

IMS Profile for Voice, Video and SMS over Wi-Fi

Version 2.1

13 August 2015

This is a Non-binding Permanent Reference Document of the GSMA.

Security Classification: Non-confidential

Access to and distribution of this document is restricted to the persons permitted by the security classification. This document is confidential to the Association and is subject to copyright protection. This document is to be used only for the purposes for which it has been supplied and information contained in it must not be disclosed or in any other way made available, in whole or in part, to persons other than those permitted under the security classification without the prior written approval of the Association.

Copyright Notice

Copyright © 2015 GSM Association

Disclaimer

The GSM Association ("Association") makes no representation, warranty or undertaking (express or implied) with respect to and does not accept any responsibility for, and hereby disclaims liability for the accuracy or completeness or timeliness of the information contained in this document. The information contained in this document may be subject to change without prior notice.

Antitrust Notice

The information contain herein is in full compliance with the GSM Association's antitrust compliance policy.

Table of Contents

1 Introduction 4
1.1 Overview 4
1.2 Relationship to existing standards 4
1.2.1 3GPP Specifications 4
1.3 Scope 5
1.4 Definitions 5
1.5 References 6
2 IMS feature set 6
2.1 General 6
2.2 Support of generic IMS functions 6
2.2.1 SIP Registration Procedures 6
2.2.2 Authentication 7
2.2.3 Addressing 7
2.2.4 Call Establishment and Termination 7
2.2.5 Forking 7
2.2.6 The use of Signalling Compression 7
2.2.7 Hosted NAT Traversal 8
2.3 Supplementary Services 8
2.4 Call Set-up Considerations 8
2.4.1 SIP Precondition Considerations 8
2.4.2 Integration of resource management and SIP 8
2.4.3 Voice Media Considerations 8
2.4.4 Video Media Considerations 8
2.5 SMS over IP 8
3 IMS media 9
4 Radio and packet core feature set 9
4.1 Radio capabilities 9
4.1.1 Alignment with Wi-Fi Alliance Certification programmes 9
4.1.2 WLAN Policy provisioning 9
4.1.3 Connection management 9
4.2 Trusted/Untrusted Wi-Fi IP Access Network Detection 9
4.3 Wi-Fi Access Network Selection 9
4.4 Non-3GPP Access Authentication and Security 9
4.5 Multiple PDN connections 10
4.6 APN Considerations for SIP Signalling and XCAP 10
4.7 PDN Connectivity Service 11
4.7.1 Untrusted Access 11
4.7.2 Trusted Access 12
4.8 Mobility Management 12
4.9 P-CSCF Discovery 12
5 Common Functionalities 12
5.1 IP Version 12

5.2 IP Address Allocation 13
5.3 Emergency Service 13
5.4 Roaming Considerations 13
Annex A Document Management 14
A.1 Document History 14
A.2 Other Information 14

1 Introduction

1.1 Overview

The IP Multimedia Subsystem (IMS) Profile for Voice and Video, documented in this Permanent Reference Document (PRD), defines a profile that identifies a minimum mandatory set of features which are defined in 3GPP specifications that a wireless device (the User Equipment (UE)) and network are required to implement in order to guarantee interoperable, high quality IMS-based telephony and conversational video services over Wi-Fi access.

"Wi-Fi" is a trademark of the Wi-Fi Alliance and the brand name for products using WFA programs based on the IEEE 802.11 family of standards.

In this document, Wi-Fi access refers to a WLAN access to EPC, either trusted (S2a interface) or untrusted (S2b interface), as defined in 3GPP TS 23.402 [6].

The scope includes the following aspects:

- IMS basic capabilities and supplementary services for telephony [Chapter 2]
- Real-time media negotiation, transport, and codecs [Chapter 3]
- Wi-Fi radio and (evolved) packet core capabilities [Chapter 4]
- Functionality that is relevant across the protocol stack and subsystems [Chapter 5].

The conversational video services comprise calls with full duplex voice and simplex/full-duplex video media with tight synchronization between the constituent streams. The call can be a point to point call or a multiparty conference call. The conversational video service can also be used to interact with for example dial in video conference systems.

A UE and a network compliant to this profile must support IMS-based telephony. A UE and a network compliant to this profile may support conversational video services.

1.2 Relationship to existing standards

1.2.1 3GPP Specifications

This profile is based on the open and published 3GPP specifications as listed in Section 1.5. 3GPP Release 11 is taken as a basis. It should be noted, however that not all the features specified in 3GPP Release 11 are required for compliance with this profile.

Conversely, some features required for compliance with this profile are based on functionality defined in 3GPP Release 12 or higher releases.

All such exceptions are explicitly mentioned in the following sections along with the relevant Release 11 or higher 3GPP release specifications, respectively.

Unless otherwise stated, the latest version of the referenced specifications for the relevant 3GPP release applies.

1.3 Scope

This document defines a voice and video over Wi-Fi IMS profile by profiling a number of Wi-Fi, (Evolved) Packet Core, IMS core, and UE features which are considered essential to launch interoperable IMS based voice and video on Wi-Fi. This document is based on the IMS Voice and SMS profile described in PRD IR.92 [3] and on the IMS Profile for Conversational Video Service profile described in PRD IR.94 [2]. The defined profile is compliant with 3GPP specifications. The scope of this version of the profile is the interface between UE and network.

The profile does not limit anyone, by any means, to deploy other standardized features or optional features, in addition to the defined profile.

1.4 Definitions

Term	Description
3GPP	3rd Generation Partnership Project
APN	Access Point Name
DNS	Domain Name System
EAP-AKA	Extensible Authentication Protocol – Authentication and Key Agreement
ePDG	Evolved Packet Data Gateway
FQDN	Fully Qualified Domain Name
IKEv2	Internet Key Exchange version 2
IM	IP Multimedia
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IPsec	IP Security
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
MAPCON	Multi-Access PDN Connectivity
NAT	Network Acess Translation
P-CSCF	Proxy - Call Session Control Function
RTCP	RTP Control Protocol
RTP	Real Time Protocol
SDP	Session Description Protocol
SIP	Session Initiation Protocol
UE	User Equipment
VoIP	Voice Over IP
XCAP	XML Configuration Access Protocol
XML	eXtensible Markup Language

1.5 References

Ref	Doc Number	Title
[1]	GSMA PRD IR.92	IMS Profile for Voice and SMS.
[2]	GSMA PRD IR.94	IMS Profile for Conversational Video Service
[3]	GSMA PRD IR.61	WLAN Roaming Guidelines (Inter-Operator Handbook)
[4]	GSMA PRD TS.22	Recommendations for Minimal Wi-Fi Capabilities of Terminals
[5]	3GPP TS 24.229	IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3
[6]	3GPP TS 23.402	Architecture enhancements for non-3GPP accesses
[7]	GSMA PRD IR.88	LTE Roaming Guidelines
[8]	3GPP TS 23.003	Numbering, addressing and identification
[9]	3GPP TS 33.402	Security aspects for non-3GPP accesses
[10]	IETF RFC 4187	Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)
[11]	IETF RFC 5448	Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA')
[12]	3GPP TS 24.302	Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP access networks; Stage 3
[13]	IETF RFC 5996	Internet Key Exchange Protocol Version 2 (IKEv2)
[14]	3GPP TS 23.228	IP Multimedia Subsystem (IMS); Stage 2
[15]	3GPP TS 24.237	IP Multimedia (IM) Core Network (CN) subsystem IP Multimedia Subsystem (IMS) service continuity; Stage 3
[16]	3GPP TS 24.244	Wireless LAN control plane protocol for trusted WLAN access to EPC; Stage 3

2 IMS feature set

2.1 General

The IMS profile part lists the mandatory capabilities, which are required over the Gm and Ut reference points.

2.2 Support of generic IMS functions

2.2.1 SIP Registration Procedures

The UE and the network must fulfil the requirements on IMS feature set specified in section 2.2.1 of GSMA PRD IR.92 [1], with the exception that section L.3.1.2 of 3GPP TS 24.229 [5] is not applicable.

Note: PRD IR.92 [1] contains explicit statements when the UE must register with the IMS. Currently 3GPP specifications do not have similar statements regarding VoWi-Fi. It is for further study if explicit statements can be created for VoWi-Fi (in addition to what is specified in section 2.4.2.1).

A UE and a network supporting Conversational Video Service over Wi-Fi must fulfil the additional requirements on IMS feature set as specified in section 2.2.1 of GSMA PRD IR.94 [2].

The UE must support and use access-type in P-Access-Network-Info as specified in 3GPP TS 24.229 [5] section 7.2A.4.2. The P-Access-Network-Info header must contain one or more access-infos, one of them being the i-wlan-node-id parameter as specified in 3GPP TS 24.229 [5] section 7.2A.4.2. The i-wlan-node-id shall be set to the value of the MAC address of the WLAN Access Point.

If moving the PDN connection to the IMS well-known APN between Wi-Fi and cellular access as described in section 6.5 of this document, the UE must

- initiate re-registration procedure as specified in 3GPP TS 24.229 [5], section 5.1.1.4 and 3GPP TS 23.228 [14] in section 5.2.2.4,
- update P-Access-Network-Info header field, and
- if it is a Session Continuity UE (SC-UE), update the g.3gpp.accesstype media feature tag as specified in section 6.2.2 of 3GPP TS 24.237 [15].

2.2.2 Authentication

The UE and the network must fulfil the requirements on IMS feature set specified as specified in section 2.2.2 of GSMA PRD IR.92 [1].

2.2.3 Addressing

The UE and the network must fulfil the requirements on IMS feature set as specified in section 2.2.3 of GSMA PRD IR.92 [1].

2.2.4 Call Establishment and Termination

The UE and the network must fulfil the requirements on IMS feature set as specified in section 2.2.4 of GSMA PRD IR.92 [1].

A UE and a network supporting Conversational Video Service over Wi-Fi must fulfil the additional requirements on IMS feature set as specified in section 2.2.2 of GSMA PRD IR.94 [2].

2.2.5 Forking

The UE and the network must fulfil the requirements on IMS feature set as specified in section 2.2.5 of GSMA PRD IR.92 [1].

A UE and a network supporting Conversational Video Service over Wi-Fi must fulfil the additional requirements on IMS feature set as specified in section 2.2.3 of GSMA PRD IR.94 [2].

2.2.6 The use of Signalling Compression

The UE must not use SIGCOMP when the initial IMS registration is performed over Wi-Fi.

2.2.7 Hosted NAT Traversal

The UE and the network shall support the procedures for traversal of a hosted NAT specified in 3GPP TS 24.229 [5], Annex F.

The UE must send keepalives for each RTP media stream, as described in 3GPP TS 24.229 [5], Annex F.5, if the normal RTP media stream packet sending frequency is too low to maintain the NAT bindings.The UE shall send RTP keep-alive as soon as an SDP offer or answer is received as described in 3GPP TS 24.229 [5], Annex F.5.

The bandwidth used for RTCP shall be sufficient to keep NAT bindings open for the RTCP flow, as described in IETF RFC 6263.

2.3 Supplementary Services

The UE and the network must fulfil the requirements on IMS feature set as specified in section 2.3 of GSMA PRD IR.92 [1].

A UE and a network supporting Conversational Video Service over Wi-Fi must fulfil the additional requirements on IMS feature set as specified in section 2.3 of GSMA PRD IR.94 [2].

2.4 Call Set-up Considerations

2.4.1 SIP Precondition Considerations

The UE and the network must fulfil the requirements on IMS feature set as specified in section 2.4.1 of GSMA PRD IR.92 [1].

Note: Even though resources are available, the UE uses preconditions and sets the local preconditions accordingly in SDP offer and answer.

2.4.2 Integration of resource management and SIP

2.4.2.1 Loss of Radio Connection

If the UE loses radio connectivity and the IMS registration has expired prior to regaining radio connectivity, then upon regaining radio connectivity the UE must perform a new initial registration to IMS.

2.4.3 Voice Media Considerations

The UE and the network must fulfil the requirements on IMS feature set as specified in section 2.4.3 of GSMA PRD IR.92 [1].

2.4.4 Video Media Considerations

A UE and a network supporting Conversational Video Service over Wi-Fi must fulfil the requirements on IMS feature set as specified in section 2.4.2 of GSMA PRD IR.94 [2].

2.5 SMS over IP

The UE and network must fulfil the requirements on IMS feature set as specified in section 2.5 of GSMA PRD IR.92 [1].

3 IMS media

The UE and the network must fulfil the requirements on IMS media as specified in section 3 of GSMA PRD IR.92 [1].

A UE and a network supporting Conversational Video Service over Wi-Fi must fulfil the additional requirements on IMS media as specified in section 2.3 of GSMA PRD IR.94 [2].

4 Radio and packet core feature set

4.1 Radio capabilities

4.1.1 Alignment with Wi-Fi Alliance Certification programmes

The UE must fulfil the requirements as specified in section 2 of GSMA PRD TS.22 [4].

4.1.2 WLAN Policy provisioning

The UE must fulfil the requirements as specified in section 3 of GSMA PRD TS.22 [4].

4.1.3 Connection management

The UE must fulfil the requirements as specified in section 4 of GSMA PRD TS.22 [4].

4.2 Trusted/Untrusted Wi-Fi IP Access Network Detection

During initial attach or handover attach a UE must discover the trust relationship per 3GPP TS 24.302 [12] (whether it is a Trusted or Untrusted Wi-Fi Access Network, see GSMA PRD. IR.61 [3]) of the Wi-Fi Access Network in order to know which Wi-Fi Access procedure to initiate The trust relationship of a Wi-Fi Access Network is made known to the UE if

1. The Wi-Fi Access supports 3GPP-based access authentication, the UE discovers the trust relationship during the 3GPP-based access authentication.
   or
2. The UE operates on the basis of pre-configured policy in the UE.

4.3 Wi-Fi Access Network Selection

The UE and the network must support access selection as specified in 3GPP TS 24.302 [12] chapter 5.

4.4 Non-3GPP Access Authentication and Security

The UE and the network must fulfil the requirements as specified in section 5.3 of GSMA PRD IR.61 [3].

For UE and network supporting untrusted access:

- Full Extensible Authentication Protocol - Authentication and Key Agreement (EAP-AKA) authentication procedure as described in 3GPP TS 33.402 [9] and IETF RFC 4187 [10] within IKEv2 as described in IETF RFC 5996 [13] shall be supported;
- Profile of Internet Key Exchange version 2 (IKEv2) as specified in 3GPP TS 33.402 [9] shall be used;
- Profile of IP Security (IPsec) as specified in 3GPP TS 33.402 [9] shall be used;

- Fast re-authentication procedure as described in 3GPP TS 33.402 [9] shall be supported;
- UE shall support to initiate rekeying of both IKE_SA and IPSEC_SA. This should be triggered by a configurable timer;
- UE shall support to receive from Evolved Packet Data Gateway (ePDG) rekeying of both IKE_SA and IPSEC_SA; and
- Network Access Translation (NAT) traversal of IKEv2 and IPsec packets must be supported.

Depending on operator policy, fast re-authentication shall be possible to be used in these scenarios:

- The UE has a SWu tunnel (see GSMA PRD IR.61 [3]) for one Access Point Name (APN). The UE moves to 3GPP for a period and then moves back to Wi-Fi and re-establishes SWu tunnel.
- The UE has at least one existing PDN connection and wants to setup a new one.

4.5 Multiple PDN connections

The UE must support multiple concurrently-active PDN connections. The UE must also support MAPCON (Multi-Access PDN Connectivity) and in this context it must support at least one PDN connection over WLAN and at least one PDN connection over 3GPP access.

Note: For MAPCON support by the network, see section 6.5 in IR.61 [3].

A UE supporting simultaneous radio transmission capability can use MAPCON to offload one or more PDN connections to Wi-Fi while keeping other PDN connections on cellular access.

MAPCON policies must be either pre-defined by the home operator and reside on the UE or be provided via ANDSF according to Release 12 3GPP TS 23.402 [6]. These MAPCON policies can state if and when a certain APN can be moved to Wi-Fi taking into account 3GPP locations (e.g. PLMN, tracking area and cell id), Wi-Fi location (i.e. SSID) location and if the UE is roaming or not.

Note: It is recommended to have MAPCON policies which keep at least one APN/PDN connection on LTE. This avoids frequent attach procedures, reducing the signaling load in the network (for a typical traffic model) and enables a quicker handover from Wi-Fi to LTE. Also, the UE must stay attached to LTE if CS Fallback is used.

4.6 APN Considerations for SIP Signalling and XCAP

When a trusted non-3GPP IP access is used, the UE and the network must support the procedure to signal APNs, as specified in section 16.8.1 of Release 12 of 3GPP TS 23.402 [6].

For SIP signalling, the IMS application in the UE must use the IMS well-known APN as defined in PRD IR.88 [7]; the UE must prevent non-IMS applications from using this APN.

For XCAP requests in Wi-Fi Access, the UE must be preconfigured or provisioned by the home operator either to use Wi-Fi access without PDN connection or with the APN to be used for XCAP requests in Wi-Fi access.

The APN for the PDN Connection used for XCAP requests in Wi-Fi Access may be either the same APN as defined in GSMA PRD IR.92 or a different APN.

Note: If a different APN is used then the IP session continuity between 3GPP and non-3GPP IP access for the PDN Connection used for XCAP requests is not provided.

4.7 PDN Connectivity Service

4.7.1 Untrusted Access

4.7.1.1 General

When an untrusted non-3GPP IP access is used, the UE and the network must fulfil the requirements for PDN Connectivity Service as specified in section 5.6.1 of GSMA PRD IR.61 [3].

4.7.1.2 ePDG Selection

The UE shall select an ePDG as specified in section 7.2.1 of 3GPP TS 24.302 [12].

Note: Domain Name System (DNS) queries for ePDG selection are sent to the DNS server provided on the Wi-Fi Internet connection.

Editor's Note: How the UE is configured to always select an ePDG in the HPMN is FFS.

4.7.1.3 Connectivity Services

The UE must establish a separate SWu instance (i.e. a separate IPsec tunnel) for the PDN connection to the IMS well-known APN and to the APN to be used for XCAP requests, see also section 6.6. The UE must provide the APN during the initial attach procedure and during the attach to additional PDN procedure as specified in 3GPP TS 23.402 [6].

4.7.1.4 UE initiated disconnect

The UE initiated disconnect procedure shall be used by UE in the following scenarios:

- The UE is turned off and has one or more active SWu connections to ePDG;
- Wi-Fi connection is turned off and the UE has one or more active connections to ePDG that according to the UE/operator policy should not be handed over to cellular (i.e. depending on policies, see section 6.5);
  and
- Wi-Fi connection is turned off and UE has one or more active connections to ePDG and no cellular coverage.

For each PDN connection the UE should disconnect, it shall send a IKE Informational request with Delete Payload, which contains the SPI of the IKEv2 SA corresponding to the WLAN UE session to be disconnected.

4.7.1.5 Network initiated disconnect

The UE shall be able to receive an IKEv2 Informational request with Delete Payload, which contains the SPI of the IKEv2 SA corresponding to the WLAN UE session to be disconnected. The UE shall reply with an IKEv2 Information response.

Note: The network that initiates the disconnect can be triggered by many reasons like subscription changes, maintenance in network etc.

4.7.2 Trusted Access

When a trusted non-3GPP IP access is used, the UE and the network must fulfil the requirements for PDN Connectivity Service as specified in section 5.6.2 of GSMA PRD IR.61 [3].

4.8 Mobility Management

A UE supporting untrusted access must

- support seamless handover from LTE to Wi-Fi as described in 3GPP TS 23.402 [6];
- support seamless handover from Wi-Fi to LTE as described in 3GPP TS 23.402 [6].

The network can fulfil the requirements for mobility management as specified in section 6.2 of GSMA PRD IR.61 [3].

4.9 P-CSCF Discovery

The UE and the network must support the procedures for P-CSCF discovery via EPC via WLAN, as described in method IV of Annex R.2.2.1 of Release 13 3GPP TS 24.229 [5].

When establishing a PDN connection to the IMS well-known APN via WLAN, the UE must discover the P-CSCF address(es) as described in method IV of Annex R.2.2.1 of Release 13 3GPP TS 24.229 [5]. When an untrusted non-3GPP IP access is used:

- The UE must support and use the P-CSCF_IP6_ADDRESS attribute and the P-CSCF_IP4_ADDRESS attribute as described in Release 13 3GPP TS 24.302 [12]; and
- The network must support and use the P-CSCF_IP6_ADDRESS attribute, the P-CSCF_IP4_ADDRESS attribute or both as described in Release 13 3GPP TS 24.302 [12].

If P-CSCF address(es) were discovered using the method IV, the UE must use the P-CSCF address(es) discovered using the method IV as defined in section 5.1 and 3GPP TS 24.229 [5].

5 Common Functionalities

5.1 IP Version

The UE and the network shall support both IPv4 and IPv6 for all protocols that are used for the service: SIP, SDP, RTP, RTCP and XCAP/HTTP.

Upon PDN connection procedure over untrusted non-3GPP IP access, the UE shall include proper attribute types in the CFG_REQUEST within the IKE_AUTH request message to request both IPv4 and IPv6 addresses as specified in section 7.2.2 of Release 11 version of 3GPP TS 24.302 [12].

Upon PDN connection procedure over trusted non-3GPP IP access, the UE must follow one of below procedures:

- For the trusted non-3GPP connection mode, using WLCP as signalling protocol for PDN connection handling; in order to request both IPv4 and IPv6 addresses the UE shall set the PDN type IE in the PDN CONNECTIVITY REQUEST message to IPv4v6 as specified in section 5.5.2 of Release 12 version of 3GPP TS 24.244 [16]
- For the trusted non-3GPP connection mode, using the EAP-AKA' extensions as signalling protocol for PDN connection handling; in order to request both IPv4 and IPv6 addresses, the UE shall set the PDN_TYPE item to IPv4v6 as specified in subclause 6.4.2.6.2 of Release 12 version of 3GPP TS 24.302 [12].

For PDN connection over untrusted or trusted non-3GPP IP access,if both IPv4 and IPv6 addresses are assigned for the UE, the UE must prefer the IPv6 address type.

After the UE has discovered the P-CSCF and registered to IMS with a particular IPv4 or IPv6 address, the UE must use this IP address for all SIP communication, as long as the IMS registration is valid. For all SDP and RTP/RTCP communication, the UE must use the IPv4 address used for SIP communication or an IPv6 address with the IPv6 prefix same as the IPv6 prefix of the IPv6 address used for SIP communication.

Note: There are certain situations where interworking between IP versions is required. These include, for instance, roaming and interconnect between networks using different IP versions. In those cases, the network needs to provide the interworking in a transparent manner to the UE.

5.2 IP Address Allocation

When an untrusted non-3GPP IP access is used, the UE and the network must support the IP address allocation as specified in section 4.7.3 of 3GPP TS 23.402 [6].

When a trusted non-3GPP IP access is used, the UE and the network must support the IP address allocation as specified in section 16.1.5.4 of 3GPP Release 12 TS 23.402 [6].

5.3 Emergency Service

The UE must use a cellular access for emergency call.

Note: Emergency call over EPC-integrated Wi-Fi is not specified in 3GPP.

5.4 Roaming Considerations

This profile has been designed to support IMS roaming with both P-CSCF and PGW in the visited network. For more information on this roaming model see GSMA PRD IR.61 [3]. Other roaming models are out of the scope of this profile.

Annex A Document Management

A.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
1.0	17/10/2014	New PRD IR.51	IREG/PSMC	Vincent Danno / Orange
2.0	29/05/2015	Implementation of CR1002, CR1003, CR1004, CR1005, CR1006, CR1007, CR1008, CR1009, CR1010, CR1011, CR1012, CR1013.	RILTE (email approval after Mtg #44)	Merieme El Orch / Orange
2.1	13/08/2015	Headers numbering correction	Networks Group	Merieme El Orch / Orange

A.2 Other Information

Type	Description
Document Owner	NG RILTE
Editor / Company	Merieme El Orch / Orange

It is our intention to provide a quality product for your use. If you find any errors or omissions, please contact us with your comments. You may notify us at prd@gsma.com

Your comments or suggestions & questions are always welcome.