Multi Device
Version 3.0
13 May 2020

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

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

1.1 Overview

1.1.1 General for the multi-device concept

The IP Multimedia Subsystem (IMS) Multi-device Profile, documented in this Permanent Reference Document (PRD), defines a profile that identifies a set of features which are defined in 3GPP specifications that a device (the User Equipment (UE)) and network are required to implement in order to guarantee an interoperable, high quality IMS-based multi-device voice and video telephony service.

Multi-device refers to a logical grouping or federation of devices which may be reached via one or more phone numbers/identities (encompassing both an MSISDN and a Public User Identity (IMPU)). Services available to a federated identity are then available on all of the devices within the federation. A federation thus consists of two or more devices. The identity which represents the federation is inherited from one of the individual devices within the federation. This device is known as a primary device.

A primary device has a Universal Integrated Circuit Card (UICC) and the identity assigned to the federation is one of the UICC-based identities used by that device for its previous set of (individual) services. Other devices in the federation are known as secondary devices.

A federated group of devices can be associated with either a single user (a "single user federation") or else multiple users (a "multi-user federation").

A user can also be allowed to use more than one identity. Using an identity that is in the implicit registration set (IRS) of the served user, follows the normal procedures. Using an identity that is not in the IRS requires the used identity to be in the configured service data of the served user. The concept of multi-identity can be combined with the concept of multi-device.

1.1.2 Support in this version of the document

The primary use of this version of the specification is to allow the support of a federated group of devices to be used by a single user.

The identity of a primary device is used as the default identity of the federation, but other identities within the subscription can be shared by the devices in the federation. This allows the user to make and receive calls on any of their devices.

A federation may have a single federated identity or multiple federated identities. In this version of the specification, multiple federated identities can be in the IRS as specified in 3GPP release 14, allowing the user to use the identities within its own subscription; or identities not in the IRS can be configured in the service data of the user.

A multi-user federation is not in scope of this version of the document.

1.2 Relationship to existing standards

1.2.1 3GPP specifications

This profile is based solely on the specifications as listed in section 1.5. For references to 3GPP, 3GPP Release 14 is taken as a basis; i.e. unless otherwise stated, the latest version of release 14 applies and the same is applicable for other releases if referenced. When GSMA documents are referenced, the base version is as specified in the GSMA documents. Documents of other standards bodies are referenced with a specific version.

1.3 Scope

This document defines a profile for multi-device and multi-identity voice and video services over IMS, by listing a minimum set of IMS core network and UE features and procedures that are considered essential to launch interoperable services. The defined profile is compliant with and based on 3GPP specifications. The scope of this profile is the interface between the UE and network.

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

The present document does not specify any requirements on the federation process. Instead, it specifies the information needed to be provided to the devices in order for the device to successfully use the IMS functions

A network can implement a multi-device service without affecting the UNI, such as mapping a native identity to a federated identity. This specification does not preclude such implementations, but the network functions are out of scope of this specification.

Requirements on the user interface are out of scope of this document.

1.4 Definition of acronyms and terms

1.4.1 Acronyms

Acronym	Description
3GPP	3rd Generation Partnership Project
ALG	Application Layer Gateway
APN	Access Point Name
CW	Communication Waiting
e2ae	end-to-access edge
e2e	end-to-end
EPC	Evolved Packet Core
FIR	Full Intra Request
IMPI	IP Multimedia Private User Identity
IMPU	IP Multimedia Public User Identity
IMS	IP Multimedia Subsystem
IMS-ALG	IMS Application Layer Gateway

Acronym	Description
ISDN	Integrated Services Digital Network
ISIM	IP Multimedia Subscriber Identity Module
IP	Internet protocol
IRS	Implicit Registration Set
MDV2	Multi Device Voice and Video
MSISDN	Mobile Subscriber ISDN Number
NAL	Network Abstraction Layer
PPS	Picture Parameter Set
PRD	Permanent Reference Document
RTCP	RTP Control Protocol
RTP	Real-time Transport Protocol
SDES	Session Description Protocol Security Descriptions for Media Streams
SDP	Session Description Protocol;
SMS	Short Message Service
SIP	Session Initiation Protocol
SPS	Sequence Parameter Set
SRTP	Secure RTP
STUN	Simple Traversal of User Datagram Protocol through Network Address Translations
UDP	User Datagram Protocol
UDUB	User Determined User Busy
UE	User Equipment
UICC	Universal Integrated Circuit Card
URI	Uniform Resource Identifier
USIM	Universal Subscriber Identity Module

1.4.2 Terms

Term	Description
Downloadable Client	An IMS client used to access telephony and messaging services that has been downloaded or pre-installed onto a UE and is unable to access any UICC credentials for telephony services that may be present on the device. When resident on a UE, the UE may act only as a Secondary Device.
Federation	A federation is a group of devices that are configured (via the federation process) to use a given identity, or identities, for telephony and messaging purposes.
Federation Process	The mechanism by which the federation is created/destroyed. The mechanism may be controlled from the UE or other sources. The precise details of the mechanism are out of scope in this version of the document. As part of the federation process the operator can configure the UE with relevant parameters.
Federated identity	An identity used by all of the devices in the federation for telephony and messaging purposes.

Term	Description
Multi-User Federation	A federation of devices which are used by multiple end users/group of users. In this case, the devices of the federation are shared between a group of individuals such as family members, work colleagues or some other group.
Native Client	An IMS client used to access telephony and messaging services that is native to a UE carrying a UICC and able to access the credentials on that UICC. When resident on a UE, the UE may act as a primary or secondary device.
Primary device	A native client that has been selected to provide the federated identity to a federation and that is registered to IMS using credentials (e.g. IP Multimedia Private User Identity (IMPI), IMPU) obtained from an IP Multimedia Subscriber Identity Module (ISIM) or derived from a Universal Subscriber Identity Module (USIM). One (non-barred) IMPU of this device is the federated identity shared with other devices in the federation.
Secondary device	A device that has been selected to belong to a federation that is registered to IMS via any valid IMS authentication mechanism, that has its own IMPI and optionally its own IMPU (which is different from the federated identity), and shares the federated identity from the primary device of the federation.
Single-User Federation	A federation of devices all of which are used by a single end user.
Subscription	IMS subscription as defined in 3GPP TS 23.228 [13]
UE	The term UE is used for devices where it is irrelevant if the device is a primary device or a secondary device.
UICC	In this specification UICC is also used to refer to embedded UICC (eUICC)

1.5 Document cross-references

Ref	Doc Number	Title
[1]	IETF RFC 2119	Key words for use in RFCs to Indicate Requirement Levels.
[2]	GSMA PRD IR.92	IMS Profile for Voice and SMS.
[3]	GSMA PRD IR.94	IMS Profile for Conversational Video Service
[4]	GSMA PRD NG.102	IMS Profile for Converged IP Communications
[5]	void	
[6]	GSMA PRD RCC.14	Service Provider Device Configuration v5.0
[7]	GSMA PRD RCC.15	IMS Device Configuration and Supporting Services v4.0
[8]	GSMA PRD IR.51	IMS Profile for Voice, Video and SMS over untrusted Wi-Fi access v5.0
[9]	IETF RFC 4235	An INVITE-Initiated Dialog Event Package for the Session Initiation Protocol (SIP)
[10]	3GPP TS 24.229	"IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3"
[11]	GSMA PRD NG.106	"IMS profile for Video, Voice and SMS over trusted Wi-Fi access"

Ref	Doc Number	Title
[12]	IETF RFC 7315	"Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3GPP"
[13]	3GPP TS 23.228	IP Multimedia Subsystem (IMS); Stage 2
[14]	IETF RFC 5104	Codec Control Messages in the RTP Audio-Visual Profile with Feedback (AVPF), IETF RFC
[15]	IETF RFC 4961	Symmetric RTP / RTP Control Protocol (RTCP)
[16]	IETF RFC 3711	The Secure Real-time Transport Protocol (SRTP)
[17]	IETF RFC 4568	Session Description Protocol (SDP) Security Descriptions for Media Streams
[18]	3GPP TS 33.328	"IP Multimedia Subsystem (IMS) media plane security"
[19]	3GPP TS 24.174	"Support of multi-device and multi-identity in the IP Multimedia Subsystem (IMS); Stage 3"
[20]	3GPP TS 24.175	"Multi-device and multi-Identity in the IP Multimedia Subsystem (IMS); Management Object (MO)"
[21]	OMA-ERELD-DM-V1_2	Enabler Release Definition for OMA Device Management, Version 1.2
[22]	GSMA PRD TS.32	Technical Adaptation of Devices through Late Customisation

1.6 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 RFC 2119 **Error! Reference source not found.**."

2 IMS feature set

2.1 General

The IMS profile part lists the mandatory capabilities that are required over the Gm reference point. The Multi Device Voice and Video (MDV2) services are based on GSMA PRD IR.92 [2] and GSMA PRD IR.94 [3]. The connection over EPC (Evolved Packet Core) integrated Wi-Fi access are specified in GSMA PRD IR.51 [8] and GSMA PRD NG.106 [11], and over direct Wi-Fi is in GSMA PRD RCC.07 [5].

2.2 Support of generic IMS functions

2.2.1 Registration pre-requisites

In order to perform a SIP registration, the UE first needs to attach to the network, discover a Proxy Call Session Control Function (P-CSCF) address and be provided with at least one identity to be included in the REGISTER request. The source of this data is dependent on whether the device has and uses a UICC for telephony and messaging purposes as indicated in Table 1.

Data Item	Native client	Downloadable client
APN	IMS-APN	Internet APN / Direct Wi-Fi access
P-CSCF Address	As section 4.4 of PRD IR.92 [2] and section 6.9 of PRD IR.51 [8].	Via configuration (e.g. RCC.15 [7])
IMPU	As section 2.2.1 of PRD IR.92 [2].	Via configuration (e.g. RCC.15 [7])
IMPI	As section 2.4.2.2 of PRD NG.102 [4].	Via configuration (e.g. RCC.15 [7])
+sip.instance	As section 2.2.1 of PRD IR.92 [2]	Via configuration (e.g. RCC.15 [7]) or generated by the UE (UUID).

Table 1: Pre-requisite items for IMS Registration

2.2.2 SIP registration procedures

A native client must register to the IMS network for MDV^2 service by following IMS registration procedures, specified in section 2.5 of GSMA PRD NG.102 [4]. A native client supporting audio only must conform to section 2.2.1 of GSMA PRD IR.92 [2] and a native client supporting video, must conform to section 2.2.1 of GSMA PRD IR.94 [3].

A downloadable client must register to the IMS network for MDV^2 service by following IMS registration procedures, specified in section 2.2.1 of GSMA PRD IR.92 [2] for voice support and section 2.2.1 of GSMA PRD IR.94[3] for video support, with the following differences:

- the IMPU and IMPI are obtained as shown in Table 1.
- the +sip.instance header field is obtained as shown in Table 1.
- the Internet APN is used instead of the IMS-APN in line with Table 1.

The registration parameters for native and downloadable clients are summarized in Table 1.

A UE will receive a P-Associated-URI header field, in the 200 (OK) response to the REGISTER request. All identities in the P-Associated-URI are identities within the subscription.

A UE in a federation must subscribe to the reg event package as specified in section 2.2.1 of GSMA PRD IR.92 [2]. This ensures that all federated devices are aware of all other active devices within the federation.

2.2.3 Authentication

A native client and the IMS core network must conform to section 2.2.2 of GSMA PRD IR.92 [2].

A downloadable client should authenticate as described in section 2.12.1.1.2 of GSMA PRD RCC.07 [5]. It is the operator responsibility to provide the device with the necessary credentials via configuration.

2.2.4 Addressing

A UE and the IMS core network must conform to section 2.2.3 of GSMA PRD IR.92 [2].

2.2.5 Call establishment and termination

A UE and the IMS core network must conform to section 2.2.3 of GSMA PRD IR.92 [2] and to section 2.2.2 of GSMA PRD IR.94 [3].

2.2.6 Forking

The UE must conform to section 2.2.5 of GSMA PRD IR.92 [2].

The network must support forking by sending a SIP CANCEL request including a Reason header field with values of:

- SIP; cause=200; text="Call completed elsewhere"
- SIP; cause=603; text="Declined"
- SIP; cause=600; text="Busy Everywhere"

for forked calls as defined in 3GPP TS 24.229 [10].

Note: The network uses Application Server based forking in order to fulfil requirements on parallel or sequential ringing.

As stated in section 2.2.4 of GSMA PRD IR.92 [2], the UE must send a SIP 486 (Busy here) response to the network to indicate User Determined User Busy (UDUB). The Network can treat a 486 (Busy Here) response as a trigger to release other terminating legs via SIP CANCEL based on some criteria independent of the UNI (e.g. if received from the primary device of a federated group). In this case, the Reason header must contain "cause=600" as indicated above.

2.2.7 The use of signalling compression

The UE must not use signalling compression.

2.2.8 Early media and announcements

The UE must conform to section 2.2.7 of GSMA PRD IR.92 [2].

2.2.9 SIP session timer

The UE must conform to section 2.2.8 of GSMA PRD IR.92 [2].

2.3 Supplementary services

IMS supplementary services should be available on all federated devices based on the device capabilities.

2.3.1 Supplementary services overview

The UE and the network must conform to section 2.3 of GSMA PRD IR.92 [2] and section 2.3 of GSMA PRD IR.94 [3] with the additions and clarifications related to multi-device aspects added in the following subsections.

2.3.2 Supplementary service configuration

The primary device uses the Ut interface for supplementary service configuration as specified in section 2.3.2 of GSMA PRD IR.92 [2]. Secondary devices can use other mechanisms not specified in the present document.

2.3.3 Ad-hoc multi party conference

For ad-hoc multiparty conference where one device from the federation participates no specific procedures beyond what is specified in section 2.3.3 of GSMA PRD IR.92 [2] are needed.

When the UE uses an identity not in the IRS for conference calling, the UE must use the same identity for the conference call and the calls to be added to the conference as specified in section 4.6.8.2.1 of 3GPP Release 16 24.174 [19].

2.3.4 Communication waiting

No specific requirements are needed besides what is specified in section 2.3.4 of GSMA PRD IR.92 [2]. The IMS network must treat the early dialogs for the incoming waiting call separately. No multi-device specific procedures are needed, i.e. a busy device receiving an

incoming session gives Communication Waiting (CW) indication to the user whilst other devices ring.

2.3.5 Message waiting indication

No specific requirements are needed besides what is specified in section 2.3.5 of GSMA PRD IR.92 [2].

2.3.6 Originating identification restriction

No specific requirements are needed besides what is specified in section 2.3.6 of GSMA PRD IR.92 [2].

2.3.7 Terminating identification restriction

No specific requirements are needed besides what is specified in section 2.3.7 of GSMA PRD IR.92 [2].

2.3.8 Communication diversion

When the network has determined that a session is to be diverted, the network must cancel any leg in early dialog state.

2.3.9 Communication barring

The IMS network must interpret the conditions related to barring of roaming users based on the location of the device originating/terminating a session.

2.3.10 Communication hold

No specific requirements are needed besides what is specified in section 2.3.10 of GSMA PRD IR.92 [2].

2.3.11 Explicit communication transfer – consultative

For Explicit Communication Transfer where one device from the federation participates, no specific procedures besides what is specified in section 2.3.11 of GSMA PRD IR.92[2] are needed.

2.3.12 Originating identification presentation

No specific requirements are needed besides what is specified in section 2.3.12 of GSMA PRD IR.92 [2].

2.4 Call set-up considerations

2.4.1 SIP precondition considerations

Native clients and the network must conform to section 2.4.1 of GSMA PRD IR.92 [2] and section 2.4.3 of GSMA PRD IR.94 [3].

Downloadable clients can optionally conform to section 2.4.1 of GSMA PRD IR.92 [2] and section 2.4.3 of GSMA PRD IR.94 [3].

2.4.2 Integration of resource management and SIP

Native clients and the network must conform to section 2.4.2 of GSMA PRD IR.92 [2], section 2.4.1 of GSMA PRD IR.94 [3] and section 2.4.2 of GSMA PRD IR.51 [8].

Downloadable clients are not impacted by the integration of resource management and SIP.

2.4.3 Voice media considerations

The UE and the network must conform to section 2.4.3 of GSMA PRD IR.92 [2].

2.4.4 Video media considerations

The UE and the network must conform to section 2.4.2 of GSMA PRD IR.94 [3].

2.4.5 Multimedia considerations

The UE and the network must conform to section 2.4.4 of GSMA PRD IR.92 [2].

2.4.6 Identity considerations

2.4.6.1 Identities in the IRS

The UE receives the identities within the subscription as P-Associated-URIs in the SIP 200 (OK) response to the REGISTER request, see section 2.2.1.

For outgoing calls, the UE and the network must support the P-Preferred-Identity header field in the outgoing INVITE as described in section 5.1.2A.1.1 of 3GPP TS 24.229 [10]. The user can select, which of the available identities within the subscription the user wants to use and if the selected identity is not the default public user identity, the UE must indicate the selected identity in the P-Preferred-Identity header field.

2.4.6.2 Identities not in the IRS

The UE learns the available identities that are outside the subscription either using the Ut interface as specified in section 4.8 of 3GPP Release 16 TS 24.174 [19] or from the device configuration as specified in 3GPP Release 16 TS 24.175 [20]. For outgoing calls, in order to use an identity outside the subscription (i.e. not in the IRS), the UE must include this identity, see section 4.5.3.1 of 3GPP Release 16 TS 24.174 [19], in an Additional-Identity header field, specified in section 7.2.20 of 3GPP Release 16 TS 24.229 [10].

For incoming voice or video call, the network and the UE must support the P-Called-Party-ID header field to indicate the identity to which the received call was addressed as described in RFC 7315 [12].

Note: The P-Preferred-Identity and P-Associated-URI header fields are not supported as AT commands. So there is no standardized mechanism to transport this information between the application layer and the lower layers in the device.

For incoming voice or video calls where the UE has been called using an identity not in the IRS, the UE learns this identity from the Additional-Identity header field, as specified in section 4.5.3.6 of 3GPP Release 16 TS 24.174 [19].

2.4.6.3 Identities delegated to other users

The UE can allow other users to use its own registered identity. The UE learns the identities that are allowed to use its own registered identity either using the Ut interface or using the device configuration as specified in annex A. The UE can activate or deactivate a delegated identity as specified in section 4.5.2 of 3GPP Release 16 24.174 [19].

2.5 SMS over IP

The Identity Considerations described in section 2.4.6 are applied to SMS (Short Message Service) as follows.

For outgoing SMS, the UE and the network must support the P-Preferred-Identity header field in the outgoing MESSAGE as described in section 5.1.2A.1.1 of 3GPP TS 24.229 [10]. The user can select, which of the available identities within the subscription has to use and if the selected identity is not the default public user identity, then the UE must indicate the selected identity in the P-Preferred-Identity header field.

For incoming SMS, the network and the UE must support the P-Called-Party-ID header field to indicate the identity to which the received call was addressed as described in RFC 7315 [12].

Note: It is an operator option to support SMS over IP (Internet Protocol) for secondary devices. How the operator disables SMS over IP for these devices is out of scope for this document.

2.6 Emergency service

2.6.1 General

A native client uses the Mobile Subscriber ISDN Number (MSISDN), the native identity, for originating emergency calls. Emergency calling is a regulatory service which is not affected by multi-device. Emergency calls are defined in GSMA PRDs GSMA PRD IR.92 [2] section 5.2, GSMA PRD IR.94 [3] annex B.2 and GSMA PRD IR.51 [8] section 5.3 and GSMA PRD NG.106 [11] section 5.3.

A primary device uses the identity allocated to the federation to make an emergency call and any callback will go to all the devices in the federation.

A downloadable client may support emergency calls subject to local regulation. In this case, location information may be provided by a market specific mechanism or may not be available.

2.7 Call log

A call log holds pertinent information such as Caller Id, call duration, call type, time of call etc. To use the call log, the UE must support the procedures specified in sections 4.5.3.1 and 4.5.3.6 of 3GPP Release 16 TS 24.174 [19]. The UE learns the call log URI from the UE configuration as specified in 3GPP Release 16 TS 24.175 [20].

When a call is cancelled towards a terminating UE the CANCEL may contain a Reason header as specified in section 2.2.6. The table below provides a mapping between the cause

value and how the UE should label the call in the call log. The call log function must support the following values:

Cause value	Label
200	Call completed elsewhere
408	Missed
600	Rejected/Missed
603	Rejected

Table 2: Cause Value and Label Table

2.8 Radio and Packet Core Feature Set

Native clients and the network must conform to section 4 of GSMA PRD IR.92 [2], section 4 of GSMA PRD IR.94 [3] and section 4 of GSMA PRD IR.51 [4].

2.9 Direct Wi-Fi considerations for secondary devices

2.9.1 RTP and NAT Traversal

To combat the negative effects of NAT traversal on the RTP protocol when connecting over direct Wi-Fi, the client:

- must support a keep-alive mechanism to open and maintain the NAT binding alive regardless of whether the media stream is currently inactive, send-only, receive-only or send-receive. The recommended standard keep-alive mechanism is an empty (no payload) RTP packet with a payload type of 20 (as per 3GPP TS 24.229 [10]).
    - Must when sending empty packets instead of using STUN and it is about to receive a video stream, send these dummy RTP packets at a high rate (recommended range: 50 to 100ms) from the moment the SIP INVITE request is received (or the 180 RINGING is sent) in bursts sent regularly (a 1 second burst every 15 seconds is recommended). This must be done until one of the following conditions is met:
        - The first RTP packet of a video stream is received, or,
        - The client starts streaming itself in case of a bi-directional RTP stream, or,
        - A final response is sent on the SIP INVITE request. In case this final response is a 200 OK response, the client must continuously send the dummy RTP packets until either the first RTP packet of a video stream is received or the client starts streaming itself in case of a bi-directional RTP stream.

      Once the first RTP packet is received, the dummy packets must be sent at a lower rate (a transmission every 15 sec is recommended) for the remainder of a uni-directional session or not at all in case the RTP stream is bi-directional.
    - If the first frame is not an I-Frame or Network Abstraction Layer (NAL) unit carrying a Sequence Parameter Set (SPS) or Picture Parameter Set (PPS), the receiving client must send an RTP Control Protocol (RTCP) Full Intra Request (FIR) (see section 4.3.1 of RFC 5104 [14]) to the sender.

- Must reset the encoder as specified in RFC 5104 [14] when receiving an RTCP FIR, and send SPS, PPS (if not provided in the SDP) and an I-Frame to the receiver.

- Must use symmetric media mechanism (i.e. use the same port number for sending and receiving packets) as defined in RFC 4961 [15] which is summarized below:
  - When an invitation for IP Video Calling is received and accepted, the 200 OK response contains an SDP body with all the necessary fields (including the destination port) for the sender to send the RTP packets.
  - Immediately after sending the 180 Ringing response, the receiver will send a keep-alive packet back to the sender to secure the timely setup of the media path:
  - The source port must be identical to the one included in the m field of the SDP payload inside the 200 OK response.
  - The destination port must be identical to the one included in the m field of the SDP payload inside the SIP INVITE message.
  - The sender should allow enough time for the media path to be secured.

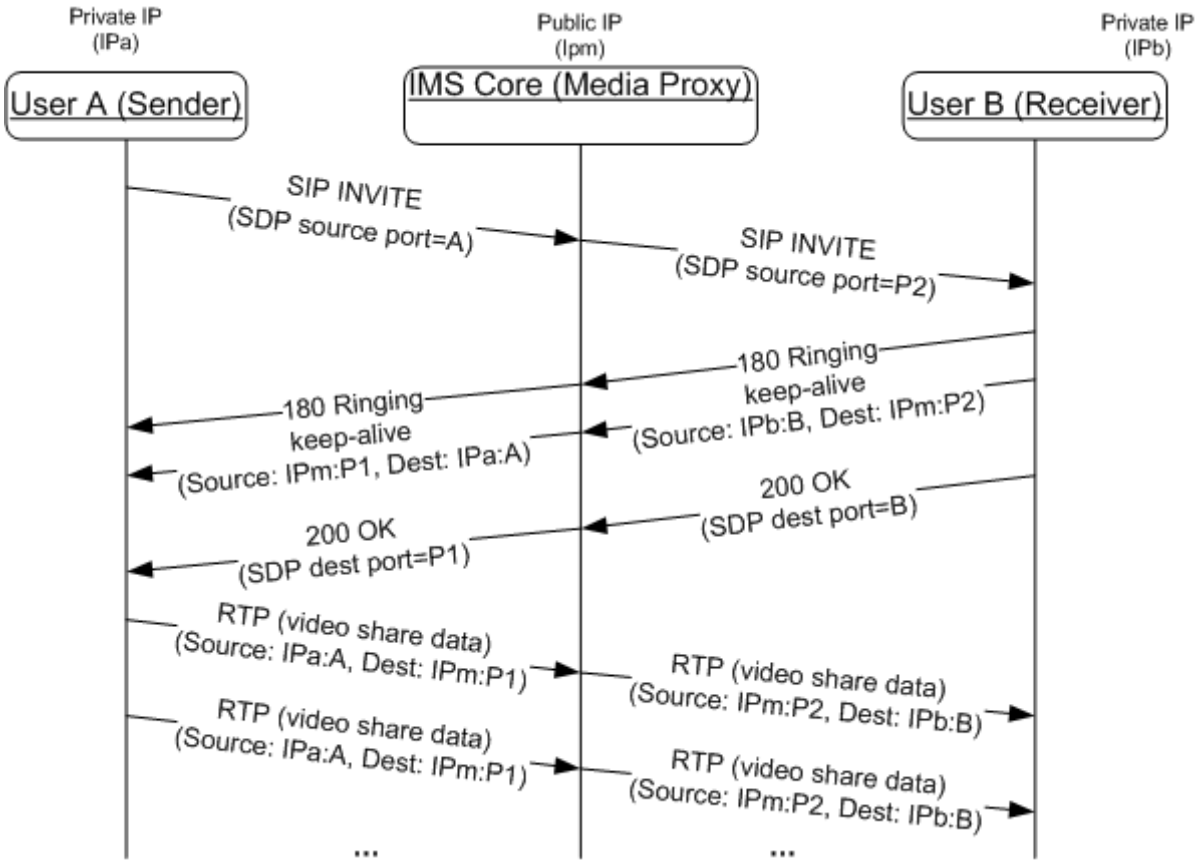

Figure 1: RTP symmetric media path establishment

Note: As a general recommendation, User A should also send a keep-alive once it receives the SDP from the other side.

- Must use RTCP: The symmetric media procedure described for the RTP protocol is, in general, applicable to any UDP stream. As the usage of RTCP is also mandatory, an analogous mechanism must be implemented to prevent any RTCP streams from

being blocked. Therefore, the symmetric media procedure described in this section for RTP is also applicable to RTCP and must be employed (meaning, a dummy packet is sent by the receiver to secure the RTP flow and a second one is used to secure the RTCP flow). Also the sender client must send a dummy packet when the session is established to secure the RTCP flow on their side and ensure the reception of any RTCP RR (Receiver Report) sent by the receiving side. The dummy packet format recommended for establishing the RTCP flow is an empty RTCP RR or empty RTCP SR (Sender Report).

2.9.2 Secure RTP (SRTP)

SRTP as defined in RFC 3711 [16] may be used to provide per message authentication, integrity protection and encryption for both RTP and RTCP streams involved in real-time video and voice sessions.

The use of SRTP is recommended for communications over any untrusted network in which confidentiality (or lack of) is a concern. As an example, a voice or video call over a Wi-Fi network (e.g. “Hot Spot”) without any WLAN (Wireless Local Area Network) encryption is highly susceptible to eavesdropping.

The establishment and key exchange for SRTP must be based on SDES (Session Description Protocol Security Descriptions for Media Streams, RFC4568 [17]) which is transported within SDP, following the SIP SDP offer/answer model. SDES and SRTP profiles for media security in IMS are specified in 3GPP TS 33.328 [18].

Note 1: 3GPP TS 33.328 [18] defines two modes of operation for SDES/SRTP: e2ae (end-to-access edge) mode and e2e (end-to-end) mode. For the e2ae mode, SDES is run between an IMS client and a SIP edge proxy, i.e. a P-CSCF (IMS-ALG or IMS Application Layer Gateway). An IMS access Gateway controlled by a P-CSCF (IMS-ALG) provides the SRTP termination for the “Access Edge”. In the e2e mode, SDES and SRTP is transported end-end between two end user clients.

A client that supports SRTP and SDES and also supports e2ae mode, must indicate this during the IMS registration according to 3GPP TS 24.229 [10]. The P-CSCF (IMS-ALG), if supporting e2ae mode, indicates this to the UE as part of the IMS registration procedures according to 3GPP TS 24.229 [10]. The use of SRTP is enabled through the client configuration parameters (e.g. as per GSMA PRD RCC.15 [7]), and whether it is used or not can be configured differently for Wi-Fi access and cellular access.

However not all end user clients may support SRTP. Therefore, the Service Provider’s network equipment should support e2ae mode. A client that supports SRTP and SDES must also support e2ae mode.

When using SRTP/SDES, the client can include preference of security mode to use in accordance to3GPP TS 33.328 [18]. It is recommended that e2ae mode be used by the UE, if also indicated to be supported by the P-CSCF (IMS-ALG). Otherwise, the client may try e2e by not indicating any preference during the session setup.

Note 2: This does not exclude that the Service Provider network still may decide to terminate the media security in the network (P-CSCF (IMS-ALG)).

For terminating sessions, when the UE has indicated support for e2ae SRTP/SDES in the registration, the P-CSCF (IMS-ALG) must behave as specified in 3GPP TS 24.229 [10], i.e. ensure that SRTP is used, and facilitate interworking from RTP to SRTP when needed.

For terminating session, when the UE has not indicated support for e2ae SRTP/SDES, the P-CSCF (IMS-ALG) decides based on local policy, whether to apply SRTP / SDES towards the UE. A possible local policy is that the P-CSCF (IMS-ALG) invokes procedures related to SDP and SRTP for Wi-Fi access, but not for cellular access.

Note 3: Enforcing SRTP/SDES on the terminating call leg towards a UE that does not support SRTP/SDES will lead to the connection establishment failing, which may be an issue for inbound roaming where the operator has no control of what clients are used, or for cases where there are other clients in the same network that use RTP.

3 Federation and configuration of secondary devices

3.1 General

How the federation (i.e. the association of a primary device with one or more secondary devices) is set up is defined by the operator and is not described in the present document. It is assumed that all UEs in the same federation are provisioned in the same IMS network. The addition/removal of secondary devices can be controlled from the primary device (e.g. via an application) or using other mechanisms. In either case, the network can restrict the size of a federation.

3.2 Secondary device procedures

If the secondary device uses a downloadable client, then it is provided with the necessary data via configuration as described in section 2.2.1. For additional security, devices can use the SMS based configuration mechanism (One Time Password) as described in GSMA PRD RCC.14 [6].

Annex A MNO provisioning and Late Customization

A.1 General

This annex describes the capabilities to support MNO provisioning for the UE to support the mechanisms specified in this document.

A.2 Configuration Methods

A.2.1 Remote Client Configuration for MNO provisioning

The UE and the network must support one of the two configuration methods in order to support MNO provisioning for the parameters that are defined in 3GPP (see also Table 3):

- OMA DM V1.2 with http binding as specified in OMA-ERELD-DM-V1_2 [21]; or
- Service provider device configuration as specified in GSMA PRD RCC.14 [6].

A.2.2 Late Customization

The UE must support late customization as specified in GSMA PRD TS.32 [22] for the parameters in Table 3Table 3.

A.3 Configuration Parameters

Table 3 contains the configuration parameters with their default values that must be supported by the UE and the network. The UE must use the default value for each parameter in Table 3 unless configured differently by any of the methods as described in section A.2.1.

Parameter	Default value	Defined in	See also section
SharedIdentity	No default value	Section 5.6 of 3GPP Release 16 24.175 [20]	2.4.6
DelegatedIdentity	No default value	Section 5.9 of 3GPP Release 16 24.175 [20]	2.4.6.3
Call log URI	No default value	Section 5.11 of 3GPP Release 16 24.175 [20]	2.7

Table 3 Configuration parameters and their default values

Annex B Document Management

B.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
1.0	21/02/2018	NG.110 MUD First Draft	TG	Jörgen Axell, Ericsson

2.0	12/11/2018	Implementation of CR#1002 and CR#1003	TG	Jörgen Axell, Ericsson
3.0	13/5/2020	Implementation of CR#1004 and CR#1005	TG	Jörgen Axell, Ericsson

B.2 Other Information

Type	Description
Document Owner	NG
Editor / Company	Jörgen Axell, Ericsson

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.