and technology vendors that will be asked to satisfy OMTP recommendations.

Application Developers; the API requirements in this document should allow smooth and seamless development of an application independent of the underlying OS or platform.

1.5 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 [2].

- MUST: This word, or the terms “REQUIRED” or “SHALL”, mean that the definition is an absolute requirement of the specification.
- MUST NOT: This phrase, or the phrase “SHALL NOT”, mean that the definition is an absolute prohibition of the specification.
- SHOULD: This word, or the adjective “RECOMMENDED”, mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
- SHOULD NOT: This phrase, or the phrase “NOT RECOMMENDED” mean that there may exist valid reasons in particular circumstances when the particular behaviour is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behaviour described with this label.
- MAY: This word, or the adjective “OPTIONAL”, means that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item. An implementation which does not include a particular option MUST be prepared to interoperate with another implementation which does include the option, though perhaps with reduced functionality. In the same vein an implementation which does include a particular option MUST be prepared to interoperate with another implementation which does not include the option (except, of course, for the feature the option provides.)

The requirements within this document are uniquely identified using the following format:

IMS-####, where:

is a number that uniquely identifies the requirement.

The following requirement types have been identified:

Standard Requirement: The requirement is a reference to standard

New Requirement: The requirement is not related with any available standard (e.g. 3GPP, OMA, JCP…).

2 USE CASES

2.1 NON-STANDARD SERVICES BASED ON IMS APPLICATIONS

An operator or a 3rd Party wishes to deploy a new IMS service not based on existing standardised services. In this case, the new service is typically offered via an application client developed using the IMS Core APIs offered by mobile Terminals.

An example of this type of application is a game which makes possible the connection between two users using IMS multimedia sessions.

2.2 COMBINED NON-STANDARD / STANDARD SERVICES

There are situations in which operators wish to create a new IMS service not supported by any standard in combination with some of the standardised capabilities offered by the handset.

An example of this type of service is a game that allows the use of PoC across the users who have joined the gaming session. Combination of a game service and presence is another example of this kind of service.

The new service is offered via an application that uses the services and functionalities exposed for accessing the core IMS capabilities and protocols in combination with those capabilities offered by the IMS Service Enablers interface (in this case PoC and presence).

Combination of services can be achieved via adding or dropping media on an existing dialog. The services added must be distinguished in order to handle media correctly. Services can also be combined via the use of independent contexts.

2.3 STANDARD SERVICES AND IOT ACROSS OPERATORS

In many cases operators wish to guarantee that the users can use IMS services in an interoperable way with other operators' subscribers. The interoperability is typically reached by defining a framework in which all the aspects of the service are defined and standardised.

An example of this type of generic services is Presence, in which users from operator A can see the presence status of one or more operator B subscribers. In combination with the presence service, it is also important to guarantee that PoC and Instant Messaging sessions can be set up across users subscribed to different operators.

These services are based mainly on the functionalities offered by standardised service enablers. To guarantee interoperability (IoT), these standards will be identified and referenced. In cases where options in these standards make IOT difficult, a de-optionalisation process will be recommended.

De-optionalisation is the identification of optional features in the standards that are deemed as essential by the operator community. A potential example related to PoC user identification is the following optional requirement in OMA PoC: “The PoC Client MAY override nicknames received from the PoC Server if a locally stored display name is available in the User Equipment.” [3]. If this requirement is considered by OMTP as essential, this document will refer to it as mandatory.

Apart from the currently available standards, some use cases considered in section 2.1 may evolve into standardised solutions (e.g. content sharing).

3 IMS TERMINAL PROFILES

IMS Terminals that may rely on these recommendations are likely to have different capabilities in terms of their processing power, memory, user interface, I/O, audio and visual support.

Due to these different capabilities and characteristics, OMTP specifies two different profiles against which Terminals may claim full compliance.

Profiles are intended to represent benchmarks of terminal capabilities in the global market.

Where individual market needs differ it may be possible to combine Profile 0 with specific Features and Feature Groups specified (see section **Error! Reference source not found.** for definitions).

It is recommended that any such "sub-profiles" should be constructed in a way to ensure interoperability in the local and global market. It should be noted that any decision to create OMTP IMS sub-profiles may lead to fragmentation across devices, markets and networks if incorrectly managed.

For a summary of the Profiles see section 3.3. For further information on the usage of feature groups see section **Error! Reference source not found.**.

3.1 TERMS

- **Feature:** A high-level capability or service of the User Equipment. Examples of features are PoC or Instant Messaging. Each requirement is linked to a feature so it is easy to understand which functionality it is related to.

- **Feature Group:** A set of Features that should be offered together because of their **functional dependencies** (e.g. PoC, presence and XDM could be considered as a feature group). The definition of a feature group is intended to provide guidance on the collection of features that must be implemented simultaneously in the Terminals. A feature may appear in multiple Feature Groups.

- **Profile**: Set of Features or Feature Groups that should be offered together on a Terminal depending on its **capabilities, target users or market considerations**.

3.2 FEATURES AND THEIR LINK TO REQUIREMENTS

This document contains a set of IMS related requirements. Some of them are based on references to standards; others are for clarifications or recommendations to adopt options in the standards. There are also

requirements that do not refer to any standards for operational or market reasons. Regardless of its nature, each requirement in this document is linked to a feature.

For instance, the following requirements are of very different type but all of them are related to the same feature (PoC):

- IMS-0740: “The UE MUST support Push-to-talk Over Cellular v1.0 as specified by OMA”
- IMS-0810: “ The UE MUST support Browser Based PoC Client Invocation as specified by OMA“
- IMS-1620: The UE MUST offer an API to allow applications to get the initiator of a PoC session

The list of features identified in this document is described below:

- **IMS Core:** IMS functionalities that can be implemented in most of Terminals and that are required for IMS enabled services.
- **Application Environment:** IMS Functionalities that allow multiple applications to be integrated in the same Terminal.
- **Presence:** Functionalities that allow the UE to collect and disseminate Presence Information subject to a wide variety of controls.
- **XDM:** Capabilities that allow the UE to generate and store XML documents (needed for the operation of other enablers) in the network where they can be located, accessed and manipulated.
- **IM:** Functionalities that allow a user to send text information to users in an interactive manner.
- **PoC:** T*wo*-way form of communications that allows users to engage in immediate communications with one or more users. Push over Cellular (PoC) service is similar to a “walkie-talkie” application such that by pressing a button a talk session with an individual user or a broadcast to a group of participants is initiated. PoC communication is subject to “Floor Control”, such that only the party having the floor can transmit at any one time.

- **Video-Share:** Functionalities that allow users to share live video over Packet Switched (PS) connection in real time simultaneously with an ongoing Circuit Switched (CS) call.
- **MMTel:** Feature that allows multimedia conversational communication between two or more end points.
- **Image Share:** Feature that allows users to share Images between them over PS connection with ongoing CS call.
- **SIP Push:** Functionalities that allow the delivery of push OTA announcements encapsulated in Session Initiated Protocol (SIP) messages.
- **Voice Call Continuity:** Functionalities that allow a voice call to persist as a Terminal moves between circuit switched and packet switched radio domains.
- **NAT Traversal:** Functionalities that allow establishing connections between hosts in private TCP/IP networks that use NAT devices.

3.3 PROFILES

The table below describes the features that are applicable for each of the profiles defined in this section[1]

[1] The list of profiles is non-exhaustive

	Profile 0	Profile 1
IMS Core	YES	YES
VCC		YES
NAT Traversal		YES
MMTel		YES
Application Environment		YES
OMA PoC		V2.0
XDM		V2.0
IM		V1.0
Presence		V1.1
Video-Share		YES
Image-Share		YES
SIP Push		YES

Compatibility between the above service enabler versions will be defined by the referenced specifications and not by OMTP.

The following sections describe the rationale behind the two defined profiles and the typical use cases addressed by them.

3.3.1 IMS OMTP LIGHTWEIGHT PROFILE (IMS P0)

The IMS OMTP Lightweight profile, or Profile 0, is a subset of the full profile and is the most basic implementation option for OMTP IMS compliance.

The IMS OMTP Lightweight profile mandates support only for the basic core features and requirements of the OMTP IMS Framework and is intended for early and/or low end IMS Terminals.

Lightweight implementations will typically reside on a Terminal in which capability limitations do not allow the full profile implementation.

The main use cases that the Lightweight Profile addresses are those covered in section 2.1, for instance:

- Basic applications that require IMS communication capabilities (e.g. a game in which IMS is used to transfer media).
- Core services like emergency calls or Voice over IP.

It is recommended that wherever possible, the Full Profile (P1) should be implemented on devices.

3.3.2 IMS OMTP FULL PROFILE (IMS P1)

The IMS OMTP Full profile, or Profile 1, is for higher end Terminals that are capable of supporting all the requirements of this specification. Effectively, these Terminals have the capability to perform all of the requirements of the OMTP IMS framework.

The main use cases that this profile addresses are those covered in section 2.1, 2.2 and 2.3, for instance:

- Applications exclusively based on advanced service enablers (e.g. SIP Push).
- Applications that make use of advanced service enablers (e.g. an application including tickers updated via SIP Push).
- Applications that require extended IMS core capabilities (e.g. a PBX application allowing media transfer, VCC)

3.4 PROFILE EXTENSIONS

OMTP defines two profiles with which implementers may claim compliance; the Lightweight Profile (P0) and Full Profile (P1).

Features are used to bridge the gap between the lightweight and full profiles by allowing implementers to append the Lightweight Profile with intermediate functionality.

The following profiles may be acceptable implementations of the OMTP IMS requirements (subject to market or operator-specific requirements):

- Lightweight Profile compliance.
- Lightweight Profile + Feature X compliance.
- Full Profile compliance.

Multiple Features can be combined with the Lightweight Profile to create a compliant sub-profile. For example, the Lightweight Profile may be combined with Videoshare, Image-Share and Feature Group 3 (shown below)

simultaneously to create a compliant sub-profile offering a rich communication suite.

3.5 FEATURE GROUPS

The feature groups are intended to describe the functional dependencies of different enablers and may be combined with the Lightweight Profile to construct 'sub-profiles' depending on different market and business needs.

Some of the features identified involve mutual dependencies. Due to those functional relationships, Features within a Feature Group must be implemented simultaneously as shown in the Feature Groups below.

For instance, Terminals offering PoC features are likely to offer also presence, XDM and IMS Core features as well.

The following list of Feature Groups has been identified[2]:

- Feature Group 1: PoC v1.0, Presence v1.1, XDM v1.1
- Feature Group 2: PoC v2.0, Presence v1.1, XDM v2.0
- Feature Group 3: IM v1.0, Presence v1.1, XDM v2.0
- Feature Group 4: Presence v1.1, XDM v1.1

[2] All the feature groups require the OMTP IMS Lightweight Profile (P0)

4 STRUCTURE OF THE REQUIREMENTS

The following sections include a set of tables summarising the requirements that apply for each Terminal profile. All the tables include the following information for each requirement:

- Requirement ID: Unique identifier for the requirement following the numbering described in section 1.5.
- Requirement: Description of the requirement.
- Type: Indicates whether the requirement is a reference to a standard (Std) or a new requirement (New).
- Feature: Identifies the functional category which the requirement is linked to.
- Version Applicability: Identifies the version(s) of the referred standard the requirements applies to.

5 FUNCTIONAL REQUIREMENTS

5.1 USER EQUIPMENT (UE) BEARER SPECIFIC REQUIREMENTS

REQ. ID	REQUIREMENT	TYPE	FEATURE
IMS-0010	The Terminal MUST be able to support (depending on operator's preference) a minimum of 2 simultaneous UMTS/GPRS contexts with different APNs (i.e. primary PDP contexts, see TS 23.060 [4] 9.2.2.1).	**STD**	**IMS CORE**
IMS-0020	The UE MUST support secondary PDP contexts (see TS 23.060 [4] Section 9.2.2.1.1).	**STD**	**IMS CORE**
IMS-0030	The UE MUST be able to setup a dedicated primary PDP Context for SIP signalling. When this dedicated context is used, it SHALL handle the "signalling indication" and the "signalling flag".	**STD**	**IMS CORE**
IMS-2900	The UE SHOULD allow simultaneous CS and PS communications. NOTE: This requirement is overridden by requirements IMS-0910 and IMS-0941 for Video-Share and Image-Share respectively.	**STD**	**IMS CORE**
IMS-0070	The UE MUST setup the PDP contexts and make them available for any media streams resulting from session setups.	**NEW**	**IMS CORE**

5.2 IMS Related Protocols

Following requirements describe the critical protocols (non-exhaustive) for IMS offering. For complete protocol reference, please refer to 3GPP Release 7 specifications.

Req. ID	Requirement	Type	Feature
IMS-0080	The UE MUST support Session Initiation Protocol (SIP) as specified in TS 24.229 [5] Section 5.	**Std**	**IMS Core**
IMS-0090	The UE MUST support Session Description Protocol (SDP) as specified in TS 24.229 [5] Section 6.	**Std**	**IMS Core**
IMS-0100	The UE MUST support IPv4 as specified in RFC 791 [6].	**Std**	**IMS Core**
IMS-0110	The UE MUST support IPv6 as specified in RFC 2460 [7].	**Std**	**IMS Core**
IMS-0120	The UE MUST support IPSec-3GPP as specified in RFC 3329 [8].	**Std**	**IMS Core**
IMS-0130	The UE SHOULD support DHCPv6 as specified in RFC 3315 [9].	**Std**	**IMS Core**
IMS-0131	The UE MUST support DHCPv4 as specified in RFC 2131 [47]	**Std**	**IMS Core**
IMS-0140	The UE MUST support DNS as specified in RFC 1591 [10].	**Std**	**IMS Core**
IMS-0150	The UE MUST support RTP and RTCP as specified in RFC 3550 [11].	**Std**	**IMS Core**
IMS-2910	The UE SHOULD support RTSP as specified in RFC 2326 [12].	**Std**	**IMS Core**
IMS-2920	The UE SHOULD support XCAP as defined in [13].	**Std**	**IMS Core**
IMS-0180	The UE MUST support HTTPS as specified in RFC 2660 [14].	**Std**	**IMS Core**

REQ. ID	REQUIREMENT	TYPE	FEATURE
IMS-0190	The UE MUST support SIP SigCOMP as specified in TS 24.229 [5], Section 8.1.	**STD**	**IMS CORE**
IMS-2930	The UE SHOULD support MSRP as specified in 3GPP TS 24.247 [15], Section 9.	**STD**	**IMS CORE**

5.3 IMS CORE

5.3.1 GENERAL REQUIREMENTS

REQ. ID	REQUIREMENT	TYPE	FEATURE
IMS-0230	The UE MUST manage the IMS signalling (e.g. SIP, XCAP, SDP) as defined by 3GPP TS 24.229 [5] in Sections 5, 6 and 7 and provide an abstraction of this functionality to connected applications through the appropriate API.	NEW	IMS CORE
IMS-0220	The UE MUST be able to maintain IMS Registration and Sessions automatically (e.g. keep alive according to SIP timers, QoS re-negotiation).	NEW	IMS CORE
IMS-0240	The UE MUST keep track of SIP dialogs, transactions and states.	NEW	IMS CORE
IMS-0250	The UE MUST negotiate and determine codec and media characteristics for session setup based on the local capabilities (IMS-1150) and the media preferences provided by an application at session setup time (IMS-1210).	NEW	IMS CORE
IMS-0251	The UE SHALL support video codec adaptation mechanisms (as defined in TS 23.228 [22] Section 5.11.3.2 & 5.11.3.3 and TS 24.229 [5] Section 6.1.1 and Section 6.1.2) to deal with fluctuation in the underlying layers to provide best possible video presentation.	STD	IMS CORE
IMS-0252	The UE SHALL be able to switch to more robust or less payload intensive video codec (as defined in TS 23.228 [22] Section 5.11.3.2 & 5.11.3.3 and TS 24.229 [5] Section 6.1.1 and Section 6.1.2) when underlying or supporting layers deteriorate, in order to save the connection. UE SHALL switch back to less error tolerant or high payload video codec, when underlying layers conditions improve.	STD	IMS CORE

REQ. ID	REQUIREMENT	TYPE	FEATURE
IMS-0390	The UE MUST release any resources reserved by an application or by a session related to the application when that application exits and/or when individual sessions are terminated.	**NEW**	**IMS CORE**
IMS-0400	The UE MUST be able to handle simultaneous SIP dialogs and transactions.	**STD**	**IMS CORE**

5.3.2 REGISTRY AND UICC

REQ. ID	REQUIREMENT	TYPE	FEATURE
IMS-2940	The UE MUST be able to generate the user identity for registering purposes from USIM as specified in 3GPP TS 23.003 [16], Sections 13.3 and 13.4.	**STD**	**IMS CORE**
IMS-2850	The UE MUST be aware whether the UICC inserted has the capabilities needed for performing the IMS registration procedure (i.e. UICC with an ISIM application as specified in TS 31.103 [17] or with an USIM application as specified in TS 31.102 [18]).	**NEW**	**IMS CORE**
IMS-2950	If ISIM application is present on the UICC the UE MUST use the configured user identities for registering purposes from ISIM as specified in 3GPP TS 23.003 [16] Section 13.	**STD**	**IMS CORE**
IMS-0260	The UE MUST support the IMS-AKA procedure to perform authenticated register to an IMS Core network as specified in TS 33.203 [19] Section 6.1.	**STD**	**IMS CORE**

REQ. ID	REQUIREMENT	TYPE	FEATURE
IMS-2960	The UE MUST support early IMS Authentication as defined in TR 33.978 [20] Section 6.2.3.1. However, it SHALL be possible for the operator to disable this feature on the UE.[3]	**STD**	**IMS CORE**
IMS-2970	When early IMS Authentication is enabled, if a SIM is in use in the UE (i.e. there is no USIM or ISIM application) the UE MUST use early IMS for authentication purposes (see IMS-0310).	**STD**	**IMS CORE**
IMS-2980	When early IMS Authentication is enabled, if USIM or ISIM (or both) are in use in the UE, the UE MUST first attempt to use IMS AKA (see IMS-0300 and IMS-0340).	**STD**	**IMS CORE**
IMS-2990	When early IMS Authentication is enabled, in case the attempt described in IMS-0330 fails as described in section 8.6 of 3GPP TS 34.229 [21] the UE MUST be able to perform the mechanisms for initial registration for combined IMS support and early IMS security against a network with early IMS support only as defined in that specification.	**STD**	**IMS CORE**

5.3.3 USE OF SIP AND SDP

REQ. ID	REQUIREMENT	TYPE	FEATURE
IMS-3000	The UE MUST support IMS Procedures as defined in TS 24.229 [5] Annex A.	**STD**	**IMS CORE**
IMS-0360	The UE MUST support the timers and SIP Timers values defined in TS 24.229 [5] Section 7.7 for 2G and 3G.	**STD**	**IMS CORE**

[3] When ISIM is not used, the early IMS Authentication will be enabled in the UE.

REQ. ID	REQUIREMENT	TYPE	FEATURE
IMS-3010	The UE SHOULD support QoS pre-conditions as defined in TS 24.229 [5] (Sections 5.1.3, 5.1.4, 6.1.2 and 6.1.3).	**STD**	**IMS CORE**
IMS-0410	The UE SHALL support the P-headers as specified in TS 24.229 [5] Section 7.2A.	**STD**	**IMS CORE**
IMS-3020	The UE MUST be able to provide the basic mechanism "SIP specific event notification" as defined in RFC 3265 [23] in order to allow use of an event package not yet standardised or provided through IMS standards.	**STD / NEW**	**IMS CORE**
IMS-3030	The UE SHOULD implement the mapping for SDP to 3GPP QoS parameters as defined in TS 29.213 [24] Section 6.	**STD**	**IMS CORE**

5.3.4 EMERGENCY SERVICE

REQ. ID	REQUIREMENT	TYPE	FEATURE
IMS-3040	The UE SHOULD [4] support the Emergency Service as specified in TS 24.229 [5] (Section 5.1.6).	**STD**	**IMS CORE**
IMS-0461	If the UE supports Emergency Service over IMS, it MUST be capable of recognising operator -configured emergency numbers.	**NEW**	**IMS CORE**
IMS-0462	If the UE supports Emergency Service over IMS, it MUST be capable of making a voice call over IMS, i.e. establishing a Voice over IP session.	**NEW**	**IMS CORE**

[4] Subject to regional regulatory requirements

REQ. ID	REQUIREMENT	TYPE	FEATURE
IMS-0463	If the UE supports Emergency Service over IMS, it SHOULD support conveying its geographical location information (e.g. GPS coordinates) in the emergency session establishment request (if location information is available)[5]. NOTE: Depending on the system used to determine geographical location information, additional functionality such as support for a GPS receiver might need to be implemented in the UE. This is currently out of the scope of this specification.	**NEW**	**IMS CORE**

5.4 VOICE CALL CONTINUITY

This section describes VCC Functional Requirements. Requirements for VCC configuration are defined in the DM and Configuration section 5.8.1.

REQ. ID	REQUIREMENT	TYPE	FEATURE
IMS-3050	The UE SHOULD support VCC as specified in TS 24.206 [25]	**STD**	**VCC**

5.5 NAT TRAVERSAL

This section describes NAT Traversal Functional Requirements. Requirements for NAT Traversal configuration are defined in the DM and Configuration section 5.8.1.

REQ. ID	REQUIREMENT	TYPE	FEATURE
IMS-3060	If the UE supports accessing IMS using a non-3GPP access network (using the IP address of the local private network) the UE SHOULD support UE managed NAT Traversal mechanisms as specified in TS 24.229 [5] annex K.	**STD**	**NAT TRAVERSAL**

[5] Subject to regional regulatory requirements

REQ. ID	REQUIREMENT	TYPE	FEATURE
IMS-3070	The UE MUST know whether there is a NAT between the UE and the IMS domain or not and choose whether the mechanisms defined in IMS-0430 should be used or not.	STD	NAT TRAVERSAL
IMS-3080	When a NAT is not present between the UE and the IMS domain, the UE SHOULD NOT perform keep-alive procedures.	STD	NAT TRAVERSAL

5.6 IMS APPLICATION ENVIRONMENT

This section describes the functionality expected from IMS Terminals regarding the integration of IMS applications with the User Equipment (UE)

The UE will be responsible for controlling IMS capable applications in order to notify them about incoming messages, capabilities changes or new IMS applications installed. It shall be also responsible for controlling the IMS registration on the network taking into account the capabilities supported by the applications and the different user identities.

This section uses two different registry concepts for applications that are explained herein for the sake of clarity:

- Registry on the Terminal: This is the process by which an application indicates to the terminal that it is available and which are it's Media Feature Tags. This process is entirely done on the terminal and does not require any interaction with the network.

- Registry on the network: This is the process by which the Terminal registers the application media feature tags in the network. It is important to stress that is not the application but the Media Feature Tags that are registered in the network.

Requirements for IMS Application Environment configuration are defined in the DM and Configuration section 5.8.2.

5.6.1 UE REGISTRY AND APPLICATION CONFIGURATION

REQ. ID	REQUIREMENT	TYPE	FEATURE

REQ. ID	REQUIREMENT	TYPE	FEATURE
IMS-0430	The UE MUST offer a mechanism to select which public user identity the UE should use when registering with the IMS network.	NEW	APPLICATION ENVIRONMENT
IMS-0440	The user MUST be able to configure the timing of when the UE registers with the IMS network. At least the following options MUST be supported: – IMS network registration on Terminal switch-on: The general IMS registration is performed automatically after Terminal switch-on. – Manual IMS network registration: The IMS registration on the network is not started automatically and the end-user is the responsible for launching this process.	NEW	APPLICATION ENVIRONMENT
IMS-0450	The UE MUST provide a mechanism for allowing IMS applications to Register/Unregister on the Terminal.	NEW	APPLICATION ENVIRONMENT
IMS-0460	The UE MUST offer a mechanism for applications to request to register (e.g. media feature tags) with the existing registered public user identity (see IMS-0480) or a new public user identity.	NEW	APPLICATION ENVIRONMENT

REQ. ID	REQUIREMENT	TYPE	FEATURE
IMS-0470	The UE MUST offer a mechanism in order to allow the application to configure the timing of when its features (media feature tags, ICSIs, IARIs and etc.) will be registered in the IMS network: – On Terminal IMS network registration: The features linked to the application will be registered in the IMS network whenever the Terminal registers in the IMS network (even if the application is not started) as defined in requirement IMS-0490. – On application start: The features linked to the application will be registered in the IMS network when the application is started. They should be also un-registered when the application is stopped. This choice will be stored in the application's 'media feature tag registry' configuration defined in section 5.6.1.1.	NEW	APPLICATION ENVIRONMENT
IMS-0480	The UE MUST offer a mechanism in order to allow an Application to select which media feature tags (including ICSIs and IARIs) that the UE use when registering its features to the IMS network from the application's "media feature tags" based on the 'media feature tags registry' configuration defined in section 5.6.1.1.	NEW	APPLICATION ENVIRONMENT

REQ. ID	REQUIREMENT	TYPE	FEATURE
IMS-0490	The UE MUST offer a mechanism in order to allow an application to set its start functions upon installation to the Terminal: – Automatic start: The application is automatically started whenever the Terminal is started up. – Manual start: The application is started manually by the user This choice will be stored in the application's 'start functions' configuration defined in section 5.6.1.1.	NEW	APPLICATION ENVIRONMENT
IMS-0500	The UE MUST offer a mechanism in order to allow the user to be able to select the start mechanism upon installation or configuration time of the application (see IMS-0540) for each application.	NEW	APPLICATION ENVIRONMENT
IMS-0510	The UE MUST offer a mechanism in order to allow the user to configure an application's auto-execution behaviour (behaviour when an incoming message is directed to the application and it is not executing): – Automatic Execution: Application is started automatically and incoming messages are accepted without user confirmation. – User Confirmed Execution: The user is prompted whether he wishes to start the application and accept the incoming messages or not. – Reject Execution: The application is not started and incoming messages are rejected without user interaction. This choice will be stored in the application's 'auto-execution' configuration defined in section 5.6.1.1.	New	APPLICATION ENVIRONMENT

5.6.1.1 Application Configuration Information

The following table describes the configuration information available for each IMS application installed on the UE:

PARAMETER	DESCRIPTION
PUBLIC USER IDENTITY	The public user identity that takes the form of either SIP URL (as defined in RFC 2543 [26] and RFC 2396 [27]) or E.164 numbers.
MEDIA FEATURE TAGS	A list with all the media feature tags that represent the media capabilities or properties supported by the application. Their syntax will be specified for each service (e.g. OMA PoC +g.oma.poc, CSI +g.3gpp.cs-audio or +g.3gpp.cs-video) and compliant with registration procedure defined by RFC 2506 [28].
MEDIA FEATURE TAGS REGISTRATION	Specifies when the **capabilities supported by the application should be registered on the IMS Network**. Possible values are: – Application Capability Registration on general IMS network registration: The media feature tags (including Application Reference Media Feature Tags) linked to the application will be registered in the IMS network whenever the Terminal registers with the IMS network (even if the application is not executing). – Application Capability Registration on application start: The media feature tags (including Application Reference Media Feature Tags) linked to the application will be registered in the IMS network when the application is executed. They should be also un-registered when the application is terminated.

PARAMETER	DESCRIPTION
START FUNCTIONS (UPON INSTALLATION TO THE TERMINAL)	Identifies whether the **application should be started when the handset is started up** (see requirement IMS-0540). The possible values are: – Automatic start: The application is automatically started whenever the Terminal is started up. – Manual start: The application is started manually by the user
AUTO-EXECUTION (UPON AN INCOMING SIP MESSAGE)	Specifies whether a **non-executing application should be started whenever an incoming message is directed to it** (see requirement IMS-0560). The possible values are: – Automatic Execution: The application is started automatically without user confirmation. – User Confirmed Execution: The user is prompted whether he wishes to start the application or not. – Reject Execution: The application is not started.

5.6.2 IMS APPLICATION INTEGRATION

REQ. ID	REQUIREMENT	TYPE	FEATURE
IMS-3090	The following local capabilities of the Terminal MUST be accessible to the UE in order to negotiate sessions (see also IMS-1150): – Codecs supported, – Cameras characteristics, – Screen Resolution.	NEW	APPLICATION ENVIRONMENT
IMS-0530	The UE MUST be aware of the updates to the local capabilities described in requirement IMS-0570 (e.g. installation of a new codec).	NEW	APPLICATION ENVIRONMENT

5.6.3 Reporting Features Supported By Applications

Req. ID	Requirement	Type	Feature
IMS-0540	The UE MUST be able to report supported application features (i.e. Media Feature Tags, ICSIs and IARIs) on the IMS network using the public user identity selected for the application (from IMS-0510) and according to the registration procedures in TS 24.229 [5] Section 5.1.1.	New	Application Environment
IMS-0550	The UE MUST report to the IMS network the features (i.e. Media Feature Tags, ICSIs and IARIs) supported by Applications "Registered on the Terminal" according to its configuration as defined in section 5.6.1.1. The UE MUST provide different methods for when an application registers with the IMS network (IMS-0530).	New	Application Environment
IMS-0560	The UE MUST offer a mechanism (and mechanism configuration) to applications in order to allow them to include information to be delivered in the "Feature Media Tag" in all the REGISTER / OPTIONS / INVITE / PUBLISH / SUBSCRIBE messages sent by Terminal.	New	Application Environment
IMS-3100	The UE MUST support the "ICSI" and "IARI" mechanisms as defined in 3GPP TS 24.229 [5] 7.2A.8 and 7.2A.9 for providing a feature set that expresses the identification of the communication service (i.e. during registration procedure and service requests).	New	Application Environment

5.6.4 REDIRECTING IMS MESSAGES TO APPLICATIONS

REQ. ID	REQUIREMENT	TYPE	FEATURE
IMS-0570	The UE MUST provide a mechanism (and mechanism configuration) that permits identification of the IMS application to which the incoming requests are directed.	**NEW**	**APPLICATION ENVIRONMENT**
IMS-0651	For requests containing an Accept-Contact header field with a g.3gpp.app_ref feature tag, the UE MUST invoke the IMS application that is the best match for the ICSI value and, if included, for the IARI value contained in the g.3gpp.app_ref feature tag as specified in TS 24.229 [5] Section 5.1.2A.2. [6]	**STD**	**APPLICATION ENVIRONMENT**
IMS-0580	For requests not containing an Accept-Contact header field and containing a g.3gpp.app_ref feature tag the UE MUST support all of the following matching criteria for identifying the target application of an incoming request: • Media-Type, • Feature Tag, • SDP Fields.	**NEW**	**APPLICATION ENVIRONMENT**
IMS-0590	The UE MUST provide a mechanism (and mechanism configuration) to choose the default application for incoming requests. If more than one application can accept an undirected incoming request (i.e. request not linked to a particular application) the UE will apply the application priorities defined in IMS-0700 for message routing.	**NEW**	**APPLICATION ENVIRONMENT**

[6] The UE can receive multiple Accept-Contact header fields containing g.3gpp.app_ref feature tags. In this case it is up to the implementation which of the multiple ICSI values or IARI values it takes action on.

REQ. ID	REQUIREMENT	TYPE	FEATURE
IMS-0600	The UE MUST route an incoming request to just one application.	NEW	APPLICATION ENVIRONMENT
IMS-0610	The UE MUST provide a mechanism (in accordance with the configuration defined in IMS-0560) to allow the auto-execution of an application (as defined for the application in section 5.6.1.1) when an incoming request is routed to that application and that application is not currently running.	NEW	APPLICATION ENVIRONMENT
IMS-0620	Whenever an incoming request can be delivered to more than one application the UE SHALL: – Deliver it to the application as configured (if any), – If there is no configuration, decide which is the most suitable application using the UE default behaviour.	NEW	APPLICATION ENVIRONMENT

5.6.5 QUERYING REMOTE TERMINAL CAPABILITIES

REQ. ID	REQUIREMENT	TYPE	FEATURE
IMS-0630	The UE MUST support the functionality to query remote Terminal capabilities according to RFC 3840 [29] and the SIP OPTIONS message.	STD	APPLICATION ENVIRONMENT
IMS-0640	The UE MUST support the functionality to convey its capabilities according to RFC 3840 [29].	STD	APPLICATION ENVIRONMENT

REQ. ID	REQUIREMENT	TYPE	FEATURE
IMS-0650	The UE MUST support the mechanisms defined in RFC 3841 [30] for providing a feature set that expresses the Terminal's preferences on the characteristics of the UA that is to be reached and specific request handling directives for a server.	STD	APPLICATION ENVIRONMENT

5.7 IMS SERVICE ENABLERS

This section describes the requirements that apply to the relevant standard service enablers in an IMS capable Terminal. The requirements for a specific feature will only apply when that feature is supported.

This section describes the minimum requirements for the service enablers available at the time of publication. It is anticipated that the list of service enablers required will evolve in future versions of this document as they become standardised

5.7.1 PoC

This section describes PoC Functional Requirements. Requirements for PoC configuration are defined in the DM and Configuration section 5.8.1.

REQ. ID	REQUIREMENT	TYPE	FEATURE	VERSION APPLICABLE
IMS-0660	The UE MUST support Push-to-talk Over Cellular v1.0 as specified by OMA [3].	**STD**	**PoC**	**V1.0**
IMS-3110	The UE MUST support Push-to-talk Over Cellular v2.0 as specified by OMA [31]	**STD**	**PoC**	**V2.0**
IMS-3120	The PoC client MUST be integrated with the presence functionality.	**STD**	**PoC**	**V1.0** **V2.0**
IMS-3130	The UE MUST support new media types other than PoC Speech, specifically audio streaming, video streaming and discrete media transfer as specified by OMA [31].	**STD**	**PoC**	**V2.0**
IMS-3140	The UE MUST support Group Advertisement as specified by OMA [3].	**STD**	**PoC**	**V1.0** **V2.0**
IMS-3150	The UE SHOULD support Pre-established Sessions as specified by OMA [3].	**STD**	**PoC**	**V1.0** **V2.0**

REQ. ID	REQUIREMENT	TYPE	FEATURE	VERSION APPLICABLE
IMS-3160	The UE MUST support Sender Identification as specified by OMA [31].	**STD**	**PoC**	**V2.0**
IMS-3170	The UE MUST support Browser Based PoC Client Invocation as specified by OMA [31].	**STD**	**PoC**	**V2.0**
IMS-3180	The UE SHOULD support Simultaneous PoC Sessions as specified by OMA [3].	**STD**	**PoC**	**V1.0** **V2.0**
IMS-3190	The UE SHOULD support PoC Sessions with Multiple PoC Groups as specified by OMA [31].	**STD**	**PoC**	**V2.0**
IMS-3200	The UE SHOULD support PoC Session establishment requests with Media contents as specified by OMA [31].	**STD**	**PoC**	**V2.0**
IMS-3210	The UE SHOULD support PoC Box functionality as specified by OMA [37].	**STD**	**PoC**	**V2.0**
IMS-3220	The UE SHOULD support PoC Dispatcher functionality as specified by OMA [37].	**STD**	**PoC**	**V2.0**

5.7.2 OMA PRESENCE SIMPLE

This section describes presence SIMPLE Functional Requirements. Requirements for presence SIMPLE configuration are defined in the DM and Configuration section 5.8.1.

REQ. ID	REQUIREMENT	TYPE	FEATURE	VERSION APPLICABLE
IMS-0730	The UE MUST support OMA Presence SIMPLE v1.1 (SIP for Instant Messaging and Leveraging Extensions) as specified by OMA [32].	STD	PRESENCE	V1.1
IMS-0871	The UE SHOULD follow the Implementation Guidelines for OMA Presence SIMPLE v1.1 [48]	STD	PRESENCE	V1.1
IMS-0731	The UE MUST support the functionality to publish Service IDs according to the presence mechanism defined in the OMNA presence <service-description> Registry: http://www.openmobilealliance.org/Technical/omna/omna-prs-PidfSvcDesc-registry.aspx. This requirement only applies for these services that have Service IDs registered in OMNA.	STD	PRESENCE	V1.1

5.7.3 XML DOCUMENT MANAGEMENT

This section describes XDM Functional Requirements. Requirements for XDM configuration are defined in the DM and Configuration section 5.8.1.

REQ. ID	REQUIREMENT	TYPE	FEATURE	VERSION APPLICABLE

REQ. ID	REQUIREMENT	TYPE	FEATURE	VERSION APPLICABLE
IMS-3230	The UE MUST support OMA-XDM v1.1 (XML Document Management) as specified in [33].	**STD**	**XDM**	**V1.1**
IMS-0760	The UE MUST support OMA-XDM v2.0 (XML Document Management) as specified in [34].	**STD**	**XDM**	**V2.0**
IMS-0891	The UE SHOULD follow the Implementation Guidelines for OMA XDM v1.1 [49].	**STD**	**XDM**	**V1.1**

5.7.4 OMA SIMPLE IM

This section describes IM Functional Requirements. Requirements for IM configuration are defined in the DM and Configuration section 5.8.1.

REQ. ID	REQUIREMENT	TYPE	FEATURE	VERSION APPLICABLE
IMS-0770	The UE MUST support Instant Messaging v1.0 as specified by OMA [35].	**STD**	**IM**	**V1.0**

5.7.5 VIDEO-SHARE

This section describes Video Share Functional Requirements. Requirements for Video Share configuration are defined in the DM and Configuration section 5.8.1.

REQ. ID	REQUIREMENT	TYPE	FEATURE
IMS-3230	The UE MUST allow simultaneous CS and PS communications. NOTE: This requirement overrides IMS-0040.	**STD**	**VIDEO-SHARE**

REQ. ID	REQUIREMENT	TYPE	FEATURE
IMS-0810	A UE supporting video-share MUST use the capability query procedures defined in IMS-0710 to find out if the called party supports video-sharing and supports simultaneous CS and PS over that radio technology, and must do so each time that UE has established a CS voice call (see requirement IMS-0040) and has registered to IMS network.	STD	VIDEO-SHARE
IMS-0931	The UE MUST fulfil the "GSMA Video Share Interoperability Specification v1.1 (IR.74)" [50].	STD	VIDEO-SHARE
IMS-0932	The UE SHOULD follow the "GSMA Video Share Service Definition v.2.0 (SE.41)" [51].	STD	VIDEO-SHARE
IMS-0933	The UE SHOULD follow the IMTC Interoperability specification [56].	STD	VIDEO-SHARE

5.7.6 IMAGE SHARE

REQ. ID	REQUIREMENT	TYPE	FEATURE
IMS-3240	The UE MUST fulfil the "GSMA Image Share interoperability specifications (IR.79)" [36].	STD	IMAGE-SHARE
IMS-0941	The UE MUST allow simultaneous CS and PS communications. NOTE: This requirement overrides IMS-0040.	STD	IMAGE-SHARE

REQ. ID	REQUIREMENT	TYPE	FEATURE
IMS-0942	A UE supporting image-share MUST use the capability query procedures defined in IMS-0710 to find out whether called party supports image-share each time it has established a CS voice call over a radio technology in which it supports simultaneous CS and PS (see requirement IMS-0040) and has registered to IMS network.	STD	IMAGE-SHARE

5.7.7 SIP BASED PUSH

5.7.7.1 Introduction

Push-based service enablers in OMA define the delivery of content to a mobile Terminal utilising push methods. The OMA SIP Push 1.0 enabler ("SIP Push") extends the architectural context of such push methods to SIP-based environments. SIP Push does not define a service enabler by itself, rather it defines how service enablers can use SIP methods for push-based content delivery. Thus the specific client requirements for implementations of SIP Push are not driven by SIP Push itself, but rather by the SIP Push referencing enablers. However, specific client requirements of SIP Push can be described here, as they will be common to any enabler implementation that leverages SIP Push.

SIP Push defines functions of Push Sender Agents and Push Receiver Agents. To implement the SIP Push specification, it is necessary that the Push Sender and Receiver Agents interface with a SIP/IP Core network. An example of SIP/IP Core network definitions are 3GPP IMS and 3GPP2 MMD networks.

The scope of SIP Push includes:

- Push Receiver Agent registration performs SIP REGISTER with SIP/IP Core network.
- Service and Application addressing at the SIP layer, using 3GPP ICSI/IARI or enabler-specific methods (e.g. feature tags).
- Enabler-specific addressing e.g. support for OMA's Push Application ID based model of message routing to legacy enabler clients.
- Use of standard SIP messaging procedures and extensions,
    - Page-mode Messaging, which relies upon SIP MESSAGE.

    - Session-mode Messaging using Event Notification, which relies upon SIP SUBSCRIBE/NOTIFY.
    - Session-mode Messaging using INVITE/MSRP, which relies upon SIP INVITE/MSRP.
- Capability negotiation, through which the Push Receiver Agent and Push Sender Agent become aware of the other's capabilities.
- Client addressing by Public SIP URI and Globally Routable User Agent URIs (GRUU).
- Client identity trust via use of P-Asserted-Identity.

SIP Push focuses on the relationship between the Push Sender Agent and the Push Receiver Agent. This relationship begins with the Push Sender Agent becoming aware of the presence of the Push Receiver Agent and Terminal capabilities through the Push Receiver Agent's registration with the SIP/IP Core network. Whilst optionally using the SIPPING Configuration Framework to deliver Terminal characteristics in SIP SUBSCRIBE, e.g. OMA User Agent Profile reference or Terminal make/model.

To provide options and methods supporting content delivery under various end-to-end service requirements, SIP Push defines three push methods:

- Page-mode messaging: The MESSAGE method defined in RFC3428 [37] is an extension to SIP that allows the transfer of messages to the client. Since the MESSAGE request is an extension to SIP, it inherits all the request routing and security features of that protocol. The MESSAGE request may carry the content in the form of MIME body parts, or per RFC4483 [38] may indirectly reference the content. MESSAGE requests do not themselves initiate a SIP dialog; under normal usage each MESSAGE stands alone, much like pager messages. Thus, each MESSAGE request is independent and no session states are stored in the system. Because the content is delivered as the message body of the SIP MESSAGE, the content is limited by the maximum size of SIP MESSAGE requests.
- Session-mode Messaging (Event Notification): The SIP-based event subscription mechanism described in RFC3265 [23] uses the SIP SUBSCRIBE and SIP NOTIFY methods to allow for asynchronous notification of events during the duration of a subscription. Once created, a subscription provides a dialog between the Push Sender Agent and the Push Receiver Agent, through which the Push Sender Agent can deliver content using the SIP NOTIFY method. As with SIP MESSAGE, the content is delivered as the message body of the SIP NOTIFY, thus the content is limited by the maximum size of SIP NOTIFY requests.
- Session-mode messaging (INVITE/MSRP) avoids the limitations on pushed content size imposed by SIP MESSAGE and SIP NOTIFY. To

allow arbitrarily large messages, the content is carried by MSRP defined by RFC 4975 [39]. To use MSRP, a SIP session is established between the Push Sender Agent and Push Receiver Agent via the SIP INVITE method, with MSRP as the media component. The SIP session can be used to transmit multiple messages, according to the needs of the implementing service.

5.7.7.2 Key Terminal Requirements

The following table summarises the client static conformance requirements for SIP Push (draft: not yet finalized). As shown, there are two fundamental requirements (mandated):

- Ability to receive pushed content, by at least one of the defined methods.
- Ability to register with a SIP/IP Core network.

Beyond that, the detailed requirements of each optional feature become mandatory when the optional feature is claimed to be supported. The specific implementing enabler will define which optional features are mandatory, in the particular context as required by the needs of the specific enabler.

REQ. ID	REQUIREMENT	TYPE	FEATURE
IMS-0941	The UE MUST support the reception of push content from the Push Sender Agent by at least one of the following methods: • Reception of page mode messaging. • Subscription to push. • SIP INVITE & MSRP methods.	**STD**	**SIP PUSH**
IMS-0942	The UE acting as a Push Receiver Agent SHALL be able to register, re-register and de-register to the SIP/IP Core network according to rules and procedures of RFC 3261 with the clarifications in Section 6.1 of [57].	**STD**	**SIP PUSH**

5.7.8 MULTIMEDIA TELEPHONY (MMTEL)

3GPP R7 defines multimedia telephony and supplementary service as part of one specification pointing out to the relevant ETSI specifications:

REQ. ID	REQUIREMENT	TYPE	FEATURE
IMS-3250	The UE MUST support IMS multimedia telephony communication service and supplementary services as specified by 3GPP TS 24.173 [40].	**STD**	**MMTEL**

5.7.8.1 Codec selection

REQ. ID	REQUIREMENT	TYPE	FEATURE
IMS-0951	The UE MUST support the media formats and codecs defined in 3GPP TS 26.141 [41].	**STD**	**MMTEL**

5.8 DEVICE MANAGEMENT & CONFIGURATION

IMS offers the possibility to provide new and complex services to the end users. These IMS services usually require the UE to be flexible enough to be configured in different manners. Identifying which is the flexibility required (i.e. which are the required configuration parameters) is crucial for the success of IMS.

However, because of the increasing complexity of mobile Terminals, it is not necessary a simple task for the end-user to configure Terminal services and applications. Suitable technologies should be available in order to allow the operators to retrieve the configuration of the Terminal OTA and in the case of a detected problem, perform OTA corrective actions.

This section defines what are the configuration parameters related to IMS Services and which of them should be exposed in the DM Tree in order to allow IMS remote management. Access to the DM Tree will be restricted depending on the DM Tree ACLs as defined by OMA DM v1.2.

REQ. ID	REQUIREMENT	TYPE	FEATURE
IMS-0060	The UE MUST support OMA DM v1.2 [42].	**STD**	**IMS CORE**

5.8.1 MANAGEMENT OF THE IMS CORE AND SERVICE ENABLERS

The IMS Core and Service Enablers require several parameters to be properly configured. This section defines the configuration information that should be exposed in the UE DM Tree.

REQ. ID	REQUIREMENT	TYPE	FEATURE
IMS-0320	The UE MUST support the management object for IMS as defined in TS 24.167 [43].	**STD**	**IMS CORE**
IMS-3260	The UE SHOULD expose in the DM Tree a list with all the registered media-feature-tags.[7]	**NEW**	**IMS CORE**
IMS-3270	The UE SHOULD expose in the DM Tree a configuration parameter that allows activation/deactivation of SIP Compression.	**NEW**	**IMS CORE**
IMS-3280	The UE SHOULD expose in the DM Tree a configuration parameter that determines the preferred IP addressing mode (IPv4 or IPv6).	**NEW**	**IMS CORE**
IMS-3290	If NAT Traversal is supported, the UE SHOULD expose the STUN server address in the DM Tree.	**NEW**	**NAT TRAVERSAL**
IMS-3300	If NAT Traversal is supported the UE SHOULD expose in the DM Tree the STUN relay server address.	**NEW**	**NAT TRAVERSAL**

[7] There is no standardised MO including this parameter at the time of publication.

REQ. ID	REQUIREMENT	TYPE	FEATURE
IMS-0680	If the UE supports PoC, then it MUST support the PoC Management Object as specified by OMA [3] (Control Plane Document – Annex B).	**STD**	**POC**
IMS-0750	If the UE supports OMA presence SIMPLE, then it MUST support the presence Simple Management Object as defined specified by OMA [52]).	**STD**	**PRESENCE**
IMS-0790	If the UE supports OMA SIMPLE IM, then it MUST support the IM Management Object as defined specified by OMA [35] (Annex I).	**STD**	**IM**
IMS-3310	If the UE supports OMA XDM it MUST support the OMA Management Object for XML Document Management as defined in [53]	**NEW**	**XDM**
IMS-3320	The video-share configuration parameters SHOULD be exposed in the DM Tree	**NEW**	**VIDEO-SHARE**
IMS-3330	If VCC feature is supported the UE MUST support the Communication Continuity management object as defined in TS 24.216 [44].	**STD**	**VCC**

5.8.2 MANAGEMENT OF APPLICATION ENVIRONMENT

Section 5.6.1.1 describes a set of requirements that define the parameters which specify the behaviour of each IMS Application Registered in the Terminal. This section defines a set of requirements which specify the exposure of that data in the Terminal DM Tree.

REQ. ID	REQUIREMENT	TYPE	FEATURE
IMS-3340	For each IMS application registered in the UE, the DM Tree MAY expose to a remote management server the public user identities linked to it.	**NEW**	**APPLICATION ENVIRONMENT**

REQ. ID	REQUIREMENT	TYPE	FEATURE
IMS-3350	For each IMS application registered in the UE, the DM Tree MAY expose to a remote management server the media feature tags supported by the application.	NEW	APPLICATION ENVIRONMENT
IMS-3360	For each IMS application registered in the UE, the DM Tree MAY expose to a remote management server the parameter that defines the moment in which the related media feature tags will be registered on the network (see IMS-0520).	NEW	APPLICATION ENVIRONMENT
IMS-3370	For each IMS application registered in the UE, the DM Tree MAY expose to a remote management server the parameter that defines the moment in which the application will be started (see IMS-0540).	NEW	APPLICATION ENVIRONMENT
IMS-3380	For each IMS application registered in the UE, the DM Tree MAY expose to a remote management server the parameter that defines the auto-execution configuration upon an incoming SIP message (see IMS-0560).	NEW	APPLICATION ENVIRONMENT

6 APPLICATION PROGRAMMING INTERFACE REQUIREMENTS

This chapter identifies which IMS functionality defined in the previous sections should be exposed to Terminal applications.

6.1 GENERIC API REQUIREMENTS

REQ. ID	REQUIREMENT	TYPE	FEATURE
IMS-0820	Concurrent use of the APIs MUST be possible (i.e. applications should be able to use the API for getting the presence status of a contact simultaneously).	NEW	IMS CORE
IMS-0830	The UE MUST offer an API that allows an application to get a list of the local capabilities supported by the Terminal as defined in IMS-0570.	NEW	IMS CORE
IMS-1151	The UE MUST offer an API that allows an application to discover the supported IMS Service Enablers (i.e. PoC, presence SIMPLE, IM and XML Document Management).	NEW	IMS CORE
IMS-0840	The UE MUST offer an API that allows an application to get a list of all the media feature tags registered on the Terminal.	NEW	IMS CORE
IMS-0850	The UE SHOULD offer an API that allows an application to subscribe to the Terminal to receive events about changes on local capabilities as defined in IMS-0590.	NEW	IMS CORE

6.2 CORE API

6.2.1 SESSION API

6.2.1.1 Session Media Requirements

REQ. ID	REQUIREMENT	TYPE	FEATURE

REQ. ID	REQUIREMENT	TYPE	FEATURE
IMS-0900	The UE MUST offer an API to allow an application to create a media stream to be used during an IMS session.	NEW	IMS CORE
IMS-0910	The UE MUST offer an API that allows applications to send media through a packet media connection.	NEW	IMS CORE
IMS-0920	The UE MUST offer an API that informs an application whenever data is received through a packet media connection.	NEW	IMS CORE

6.2.1.2 Originating Endpoint Session Management Requirements

REQ. ID	REQUIREMENT	TYPE	FEATURE
IMS-0930	The UE MUST offer an API to allow an application to setup an IMS Session to a remote Terminal endpoint (TS 24.229 [5], Section 5.1.2A & 6.1), (TS 24.247 [15], Section 8.2.1).	NEW	IMS CORE
IMS-0940	The UE SHOULD offer an API to allow an application to monitor the status of the ongoing session setup from the IMS Framework (TS 24.229 [5], Section A.2.1.4.1).	NEW	IMS CORE
IMS-0950	In order for the API to setup an IMS session (IMS-0930), the API SHOULD offer the option to request that the caller's identification is withheld from the called party (TS 24.229 [5], Section 5.1.2A).	NEW	IMS CORE
IMS-0960	The UE MUST offer an API to allow an application to cancel a session setup (TS 24.229 [5], Section A.2.1.4.4).	NEW	IMS CORE

6.2.1.3 Terminating Endpoint Session Management Requirements

REQ. ID	REQUIREMENT	TYPE	FEATURE
IMS-0970	The UE MUST offer an API to allow the destination application to accept an incoming call (from the network) (TS 24.229 [5], Section A.2.1.4.1).	NEW	IMS CORE
IMS-0980	The UE MUST offer an API to allow the destination application to reject an incoming call (from the network) (TS 24.229 [5], Section A.2.1.4.1).	NEW	IMS CORE
IMS-0990	The UE MUST offer an API to allow the destination application to redirect an incoming call (from the network) (TS 24.229 [5], Section A.2.1.4.1).	NEW	IMS CORE

6.2.1.4 General Session Management Requirements

REQ. ID	REQUIREMENT	TYPE	FEATURE
IMS-3390	The UE SHOULD offer an API to allow the application to request that a session is transferred to another Terminal (TS 23.228 [22], Section 5.11.6 and TS 24.229 [5], Section A.2.1.4.11).	NEW	IMS CORE
IMS-1010	The UE MUST offer an API to allow the application to terminate a session (TS 24.229 [5], Section A.2.2.4.3).	NEW	IMS CORE
IMS-1020	The UE MUST offer an API that allows applications to receive events that inform that a session has been terminated (TS 24.229 [5], Section A.2.2.4.3, A.2.1.4.1).	NEW	IMS CORE
IMS-3400	The UE SHOULD offer an API to allow an application to place a session on hold (TS 23.228 [22], Section 5.11.1 and TS 24.229 [5], Section A.2.1.4.14).	NEW	IMS CORE

REQ. ID	REQUIREMENT	TYPE	FEATURE
IMS-3410	The UE SHOULD offer an API that allows applications to receive events that inform the API that a terminating endpoint has confirmed the session is on hold (TS 23.228 [22], Section 5.11.1 and TS 24.229 [5], Section A.2.1.4.14).	NEW	IMS CORE
IMS-3420	The UE SHOULD offer an API to allow an application to resume a session that it has previously placed on hold (TS 23.228 [22], Section 5.11.1 and TS 24.229 [5], Section A.2.1.4.14).	NEW	IMS CORE
IMS-3430	The UE SHOULD offer an API to allow applications to receive events that inform that a terminating endpoint does a session resume (TS 23.228 [22], Section 5.11.1 and TS 24.229 [5], Section A.2.1.4.14).	NEW	IMS CORE
IMS-3440	The UE SHOULD offer an API to allow applications which have requested to resume a session previously put on hold to receive events informing them when a terminating endpoint confirms the session resume through a “200 OK” message (TS 23.228 [22], Section 5.11.1 and TS 24.229 [5], Section A.2.1.4.14).	NEW	IMS CORE
IMS-1080	The UE MUST offer an API to allow an application to negotiate the resources at session setup for a new session (TS 24.229 [5] Section 6.1.2 and A.3 and TS 23.228 [22], Section 5.11.3.1).	NEW	IMS CORE
IMS-3450	The UE SHOULD offer an API to allow an application to re-negotiate the resources in an established session (TS 24.229 [5] Section 6.1.2 and A.3 and TS 23.228 [22], Section 5.11.3.2 and 5.11.3.3).	NEW	IMS CORE

REQ. ID	REQUIREMENT	TYPE	FEATURE
IMS-1100	The UE MUST offer an API to allow an application to add, modify or remove media in an existing session (TS 24.229 [5] Section 6.1.2, A.3 and TS 23.228 [22], Section 5.11.3.4).	NEW	IMS CORE
IMS-1120	The UE MUST offer an API to allow an application to receive events that inform that a session has been modified by a terminating endpoint.	NEW	IMS CORE
IMS-1130	The UE SHOULD offer an API to allow an application to send generic session related control information (RFC-2976 [45]).	NEW	IMS CORE

6.2.2 EVENT FRAMEWORK API

REQ. ID	REQUIREMENT	TYPE	FEATURE
IMS-1140	The UE MUST offer an API that supports service specific event subscription and notification according to RFC-3265 [23].	NEW	IMS CORE
IMS-1150	The UE MUST offer an API that supports publication of any service event state according to RFC-3903 [46].	NEW	IMS CORE

6.2.3 NETWORK API

REQ. ID	REQUIREMENT	TYPE	FEATURE
IMS-1200	The UE MUST offer an API to allow an application to ensure that a session is created satisfying QoS settings (as in IMS-0380).	NEW	IMS CORE
IMS-1210	The UE MUST offer an API to allow an application to receive notifications to inform about networks events (e.g. registration changes).	NEW	IMS CORE

6.2.4 REGISTRATION API

REQ. ID	REQUIREMENT	TYPE	FEATURE
IMS-1220	The UE MUST provide an API to allow an application to indicate to the Terminal that the application is available (i.e. “Registered on the Terminal”).	NEW	IMS CORE
IMS-1230	The UE MUST provide an API to allow an application to indicate to the Terminal that the application is no longer available (i.e. “Not Registered on the Terminal”).	NEW	IMS CORE
IMS-1240	The UE MUST provide an API to allow an application to register its features (i.e. Media Feature Tags, ICSIs and IARIs) to the IMS Network (i.e. “Registered on the Network”).	NEW	IMS CORE
IMS-1250	The UE MUST provide an API to allow an application to de-register its features (i.e. Media Feature Tags, ICSIs and IARIs) from the IMS Network (i.e. “Not Registered on the Network”).	NEW	IMS CORE

6.2.5 INTERROGATING API

REQ. ID	REQUIREMENT	TYPE	FEATURE
IMS-1260	UE MUST offer an API in order to allow an application to interrogate the terminating endpoint capabilities (i.e. via a SIP OPTIONS message - as defined in requirement IMS-0710 or via Presence as in IMS-0731 / IMS-2540).	NEW	IMS CORE

6.3 SERVICE API

This section describes the minimum requirements for the API offered by standard service enablers available at the time of publication of this document. It is anticipated that the list of the standard service enablers required will evolve with time as they become standardised.

6.3.1 OMA PoC API

NOTE: The PoC versions which the requirements in this section refer to are shown in the "Version Applicable" column. If one version is referred, the requirement applies exclusively to implementations of that version. When two versions are referred the requirement applies to both PoC versions.

6.3.1.1 General Requirements

REQ. ID	REQUIREMENT	TYPE	FEATURE	VERSION APPLICABLE
IMS-1450	The UE MUST offer an API to allow applications to change the status of the barring configuration (i.e. bar / unbar) for personal alerts and incoming PoC sessions.	**NEW**	**PoC**	**v1.0** **v2.0**
IMS-1510	The UE MUST offer an API to allow applications to define a change of behaviour when receiving an invitation to a PoC session from a given user (i.e. manual answer/automatic answer).	**NEW**	**PoC**	**v1.0** **v2.0**
IMS-1470	The UE MUST offer an API to allow applications to send instant personal alerts.	**NEW**	**PoC**	**v1.0** **v2.0**
IMS-1480	The UE MUST offer an API to allow applications to send group advertisements.	**NEW**	**PoC**	**v1.0** **v2.0**
IMS-1490	The UE MUST offer an API to allow applications to create a PoC group (chat or pre-arranged).	**NEW**	**PoC**	**v1.0** **v2.0**
IMS-1500	The UE MUST offer an API to allow applications to retrieve the available PoC groups.	**NEW**	**PoC**	**v1.0** **v2.0**

REQ. ID	REQUIREMENT	TYPE	FEATURE	VERSION APPLICABLE
IMS-1460	The UE MUST offer an API to allow applications to retrieve the active PoC sessions.	**NEW**	**PoC**	**v1.0** **v2.0**

6.3.1.2 PoC Sessions Managements

REQ. ID	REQUIREMENT	TYPE	FEATURE	VERSION APPLICABLE
IMS-1520	The UE MUST offer an API to allow applications to get the initiator of a PoC session.	**NEW**	**PoC**	**v1.0** **v2.0**
IMS-1530	The UE MUST offer an API to allow applications to retrieve the PoC session type (i.e. Chat, prearranged or adhoc).	**NEW**	**PoC**	**v1.0** **v2.0**
IMS-3480	The UE MUST offer an API to allow applications to set and retrieve media types negotiated through SDP element in the INVITE message during the PoC session setup. This requirement allows the set up of PoC v2.0 sessions involving a subset of all available media (e.g. a discrete media only session).	**NEW**	**PoC**	**v2.0**
IMS-3490	The UE MUST offer an API to allow applications to set “on hold” status on one of the media exchanged in a PoC session.	**NEW**	**PoC**	**v1.0** **v2.0**
IMS-1550	The UE MUST offer an API to allow applications to get the list of participants of a PoC session.	**NEW**	**PoC**	**v1.0** **v2.0**
IMS-1560	The UE MUST offer an API to allow applications to close a PoC session.	**NEW**	**PoC**	**v1.0** **v2.0**
IMS-1570	The UE MUST offer an API to allow applications to create an ad-hoc PoC Session with a list of URIs.	**NEW**	**PoC**	**v1.0** **v2.0**

REQ. ID	REQUIREMENT	TYPE	FEATURE	VERSION APPLICABLE
IMS-1580	The UE MUST offer an API to allow applications to accept or reject an invitation to participate in an ad-hoc PoC session.	**NEW**	**PoC**	**v1.0** **v2.0**
IMS-1600	The UE MUST offer an API to allow applications to get the users invited to participate in an ad-hoc PoC session. NOTE: This feature is only available to the caller.	**NEW**	**PoC**	**v1.0** **v2.0**
IMS-1610	The UE MUST offer an API to allow applications to get the user role in an ad-hoc PoC session (i.e. caller or callee).	**NEW**	**PoC**	**v1.0** **v2.0**
IMS-1620	The UE MUST offer an API to allow applications to invite additional users to an established ad-hoc PoC session. NOTE: This feature is only available to the caller.	**NEW**	**PoC**	**v1.0** **v2.0**
IMS-1660	The UE MUST offer an API to allow applications to create a Pre-arranged PoC Session with a Group identifier.	**NEW**	**PoC**	**v1.0** **v2.0**
IMS-1670	The UE MUST offer an API to allow applications to accept or reject an invitation to participate in a Pre-arranged PoC session.	**NEW**	**PoC**	**v1.0** **v2.0**
IMS-3490	The UE MUST offer an API to allow applications to get the users invited to participate in a Pre-arranged PoC session. NOTE: This feature is only available to the owner.	**NEW**	**PoC**	**v1.0** **v2.0**

REQ. ID	REQUIREMENT	TYPE	FEATURE	VERSION APPLICABLE
IMS-1710	The UE MUST offer an API to allow applications to invite additional users to an established Pre-arranged PoC session. NOTE: This feature is only available to the owner	**NEW**	**PoC**	**v1.0** **v2.0**
IMS-1700	The UE MUST offer an API to allow applications to get the model of a prearranged PoC session (i.e. one-to-many or one-to-many-to-one/dispatcher).	**NEW**	**PoC**	**v1.0** **v2.0**
IMS-3500	The UE MUST offer an API to allow applications to get the user role in a dispatcher PoC session (i.e. distinguished or ordinary participant).	**NEW**	**PoC**	**v1.0** **v2.0**
IMS-3510	The UE MUST offer an API to allow applications to invite additional users to an ongoing Dispatcher PoC session. NOTE: In 1-to-many-to-1 mode only the distinguished participant may invite another user.	**NEW**	**PoC**	**v1.0** **v2.0**
IMS-1630	The UE MUST offer an API to allow applications to connect a chat PoC Session.	**NEW**	**PoC**	**v1.0** **v2.0**
IMS-1650	The UE MUST offer an API to allow applications to close or close and disconnect a PoC session.	**NEW**	**PoC**	**v1.0** **v2.0**

6.3.1.3 PoC Session Activity

REQ. ID	REQUIREMENT	TYPE	FEATURE	VERSION APPLICABLE

IMS-1750	The UE MUST offer an API to subscribe to receive session progress events (i.e. invite accepted/rejected, join accepted or session terminated) from a PoC Server.	**NEW**	**PoC**	**v1.0** **v2.0**
IMS-1770	The UE MUST offer an API to subscribe to notifications of PoC session participant updates (i.e. whether a user joins or leaves the PoC session).	**NEW**	**PoC**	**v1.0** **v2.0**
IMS-3520	The UE MUST offer an API to allow applications to request media floor control for a specific media requiring floor control mechanism (e.g. PoC Speech, Video Streaming).	**NEW**	**PoC**	**v1.0** **v2.0**
IMS-3530	The UE MUST offer an API to allow applications to acquire the answer (granted, refused) to the media floor request.	**NEW**	**PoC**	**v1.0** **v2.0**
IMS-3540	The UE MUST offer an API to allow applications to get the identity of the user whom is granted the media floor control for a specific media requiring floor control mechanism.	**NEW**	**PoC**	**v1.0** **v2.0**
IMS-3550	The UE MUST offer an API to allow applications to release media floor control for a specific media requiring floor control mechanism (e.g. PoC Speech, Video Streaming).	**NEW**	**PoC**	**v1.0** **v2.0**
IMS-3560	The UE MUST offer an API to allow applications to send streaming contents if media floor control for the specific media is granted.	**NEW**	**PoC**	**v1.0** **v2.0**

IMS-3570	The UE MUST offer an API to allow applications to receive streaming contents.	**NEW**	**PoC**	**v2.0**
IMS-3580	The UE MUST offer an API to allow applications to send discrete media contents (images, text, audio/video clip, etc). Note: no floor control needed to send discrete media.	**NEW**	**PoC**	**v2.0**
IMS-3590	The UE MUST offer an API to allow applications to receive and store discrete media contents (images, text, audio/video clip and etc.).	**NEW**	**PoC**	**v2.0**

6.3.1.4 Out of session PoC Events

REQ. ID	REQUIREMENT	TYPE	FEATURE	VERSION APPLICABLE
IMS-1720	The UE MUST offer an API to subscribe to notifications of incoming PoC session requests.	**NEW**	**PoC**	**v2.0**
IMS-1730	The UE MUST offer an API to subscribe to notifications of incoming instant personal alerts.	**NEW**	**PoC**	**v1.0** **v2.0**
IMS-1740	The UE MUST offer an API to subscribe to notifications of incoming group advertisements.	**NEW**	**PoC**	**v1.0** **v2.0**

6.3.2 OMA SIMPLE IM API

6.3.2.1 IM Settings

REQ. ID	REQUIREMENT	TYPE	FEATURE
IMS-3600	An API MUST be offered to publish IM Service Settings.	**NEW**	**IM**

REQ. ID	REQUIREMENT	TYPE	FEATURE
IMS-3610	An API MUST be offered to publish IM specific presence.	**NEW**	**IM**

6.3.2.2 One Shot Message

One Shot Message is a message independent of any other message that the sender and/or the receivers could have sent before or will send in the future (e.g. 3GPP SMS model). A One Shot Message can be carried out inside a SIP MESSAGE method (Pager Mode Message) or creating a MSRP session (Large Message Mode) as described in OMA SIMPLE IM [35].

REQ. ID	REQUIREMENT	TYPE	FEATURE
IMS-3620	An API MUST be offered to send an IM One Shot Message (i.e. outside of an IM session) to an individual participant.	**NEW**	**IM**
IMS-3630	An API MUST be offered to send IM One Shot Message (i.e. outside of an IM session) to an ad-hoc group.	**NEW**	**IM**
IMS-3640	An API MUST be offered to send IM One Shot Message (i.e. outside of an IM session) to a pre-defined group.	**NEW**	**IM**
IMS-3650	An API MUST be offered to send an IM One Shot Message with external content.	**NEW**	**IM**
IMS-3660	An API MUST be offered to request anonymity on sending an IM One Shot Message.	**NEW**	**IM**
IMS-3670	An API MUST be offered to send a delivery report.	**NEW**	**IM**
IMS-3680	An API MUST be offered to receive an IM One Shot Message (i.e. outside of an IM session).	**NEW**	**IM**
IMS-3690	An API MUST be offered to receive an IM One Shot Message with external content.	**NEW**	**IM**

REQ. ID	REQUIREMENT	TYPE	FEATURE
IMS-3700	An API MUST be offered to receive a delivery report.	**NEW**	**IM**

6.3.2.3 Session Mode Messaging

Session Mode Messaging can only be carried out within a MSRP session, as described in [35].

REQ. ID	REQUIREMENT	TYPE	FEATURE
IMS-3710	An API MUST be offered to establish a One to One IM session with an Invited IM Client.	**NEW**	**IM**
IMS-3720	An API MUST be offered to establish an Ad-Hoc IM Conference.	**NEW**	**IM**
IMS-2100	An API MUST be offered to join a Pre-Defined IM conference.	**NEW**	**IM**
IMS-2110	An API MUST be offered to join a chat room with a unique chat alias.	**NEW**	**IM**
IMS-2120	An API MUST be offered to send a Private Message(s) in a conference session.	**NEW**	**IM**
IMS-2130	An API MUST be offered to add users to an existing IM conference session.	**NEW**	**IM**
IMS-2140	An API MUST be offered to add additional users to a one to one session (i.e. extending the session to a one to many session).	**NEW**	**IM**
IMS-2150	An API MUST be offered to expel a user from a session.	**NEW**	**IM**
IMS-2160	An API MUST be offered to subscribe to a conference event package.	**NEW**	**IM**
IMS-2170	An API MUST be offered to leave an IM Session.	**NEW**	**IM**

REQ. ID	REQUIREMENT	TYPE	FEATURE
IMS-2180	An API MUST be offered to cancel an IM Session.	**NEW**	**IM**
IMS-2190	An API MUST be offered to send the "isComposing" status during an IM Session.	**NEW**	**IM**
IMS-2200	An API MUST be offered to initiate an IM Session Modification.	**NEW**	**IM**
IMS-2210	An API MUST be offered to rejoin an IM Conference Session.	**NEW**	**IM**
IMS-2220	An API MUST be offered to request anonymity on establishing/joining an IM session.	**NEW**	**IM**
IMS-2230	An API MUST be offered to accept or reject an invitation for an IM Session.	**NEW**	**IM**
IMS-2240	An API MUST be offered to receive the release for an IM Session.	**NEW**	**IM**
IMS-2250	An API MUST be offered to receive an IM Session modification request.	**NEW**	**IM**
IMS-2260	An API MUST be offered to receive an IM session cancel request.	**NEW**	**IM**
IMS-2270	An API MUST be offered to receive the "isComposing" status during an IM Session.	**NEW**	**IM**
IMS-2280	An API MUST be offered to receive a Private Message(s) in a conference session.	**NEW**	**IM**

6.3.2.4 File Transfer

REQ. ID	REQUIREMENT	TYPE	FEATURE
IMS-2290	An API MUST be offered to transfer one or more files inside an ongoing session.	**NEW**	**IM**

REQ. ID	REQUIREMENT	TYPE	FEATURE
IMS-2300	An API MUST be offered to transfer one or more files outside an ongoing session.	**NEW**	**IM**
IMS-2310	An API MUST be offered to receive one or more files transferred inside an ongoing session.	**NEW**	**IM**
IMS-2320	An API MUST be offered to receive one or more files transferred outside an ongoing session.	**NEW**	**IM**

6.3.2.5 Deferred Messages

REQ. ID	REQUIREMENT	TYPE	FEATURE
IMS-2330	An API MUST be offered to retrieve a particular or multiple selected or all deferred messages.	**NEW**	**IM**
IMS-2340	An API MUST be offered to retrieve deferred Message metadata.	**NEW**	**IM**
IMS-2350	An API MUST be offered to delete a particular or multiple selected or all deferred messages.	**NEW**	**IM**
IMS-2360	An API MUST be offered to deliver report for deferred messages.	**NEW**	**IM**
IMS-2361	An API MUST be offered to receive deferred messages.	**NEW**	**IM**

6.3.2.6 Conversation History

REQ. ID	REQUIREMENT	TYPE	FEATURE

REQ. ID	REQUIREMENT	TYPE	FEATURE
IMS-2370	An API MUST be offered to turn on/off the Conversation History Function in a session (i.e. adding/removing the Conversation History function as a participant to that session).	**NEW**	**IM**
IMS-2380	An API MUST be offered to retrieve a particular or multiple selected or all IM Histories.	**NEW**	**IM**
IMS-2390	An API MUST be offered to retrieve History metadata.	**NEW**	**IM**
IMS-2400	An API MUST be offered to delete a particular or multiple selected or all IM Histories.	**NEW**	**IM**

6.3.3 OMA PRESENCE API

6.3.3.1 Presentity Requirements

This section describes the API requirements related to managing different information (e.g. presence Information, different related XDM documents - authorization rules and subscription lists) about a Presentity. Typically, a presence Source performs such management operation on behalf of a Presentity.

REQ. ID	REQUIREMENT	TYPE	FEATURE
IMS-1270	The UE MUST offer an API to allow an application to locally manipulate presence information (including presence information element: Terminal, person and service information) of the local presentity for each public identity used during registration.	NEW	PRESENCE
IMS-2411	The UE MUST offer an API to allow an application to retrieve presence information (including presence information element: Terminal, person and service information) of the local presentity for each public identity used during registration.	NEW	PRESENCE
IMS-2420	The UE MUST offer an API to allow an application to create presence authorisation policies of the local presentity.	NEW	PRESENCE
IMS-2421	The UE MUST offer an API to allow an application to retrieve presence authorisation policies of the local presentity.	NEW	PRESENCE
IMS-1290	The UE MUST offer an API to allow an application to manipulate (adding, modifying or removing) each presence information element (both standard and application specific elements) defined in the presence document. OMA-Presence DDS [new ref], Section 10.	NEW	PRESENCE

REQ. ID	REQUIREMENT	TYPE	FEATURE
IMS-1300	The UE MUST offer an API to allow an application to manipulate (adding, modifying or removing) presence authorisation policies related to a local presentity. Presence XDM Specification [54], Section 5.1.1.	NEW	PRESENCE
IMS-1310	The UE MUST offer an API to allow an application to manipulate (adding, modifying or removing) presence content rules related to a local presentity. Presence XDM Specification [54], Section 5.1.2.	NEW	PRESENCE
IMS-1330	The UE MUST offer an API to allow an application to manage (create, update, remove, subscribe to changes etc.) XDM–based presentity lists. OMA-Presence [32], Section 5.6 and Presence Resource List Server XDM Specification [55].	NEW	PRESENCE

6.3.3.2 Presence Publication

This section describe the API requirements related to the presence information publication as described in OMA Presence v1.1 [32] section Publication

REQ. ID	REQUIREMENT	TYPE	FEATURE
IMS-1340	The UE MUST offer an API to allow an application to publish the presence information, represented according to IMS-2410, for a local presentity. OMA-Presence [32], Section 5.1.1.	NEW	PRESENCE
IMS-1350	The UE MUST offer an API to allow an application to refresh publications.	NEW	PRESENCE
IMS-1360	The UE MUST offer an API to allow an application to receive indication if its publications are near expiration.	NEW	PRESENCE

REQ. ID	REQUIREMENT	TYPE	FEATURE
IMS-1370	The UE MUST offer an API to allow an application to remove its publications.	NEW	PRESENCE

6.3.3.3 Presence subscription

This section describes the API requirements related to the presence information subscription as described in OMA Presence v1.1 [32] section subscription.

REQ. ID	REQUIREMENT	TYPE	FEATURE
IMS-1380	The UE MUST offer an API to allow an application to subscribe/unsubscribe for presence information of a remote presentity or presence list (representing multiple presentities). OMA-Presence [32], Section 5.2.2.	NEW	PRESENCE
IMS-1400	The UE MAY offer an API to allow an application to subscribe for the watcher information as defined in OMA-Presence [32], Section 5.3.	NEW	PRESENCE
IMS-1410	The UE MUST offer an API to allow an application to refresh subscriptions.	NEW	PRESENCE
IMS-1420	The UE MUST offer an API to allow an application to receive indication if its subscriptions are judged to be near expiration by the UE as specified by the timers maintained from IMS-0370.	NEW	PRESENCE
IMS-1430	The UE MUST offer an API to allow an application to receive indication if a subscription was cancelled or terminated.	NEW	PRESENCE
IMS-1440	The UE MUST offer an API to allow an application to perform one-time subscription for presence information of a remote presentity or presence list. OMA-Presence [32].	NEW	PRESENCE

6.3.3.4 Presence notification

This section describes the API requirements related to the presence and watcher information notification as described in OMA Presence v1.1 [32], notification section.

REQ. ID	REQUIREMENT	TYPE	FEATURE
IMS-1390	The UE MUST offer an API to allow an application to receive presence information in notification of the subscribed presentity or presence list.	NEW	PRESENCE
IMS-2561	The UE MAY offer an API to allow an application to receive updated watcher information notification as defined in OMA-Presence [32], Section 5.3.	NEW	PRESENCE

6.3.4 OMA XML DOCUMENT MANAGEMENT API

This section describes the API requirements related to the XDM functionalities described in XDM 1.1 [33] and XDM 2.0 [34].

NOTE: The XDM versions which the requirements in this section refer to are shown in the "Version Applicable" column. If one version is referred to, the requirement applies exclusively to implementations of that version. When two versions are referred to the requirement applies to both PoC versions.

6.3.4.1 Document Manipulation

REQ. ID	REQUIREMENT	TYPE	FEATURE	VERSION APPLICAB
IMS-1810	The UE MUST offer an API to allow an application to be able to create a new XML document on the XDMS stating the PUID to use for document creation.	**NEW**	**XDM**	**v1.1** **v2.0**
IMS-1820	The UE MUST offer an API to allow an application to delete an XML document on the XDMS.	**NEW**	**XDM**	**v1.1** **v2.0**
IMS-1830	The UE MUST offer an API to allow an application to retrieve an existing XML document from the XDMS.	**NEW**	**XDM**	**v1.1** **v2.0**
IMS-1840	The UE MUST offer an API to allow an application to replace an existing XML document on the XDMS.	**NEW**	**XDM**	**v1.1** **v2.0**
IMS-1860	The UE MUST offer an API to allow an application to modify an existing XML document on the XDMS.	**NEW**	**XDM**	**v1.1** **v2.0**
IMS-1890	The UE MUST offer an API to allow an application to search User Profile and Groups in an existing XML document on the XDMS.	**NEW**	**XDM**	**v2.0**

REQ. ID	REQUIREMENT	TYPE	FEATURE	VERSION APPLICAB
IMS-1920	The UE MUST offer an API to allow an application to retrieve a list of documents (i.e. directory.xml) that it owns on the XDMS.	**NEW**	**XDM**	**v1.1** **v2.0**

6.3.4.2 Element and Attribute Manipulation

REQ. ID	REQUIREMENT	TYPE	FEATURE	VERSION APPLICAB
IMS-1930	The UE MUST offer an API to allow an application to create an element for an existing XML document on the XDMS.	**NEW**	**XDM**	**v1.1** **v2.0**
IMS-1940	The UE MUST offer an API to allow an application to delete an element from an existing XML document on the XDMS.	**NEW**	**XDM**	**v1.1** **v2.0**
IMS-1950	The UE MUST offer an API to allow an application to retrieve an element from an existing XML document on the XDMS.	**NEW**	**XDM**	**v1.1** **v2.0**
IMS-1960	The UE MUST offer an API to allow an application to replace an element for an existing XML document on the XDMS.	**NEW**	**XDM**	**v1.1** **v2.0**
IMS-1970	The UE MUST offer an API to allow an application to create an attribute for an existing XML document on the XDMS.	**NEW**	**XDM**	**v1.1** **v2.0**
IMS-1980	The UE MUST offer an API to allow an application to delete an attribute from an existing XML document on the XDMS.	**NEW**	**XDM**	**v1.1** **v2.0**

REQ. ID	REQUIREMENT	TYPE	FEATURE	VERSION APPLICAB
IMS-1990	The UE MUST offer an API to allow an application to retrieve an attribute from an existing XML document on the XDMS.	**NEW**	**XDM**	**V1.1** **V2.0**
IMS-2000	The UE MUST offer an API to allow an application to replace an attribute for an existing XML document on the XDMS.	**NEW**	**XDM**	**V1.1** **V2.0**

6.3.4.3 Subscriptions (XDMS)

REQ. ID	REQUIREMENT	TYPE	FEATURE	VERSION APPLICAB
IMS-2010	The UE MUST offer an API to allow an application to subscribe to the XDMS for change notifications if an XML document is changed.	**NEW**	**XDM**	**V2.0**
IMS-2020	The UE MUST offer an API to allow an application to unsubscribe from the XDMS for change notifications established in IMS-2820.	**NEW**	**XDM**	**V2.0**

6.3.5 MMTEL API

Although each service could offer specific operations to the application, MMTEL defines PSNT/ISDN simulation services, so it is likely that the APIs on the UE could be available and quite similar to those already defined for the mobile Terminal (e.g. GSM Terminal).

Typical operations that UE must be able to perform, and so also be available as API, should be:

REQ. ID	REQUIREMENT	TYPE	FEATURE
IMS-2840	The UE MUST offer an API to allow an application to activate the service.	NEW	MMTEL
IMS-2841	The UE MUST offer an API to allow an application to deactivate the service.	NEW	MMTEL
IMS-2842	The UE MUST offer an API to allow an application to register some information about the service.	NEW	MMTEL
IMS-2843	The UE MUST offer an API to allow an application to erasure of the information about the service.	NEW	MMTEL
IMS-2844	The UE MUST offer an API to allow an application to interrogate the service.	NEW	MMTEL

7 FURTHER WORK

This section lists those which may be addressed in future versions of this document (with no priority order). Some additional items might be also considered:

- **3GPP Release 8**: OMTP recommendations have focused on 3GPP Release 7 specifications. Apart from the evolution of the documents referred in these recommendations there are several new areas that will be included in Release 8 that should be considered in the future.

- **New OMA Enablers (non-exhaustive):**

    - **OMA SIP Based Push v2.2:** The scope of this work item is to introduce SIP as a transport bearer for WAP push; maintaining compatibility with the existing WAP push architecture, push message definitions and service specifications is a high priority. The resulting SIP Push OTA specifications preferably utilise already existing SIP extensions, namely SIP for Instant Messaging or the SIP events framework.

    - **OMA Converged IP Messaging (OMA CPM):** The goal of this work item is to specify the future messaging functionalities as common reusable capabilities that support the building of a range of IP-based Services needing messaging functionality. The evolutionary interoperability between future IP-based messaging services and legacy Mobile Messaging Services e.g., SMS, MMS and IMPS, is included in the overall architecture in order to achieve maximum connectivity between end-users (independent of whether they are using the future IP-based messaging services or legacy Mobile Messaging Services).

    - **OMA Converged Address Book (OMA CAB):** The Converged Address Book (CAB) Enabler provides consistent mechanisms to manage contact information in both user facing applications as well as in support of network facing activities. At the core of this enabler is a network-based contact repository which a user can use to store contact information which can be retrieved by any properly enabled device. The network-based repository is also able to provide specific contact information to other users and to keep them up-to-date whenever the data is updated.

    - **OMA Dynamic Content Delivery (DCD):** The scope of this work item is to provide an enabler for automated delivery of personalized content direct to users' devices. Support for DCD over SIP/IMS will enhance the dynamic characteristics of the enabler; so that it can more effectively support server initiated

(pushed) content delivery, enabler integration (e.g. Presence, Location) and availability over a variety of network technologies. In the SIP/IMS environment, DCD will leverage SIP/IMS features directly, and other SIP-related OMA enablers as available.

- **OMA Presence 2.0:** OMA is in the process of releasing a new version of the Presence SIMPLE enabler which version 1.1 is already referred in this document.

- **OMA Data Synchronization (DS):** The scope of this work item is to provide an enabler for synchronising content between the network and devices via the SyncML standard. Support for DS in the SIP/IMS environment will enable portability of IMS settings, services and service characteristics across a range of personal devices.

- **Security:** Future versions of this document should also address additional security aspects like Bootstrapping Architectures, security algorithms etc.

- **Policy and Charging Control Architecture:** Future versions of this document may also address policy and charging control aspects as defined in 3GPP. TS 23.203 which specifies the overall stage 2 level functionality for Policy and Charging Control that encompasses flow based charging and policy control for IP-CANs (e.g. GPRS, I-WLAN, Fixed Broadband etc.).

7.1 FORWARD LOOKING REQUIREMENTS

There are some requirements that were elicited in the generation of this recommendation which do not yet have standards to support them, but which will require standardisation to be actively implemented within mobile Terminals.
The following list of requirements is intended to give a clear indication of what will be expected in the future.

REQ. ID	REQUIREMENT	TYPE	FEATURE
IMS-3460	The UE MAY provide an API to allow an application to request the list of all available radio access technologies supported by the UE (e.g. WiFi, EDGE, UMTS, GPRS, etc).	NEW	IMS CORE

REQ. ID	REQUIREMENT	TYPE	FEATURE
IMS-1170	The UE MUST offer an API to allow an application to choose the bearer (from the list provided in IMS-1440) for the SIP signalling subject to Bearer Policy.	NEW	IMS CORE
IMS-1180	The UE MUST offer an API to allow an application to choose the bearer (from the list provided in IMS-1440) for a media connection subject to Bearer Policy.	NEW	IMS CORE
IMS-1190	The UE MUST provide an API to allow an application to receive notifications when the set of available bearers change.	NEW	IMS CORE
IMS-3470	The UE SHOULD offer an API to allow an application to transfer media to another Terminal.	NEW	IMS CORE

8 DEFINITION OF TERMS

TERM	DESCRIPTION
APPLICATION REFERENCE MEDIA FEATURE TAG	Media Feature Tag that indicates the software applications supported by the UE (i.e. ICSI and IARI). It is identified by the name: g.3gpp.app_ref.
APPLICATION REGISTERED ON THE TERMINAL	Application which has indicated to the UE that it is available. The application does not necessarily need to be registered on the IMS network (see Application Registered on the IMS Network definition).
APPLICATION REGISTERED ON THE IMS NETWORK	Application which has had its capabilities registered on the IMS network by the UE.
BEARER POLICY	Access network control defined by handset manufacturer, operator or 3rd party.
CORE API	Programmatic interfaces exposed by the IMS Core in order to provide access to IMS Core Functionalities.
IMS AUTHENTICATION	Establishment of a secure association between a UE and an IMS network.
IMS CORE	The block providing the basic IMS functionality using the capabilities of the IMS related protocols and stacks.
IMS FRAMEWORK	Set of all the modules (e.g. libraries, applications, APIs) that implement IMS Functionalities on UE.
IMS SERVICE ENABLERS	IMS Service Enablers offer functionality focused in a specific service (e.g. PoC, IM, Presence).
MANAGEMENT OBJECT	Management objects are the entities that can be manipulated by management actions carried over the OMA DM protocol.

TERM	DESCRIPTION
ONE SHOT MESSAGE	Message independent of any other message that the sender and/or the receivers could have sent before or will send in the future (e.g. 3GPP SMS model). A One Shot Message can be carried out inside a SIP MESSAGE method (Pager Mode Message) or creating a MSRP session (Large Message Mode) as described in OMA-ERP-SIMPLE_IM-V1_0-C.
PRESENTITY (PRESENCE ENTITY)	Entity described by Presence information.
REGISTER / UNREGISTER ON THE TERMINAL	Process by which an Application indicates to the UE that it is available / unavailable (see Application Registered On The Terminal). The application does not necessarily need to be registered on the IMS network (see Application Registered on the IMS Network definition).
SERVICES API	Programmatic interfaces offered by the IMS Service Enablers (e.g. PoC) in order to provide access to IMS Service Enablers Functionalities.
TERMINAL	Used as an alternative term for a cellular telephone or handset.
USER EQUIPMENT	Combination of mobile Terminal and UICC.

9 ABBREVIATIONS

ABBREVIATION	DESCRIPTION
3GPP	3rd Generation Partnership Project
3GPP2	3rd Generation Partnership Project 2
ACL	Access Control List
AKA	Authentication and Key Agreement Protocol
API	Application Programming Interface
APN	Access Point Name
ASF	Application Security Framework
BICC	Bearer Independent Call Control
CAMEL	Customised Applications for Mobile network Enhanced Logic
CAP	CAMEL Application Part
CN	Core Network
CPM	Converged IP Messaging
CS	Circuit Switched
CSI	Combinational Services
CSICS	Circuit Switched IMS Combinational Services
DCD	Dynamic Content Delivery
DHCP	Dynamic Host Configuration Protocol
DL	Download Link
DM	Device Management
DNS	Domain Name System
EDGE	Enhanced Data rates for Global Evolution
ETSI	European Telecommunications Standards Institute

ABBREVIATION	DESCRIPTION
GCF	Global Certification Forum
GERAN	GSM EDGE Radio Access Network
GLM	Group List Management
GPRS	General Packet Radio System
GRUU	Globally Routable User Agent URIs,
GSM	Global System for Mobile Communications
GSMA	GSM Association
HTTP	Hyper Text Transfer Protocol
HTTPS	Secure HTTP
I-WLAN	Interworking - WLAN
IARI	IMS Application Reference Identifier
ICSI	IMS Communication Service Identifier
ID	Identifier
IETF	Internet Engineering Task Force
IM	Instant Messaging
IMPS	Instant Messaging and Presence Service
IMS	IP Multimedia System
IMTC	International Multimedia Telecommunication Consortium
I/O	Input / Output
IoT	Inter Operability
IP	Internet Protocol
IP-CAN	IP-Connectivity Access Network
IPSEC	IP Security

ABBREVIATION	DESCRIPTION
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
ISDN	Integrated Services Digital Network
ISIM	IP Multimedia Services Identity Module
ISUP	ISDN User Part
J2ME	Java 2 Micro Edition
JCP	Java Community Process
JSR	Java Specification Request
MAP	Mobile Application Part
MMD	Multimedia Domain
MMS	Multimedia Message Service
MMTEL	Multimedia Telephony
MSRP	Message Session Relay Protocol
NAS	Non-Access Stratum
NAT	Network Address Translation
OMA	Open Mobile Alliance
OMNA	Open Mobile Naming Authority
OMTP	Open Mobile Terminal Platform
OS	Operating System
OTA	Over The Air
PBX	Private Branch Exchange
PCS	Personal Communications Service
PDP	Packet Data Protocol

ABBREVIATION	DESCRIPTION
PoC	Push Over Cellular
PS	Packet Switched
PSTN	Public Switched Telephone Network
PTCRB	PCS Type Certification Review Board
PUID	Public User Identity
QoS	Quality of Service
RAB	Radio Access Bearer
RFC	Request For Comments
RTP	Real Time Protocol
RTCP	Real Time Control Protocol
RTSP	Real Time Streaming Protocol
SDO	Standard Definition Organization
SDP	Session Description Protocol
SIGCOMP	Signalling Compression
SIM	Subscriber Identity Module
SIMPLE	SIP for Instant Messaging and Leveraging Extensions
SIP	Session Initiation Protocol
SMS	Short Message Service
STD	Standard
STUN	Simple Traversal of User Datagram Protocol
TBF	Temporary Block Flow
TISPAN	Telecoms & Internet converged Services & Protocols for Advanced Networks
TS	Technical Specification

ABBREVIATION	DESCRIPTION
UA	User Agent
UE	User Equipment
UICC	Universal Integrated Circuit Card
UMTS	Universal Mobile Telecommunications System
URI	Uniform Resource Indentifier
USIM	Universal Subscriber Identity Module
VCC	Voice Call Continuity
WAP	Wireless Application Protocol
WIFI	Wireless Fidelity
WLAN	Wireless Local Area Network
XCAP	XML Configuration Access Protocol
XDM	XML Document Management
XDMS	XML Document Management Server
XML	Extensible Markup Language

10 REFERENCED DOCUMENTS

The following table summarises the documents referred within this set of recommendations.

References are either specific (identified by date of publication and/or edition number or version number) or non specific.

- For a specific reference, subsequent revisions do not apply.
- For a non specific reference, the latest version applies. In the case of a reference to a Rel 7 document, a non specific reference implicitly refers to the latest version of that document in the same Release as the present document. Similarly, a non specific reference to an OMA document of a specific version refers to the latest available document of the same version.

NO.	DOCUMENT	AUTHOR
[1]	"Application Security Framework"	OMTP
[2]	RFC 2119, "Key words for use in RFCs to Indicate Requirement Levels"	IETF
[3]	"OMA Push to talk Over Cellular V1.0"	OMA
[4]	3GPP TS 23.060 "General Packet Radio Service (GPRS); Service description", Release 7	3GPP
[5]	3GPP TS 24.229 "IP Multimedia Call Control Protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP), Stage 3 (R7)"	3GPP
[6]	RFC 791 - "Internet Protocol"	IETF
[7]	RFC 2460 - "Internet Protocol, Version 6 (IPv6) Specification"	IETF
[8]	RFC 3329 - "Security Mechanism Agreement for the Session Initiation Protocol (SIP)"	IETF
[9]	RFC 3315 - "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)"	IETF
[10]	RFC 1591 - "Domain Name System Structure and Delegation"	IETF

No.	Document	Author
[11]	RFC 3550 - “RTP: A Transport Protocol for Real-Time Applications“	IETF
[12]	RFC 2326 – “Real Time Streaming Protocol”	IETF
[13]	draft-ietf-simple-xcap-12	IETF
[14]	RFC 2660 – “The Secure Hypertext Transfer Protocol”	IETF
[15]	3GPP TS 24.247 – “Messaging service using the IP Multimedia (IM) Core Network (CN) subsystem” (Release 7)	IETF
[16]	3GPP TS 23.203 “Numbering, Addressing and Identification”	3GPP
[17]	3GPP TS 31.103 "Characteristics of the IP Multimedia Services Identity Module (ISIM) application (Release 7)"	3GPP
[18]	3GPP TS 31.102 "Characteristics of the Universal Subscriber Identity Module application (Release 7)"	3GPP
[19]	3GPP TS 33.203 “Access security for IP-based services, (Release 7)“	3GPP
[20]	3GPP TS 33.978 “Security Aspects of early IP Multimedia Subsystem (IMS)” (Release 7)	3GPP
[21]	3GPP TS 34.229-1 “Internet Protocol (IP) multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP) -User Equipment (UE) conformance specification; Part 1: Protocol conformance specification - (Release 7)”	3GPP
[22]	3GPP TS 23.228: “IP Multimedia Subsystem (IMS); Stage 2, Release 7”	3GPP
[23]	RFC 3265 - “SIP Specific Event Notification”	IETF
[24]	3GPP TS 29.213 – “Policy and Charging Control signalling flows and QoS parameter mapping” (Release 7)	3GPP
[25]	3GPP TS 24.206 “Voice Call Continuity between Circuit Switched (CS) and IP Multimedia Subsystem (IMS)”	3GPP
[26]	RFC 2543 – “SIP: Session Initiation Protocol”	IETF

No.	Document	Author
[27]	RFC 2396 – "Uniform Resource Identifiers (URI): Generic Syntax"	IETF
[28]	RFC 2506 – "Media Feature Tag Registration Procedure"	IETF
[29]	RFC 3840 - "Indicating User Agent Capabilities in the Session Initiation Protocol (SIP)"	IETF
[30]	RFC 3841 "Caller Preferences for SIP"	IETF
[31]	"OMA Push to talk Over Cellular V2.0"	OMA
[32]	Presence SIMPLE Specification V1.1 (OMA-TS-Presence_SIMPLE-V1_1)	OMA
[33]	"OMA XML Document Management V1.1"	OMA
[34]	"OMA XML Document Management V2.0	OMA
[35]	"OMA SIMPLE IM V1.0"	OMA
[36]	"IR.79 Image Share Interoperability Specifications"	GSMA
[37]	RFC 3428 "Session Initiation Protocol (SIP) Extension for Instant Messaging"	IETF
[38]	RFC 4483 "A Mechanism for Content Indirection in Session Initiation Protocol (SIP) Messages",	IETF
[39]	RFC 4975 "The Message Session Relay Protocol (MSRP)"	IETF
[40]	3GPP TS 24.173 "IMS Multimedia telephony service and supplementary services", Release 7	3GPP
[41]	3GPP TS 26.141, "IP Multimedia System (IMS) Messaging and Presence; Media formats and codecs", (Release 7)	3GPP
[42]	"OMA Device Management v1.2"	OMA
[43]	3GPP TS 24.167 "3GPP IMS Management Object; Stage 3, Release 7"	3GPP
[44]	3GPP TS 24.216 "Communication Continuity Management Object (MO)", Release 7	3GPP
[45]	RFC 2976 – "The SIP Info Method"	IETF

No.	Document	Author
[46]	RFC 3903 – "Session Initiation Protocol (SIP) Extension for Event State Publication"	IETF
[47]	RFC 2131 – "Dynamic Host Configuration Protocol"	IETF
[48]	"Implementation Guidelines for OMA Presence SIMPLE v1.1"	OMA
[49]	"Implementation Guidelines for OMA XDM v1.1"	OMA
[50]	"IR-74 Video Share Interoperability Specification v1.1"	GSMA
[51]	"SE-41 Video Share Service Definition v.2.0"	GSMA
[52]	"Presence SIMPLE Management Object v1.1"	OMA
[53]	"OMA Management Object for XML Document Management"	OMA
[54]	"OMA Presence XDM Specification v1.1"	OMA
[55]	"OMA Presence Resource List Server XDM Specification v1.1"	OMA
[56]	"IMS Video Share Test Cases V1.0"	IMTC
[57]	"OMA SIP Push v1.0 Technical Specification"	OMA
[NN]	Presence SIMPLE Data Specification V1.0 (OMA-DDS-Presence_SIMPLE-V1_0)	OMA
[NN]	IMS Functional Requirements v1.0	OMTP