TIM Specification for Gm Interface between an User Equipment and the Fixed IMS Network

Rev. 1.1   06/11/2018

INDICE DEGLI ARGOMENTI

1. SCOPE

The present document specifies the requirements on Gm interface of Telecom Italia Fixed IMS core network (i.e. interface between User Equipment and P-CSCF according to IMS Architecture).
It provides detailed information for registration, basic call procedures and FAX/POS/modem support for a UE supposed to interoperate with TIM Fixed IMS core network. As such, this document represent the baseline specification for the interoperability of a UE with the IMS network.

This document is written in the form of a list of requirements. Mandatory requirements are market with **R.** Optional requirements, which a vendor may or may not decide to implement, are marked with **Q.**: the latter have been put in this specification in order to highlight features which can improve the quality of the service for the end customer, or/and more efficient ways to interoperate with the network.

2. APPLICABILITY

The present document is applicable to User Equipments (UEs), e.g. Access Gateways, which are intended to support the TIM VoIP services based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP).

3. NORMATIVE REFERENCES

3.1 INTERNET RFCS

[DOC1] RFC 3261 - SIP: Session Initiation Protocol
[DOC2] RFC 3262 - Reliability of Provisional Responses in the Session Initiation Protocol (SIP)
[DOC3] RFC 3263 - Locating SIP Servers
[DOC4] RFC 3264 - An Offer / Answer Model with the Session Description Protocol (SDP)
[DOC5] RFC 3311 - The Session Initiation Protocol (SIP) UPDATE Method
[DOC6] RFC 3960 - Early Media and Ringing Tone Generation in the Session Initiation Protocol (SIP)
[DOC7] RFC 2617 - HTTP Authentication: basic and Digest Access Authentication
[DOC8] RFC 2833 - RTP Payload for DTMF Digits, telephony tones and telephony signals
[DOC9] RFC 4733 - RTP Payload for DTMF Digits, Telephony Tones, and Telephony Signals
[DOC10] RFC 4566 - SDP: Session Description Protocol
[DOC11] RFC 4028 - Session Timers in the Session Initiation Protocol (SIP)
[DOC12] RFC 3841 - Caller Preferences for the Session Initiation Protocol (SIP)
[DOC13] RFC 3325 - SIP Asserted Identity
[DOC14] RFC 3323 - Anonymous Tag Header
[DOC15] RFC 3515 - Refer
[DOC16] RFC 3891- The Session Initiation Protocol (SIP) “Replaces” Header
[DOC17] RFC 3892 - The Session Initiation Protocol (SIP) Referred-By Mechanism
[DOC18] RFC 3265 – Session Initiation Protocol (SIP) - Specific Event Notification
[DOC19] RFC 3842 - A Message Summary and Message Waiting Indication Event Package for the Session Initiation Protocol (SIP)
[DOC20] RFC3398 - "Integrated Services Digital Network (ISDN) User Part (ISUP) to Session Initiation Protocol (SIP) Mapping"
[DOC21] RFC3327 - Session Initiation Protocol (SIP) Extension Header Field for Registering Non-Adjacent Contacts
[DOC22] RFC5626 - Managing Client-Initiated Connection in the Session Initiation Protocol (SIP)
[DOC23] RFC3840 - Indicating User Agent Capabilities in the Session Initiation Protocol (SIP)
[DOC24] RFC5341 - The Internet Assigned Number Authority (IANA) tel Uniform Resource Identifier (URI) Parameter Registry
[DOC25] RFC5389 – Session Traversal Utilities for NAT
[DOC26] RFC7350 – Datagram Transport Layer Security (DTLS) as Transport for Session Traversal Utilities for NAT (STUN)

[DOC27] RFC2474 – Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 headers

[DOC28] RFC4961 - Symmetric RTP / RTP Control Protocol (RTCP)

[DOC29] RFC5009 - Private Header (P-Header) Extension to the Session Initiation Protocol (SIP) for Authorization of Early Media

[DOC30] RFC3407 - Session Description Protocol (SDP) Simple Capability Declaration

[DOC31] RFC5939 - Session Description Protocol (SDP) Capability Negotiation

[DOC32] RFC 3550 - RTP: A Transport Protocol for Real-Time Applications

[DOC33] RFC 3551 - RTP Profile for Audio and Video Conferences with Minimal Control

[DOC34] RFC 3605 - Real Time Control Protocol (RTCP) attribute in Session Description Protocol (SDP)

[DOC35] RFC 2198 - RTP Payload for Redundant Audio Data

3.2 3GPP STANDARDS

[DOC36] 3GPP TS 23.228 V8.8.0 (2009-03) - IP Multimedia Subsystem (IMS); Stage 2 (Release 8)

[DOC37] 3GPP TS 24.229 V8.7.0 (2009-03) - IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3 (Release 8)

[DOC38] 3GPP TS 23.003 V15.3.0 (2018-03) - Numbering, addressing and identification

3.3 ITU-T RECOMMENDATIONS

[DOC39] G.711 (11/09): Pulse code modulation (PCM) of voice frequencies

[DOC40] G.729 (06/12): Coding of speech at 8 kbit/s using conjugate-structure algebraic-code-excited linear prediction (CS-ACELP)

[DOC41] G.722 (09/12): 7 kHz audio-coding within 64 kbit/s

[DOC42] T.38 (11/15): Procedures for real-time Group 3 facsimile communication over IP networks

4. NETWORK ARCHITECTURE

TIM Network Architecture is compliant to IMS standard [DOC36] and is illustrated in Figure 1. The main functional entities in IMS are:

- **HSS (Home Subscriber Server)**: it is the central repository Database for User information. Information held in HSS comprises user identification, security, location and subscription profile;
- **SLF (Subscription Locator Function)**: in an IMS network comprising multiple HSS instances, the SLF performs identification of the HSS containing the Subscription of a giver User.
- **DNS ENUM (Domain Name Server e.164 number to SIP Address Mapping)**: ENUM is a standard defined in IETF which maps telephone number address space into the DNS. The DNS resource records can then be used to map the telephone numbers into a collection of service addresses.
- **LRF (Location Retrieval Function)**: provides to E-CSCF location information of users, in order to facilitate the routing of emergency call to a suitable PSAP (Public Safety Answering Point).
- **Call Session Control Function (CSCF):** performs routing and control of multimedia sessions. It is instantiated in four different entities:
    - **P-CSCF (Proxy CSCF)**: it is the outbound proxy for the SIP messages generated by the CPEs; performs media proxy for all session-related media streams generated by the CPEs, performing the role of QoS Policy Enforcement Point; provide access to Emergency services, without the involvement of the S-CSCF of the calling user;
    - **I-CSCF (Interrogating CSCF):** identifies the S-CSCF in charge for the calling User
    - **S-CSCF (Serving CSCF):** performs call control of multimedia sessions; provides the functionality of SIP Proxy and SIP Registrar; performs Application Server selection based on the Filter Criteria defined in the Trigger List contained in the HSS.
    - **E-CSCF (Emergency CSCF)**: performs routing of Emergency Calls, received from P- and S-CSCF, towards suitable destinations called PSAPs (Public Safety Answering Points).
- **AS (Application Server)**: performs service execution function; an example is the MTAS (Multimedia Telephony Application Server) which provides Supplementary Services such as CLIP/CLIR (Calling Line Identity Presentation / Restriction), Call Hold, Call Waiting, Three-Party, …
- **MRF (Multimedia Resource Function)**: provides announcements and voice/video interaction with users;
- **MGCF (Media Gateway Control Function)** and **MGF (Media Gateway Functions)**: these functions are performed in TIM network by the GTW-M (Gateway Metropolitano) Nodes

- **IBCF (Interconnection Border Control Function)** and **IBGF (Interconnection Border Gateway Function)**: these functions are performed by the GTW-M together with SBC NNI nodes.

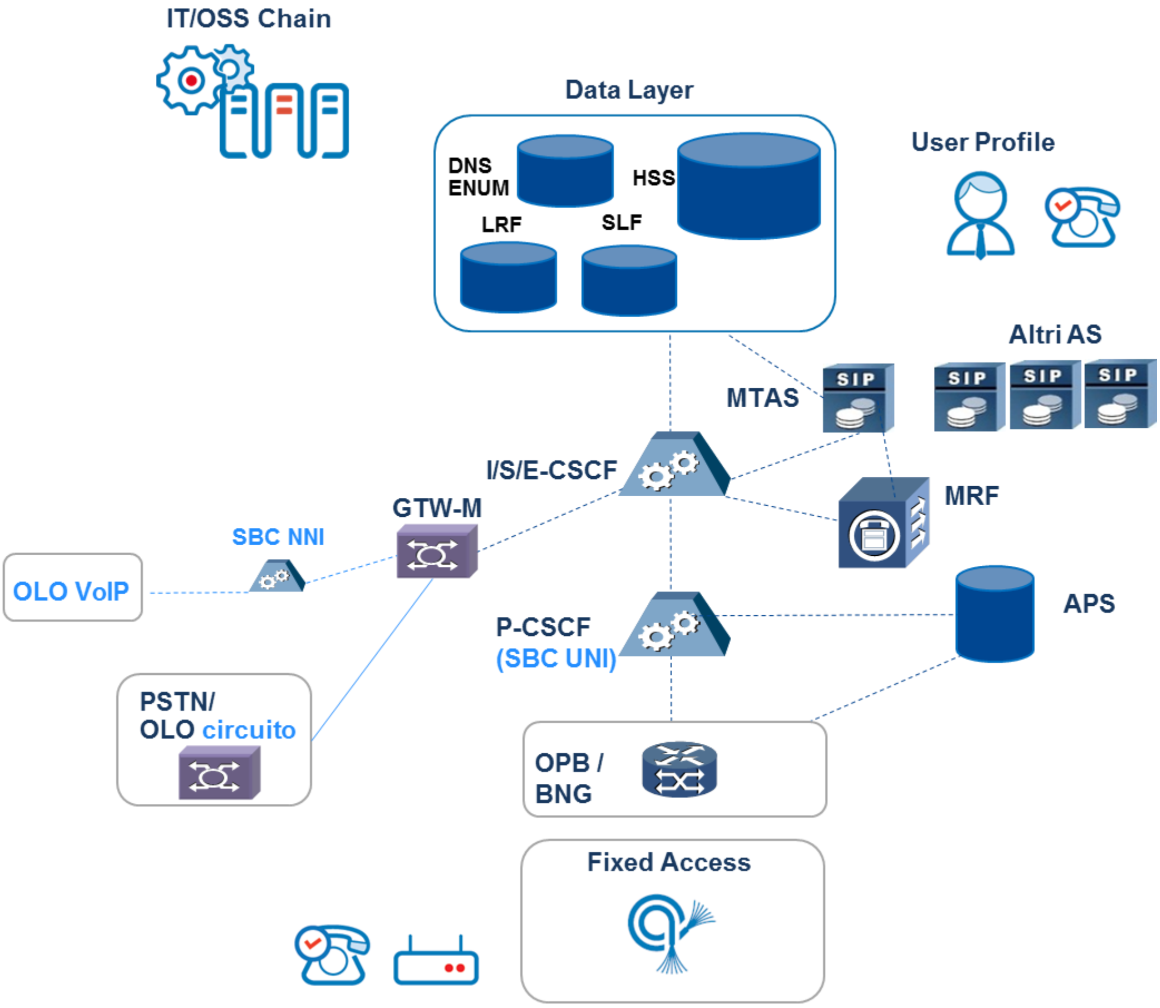

Figure 1: Telecom Italia Fixed IMS Core Network Architecture

5. GM INTERFACE

The access signalling interface between the UE (User Equipment) and the first point of signalling handling of the fixed IMS, represented by the P-CSCF (Proxy Call Session Control Function), is referenced as Gm in the IMS Architecture (ref. [DOC36]).

This interface is based on SIP as signalling protocol: SIP is defined by IETF in RFC 3261 [DOC1] as for the Core part, any in many other RFCs for extensions, some of which have been produced under solicitation of 3GPP.

Stage 3 definition of the Gm Interface, contained in 3GPP TS 24.229 (ref. [DOC37]) defines the exact protocol usage of the SIP protocol elements, defined in IETF, as signalling protocol at the access of the IMS.

Figure 2 represents the reference model.

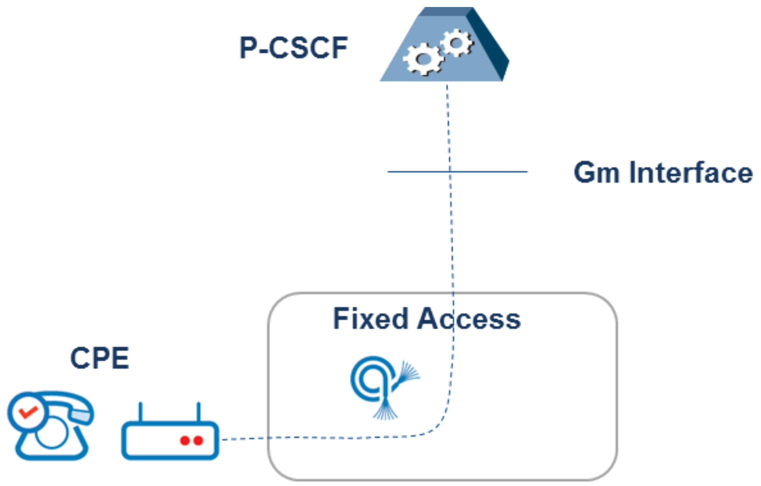

Figure 2: Telecom Italia Fixed IMS Core Network Architecture

5.1 Common Aspects

5.1.1 Identity and SIP URLs

[R.1]. The UE shall use the public user identity defined in 3GPP 23.003 ([DOC38]), par. 13.4. In particular, the UE shall use a SIP URL format, with the username part in E.164 telephone number, in international format: e.g. sip:+390612345678@telecomitalia.it. This identity shall be used also for incoming sessions.

[R.2]. For Request-URI, the UE shall use a SIP URL complying with RFC 3261 [DOC1], with:

- the “username” set to the user selection (dialed number).
- the “domain” set to the SIP domain name (telecomitalia.it)
- the "user" parameter set to "phone" (this point is optional)

[R.3]. Where the username part of the SIP URL contains “*” and “#” characters:

- The * character shall be codec normally in ASCII
- The # character shall be URL-encoded, i.e. shall be encoded as: %23

[Q.1]. For Request-URI, the UE can use, in alternative, a tel-URI, complying with RFC 5341 ([DOC24]).

5.1.2 Dial Plan

[R.4]. The UE must support an open numbering plan; that is, the length of a selection is not defined nor predictable.

[R.5]. The UE shall support en-bloc selection towards the IMS network. Overlap selection is not supported by the IMS network.

[R.6]. If the UE is supporting a FXS interface or a FXS-like user experience and dialpad, then it must support the following interdigit timeouts:

1. Initial digit timeout (start timer): shall be in the interval 10-30 seconds
2. Interdigit timeout: shall be in the interval 3-6 seconds

[R.7]. If the user selection begins with * or #, a trailing # digit is part of the user selection (i.e. shall not be interpreted as an end-of-selection in order to speed-up sending the INVITE towards the network); hence, it shall be put in the Request-URI as part of the selection.

[Q.2]. If the user selection does not begin with * nor with #, a trailing # digit can be interpreted as an end-of-selection signal, in order to speed-up sending the INVITE towards the network, and can be omitted in the Request-URI.

[Q.3]. If the user selection corresponds to one of the following emergency numbers: 112, 113, 115, 118, the UE should send the INVITE towards the network immediately, without waiting for the Interdigit timeout expiry. The list of emergency numbers should be configurable.

5.1.3 UE CONFIGURATION

[R.8]. The minimum set of configurable parameters in the UE is (mandatory):

- the public user identity (as defined in §5.1.1)
- the SIP domain name (UserAgentDomain/URI)
- the private user identity, as specified in 3GPP TS 23.228 ([DOC36]) par. 4.3.3.1 ; this parameter is used as username in SIP Digest authentication procedure; it is different from public user identity
- authentication password: used in SIP Digest authentication procedure (RFC 2617 – [DOC7]); it is required to support password lengths up to 64 characters.
- an outbound proxy: it is required the support of FQDN, as specified in par. 5.1.4.

5.1.4 DNS QUERY FOR LOCATING SIP SERVERS

[R.9]. It is required the support of RFC3263 (Locating Sip Servers – [DOC3]) for DNS queries in order to resolve Outbound Proxy FQDN. In particular, the UE shall support the RFC paragraphs 4.1 (Selecting a Transport Protocol) and 4.2 (Determining Port and IP Address), including weight and Priority.

5.1.5 USER-AGENT HEADER

[R.10]. The UE must send the User-Agent header in all SIP messages.

[Q.4]. The detailed format of the User-Agent header is up to the vendor. However, it should contain:

- In case of Physical UE:
  - UE Vendor name
  - Product Name/Model

- Firmware Version
  - Hardware Version
- In case of Software Applications:
  - Product Name and Version
  - Operating System and Version
  - Device Model/Vendor

5.1.6 LOCAL TONES AND RINGER PATTERNS

[R.11]. When required, the UE shall generate local tones according to the Table 5-1 and mapped with SIP Message in according to Table 5-2.

Tone		
Dial	Frequency	425 ± 15 Hz
	Cadence	200 ± 20 on
		200 ± 20 off
		600 ± 60 on
		1000 ± 100 off
		(repeated)
	Level	-17 ± 2 dBm
Fast Busy/ Failure	Frequency	425 ± 15 Hz
	Cadence	200 ± 20 on
		200 ±20 off
		(repeated)
	Level	-17 ± 2 dBm
Busy	Frequency	425 ± 15 Hz
	Cadence	500 ± 50 on
		500 ± 50 off
		(repeated)
	Level	-17 ± 2 dBm
Ringing	Frequency	425 ± 15 Hz
	Cadence	1000 ± 100 ms on
		4000 ± 400 ms off
	Level	-17 ± 2 dBm

Table 5-1 – Local tones characteristics

SIP MESSAGE	TONE
180	Ringing
488	Fast Busy
486, 600	Busy
4xx	Fast Busy
5xx	Fast Busy
6xx	Fast Busy

Table 5-2 – Local tones mapping with SIP Message

[Q.5]. Optionally, the UE can generate the following tone:

Tone		
Confirm/ Successful	Frequency	425 ± 15 Hz
	Cadence	Continuous
	Level	-17 ± 2 dBm

The Confirm/Successful is not mapped at the moment to a specific signalling criteria. It is for future use.

[Q.6]. Optionally, the UE can generate the following ringer pattern:

Ringer pattern		
CCBS	Cadence	400 ± 50 on
		200 ± 50 off
		400 ± 50 on
		200 ± 50 off
		800 ± 100 on
		4000 ± 100 off
		(repeated)

The CCBS ringer shall be played in case the incoming INVITE contains a specific alert-info Header:

```
Alert-Info: <urn:alert:service:auto-callback>
```

5.1.7 DSCP MARKING

[R.12]. The UE shall mark the Diffserv code point of IP packets (ref. [DOC27]) carrying outgoing SIP signaling and RTP/RTCP packets with the value: 40 (dec) = 0x28 (hex).

5.2 Registration and Authentication

[R.13]. The UE must be compliant to 3GPP TS 24.229 [DOC37] for registration and authentication procedures. The authentication mode required is “SIP Digest without TLS”, that is also compliant to:

- RFC3261 [DOC1] about the usage of HTTP authentication in SIP
- RFC2617 [DOC7] about challenge-based authentication mechanism

[Q.7]. In order to improve user experience, the the UE should be compliant to RFC5626 (Managing Client-Initiated Connections in SIP) (ref. [DOC22]), in particular, as regards the use of reg-id and +sip.instance tags. The latter tag is important in order to handle properly multiple registrations of a User Agent that may occur in case of IP address change of the UA, without impact on the multi-contact feature provided by the Network.

[R.14]. The UE shall use digest authentication for the following methods: REGISTER (first registration and registration refresh) and INVITE. Should not be authenticated: ACK, CANCEL and all the other SIP messages sent in a dialog (reINVITE, REFER, BYE, OPTIONS).

[R.15]. The UE shall propose an expire time of at least 600000 seconds (see 3GPP 24.229, par. 5.1.1.2.1).

5.2.1 Indicating User Agent Capabilities (RFC3840)

[Q.8]. In order to improve user experience, the UE should support the User Agent Capabilities (RFC3840 [DOC23]). If RFC3840 is supported, the UE shall put the following Tags in the `Contact` header:

```
audio; +g.3gpp.icsi-ref=”urn%3Aurn-7%3A3gpp-service.ims.icsi.mmtel”
```

5.2.2 Authentication with Digest and Sychronization for Registration

[R.16]. According to 3GPP 24.229, par. 5.1.1.2.3, the UE shall perform the first authentication request, in alternative:

1. Without credentials
2. With credentials, by properly populating:

i. the `username` field in the `Authorization` header, with the configured Authorization Username (private user identity)
ii. the “realm” header field parameter, set to the domain name of the home network (telecomitalia.it)
iii. the “uri” header field directive, set to the SIP URI of the domain name of the home network (sip:telecomitalia.it)
iv. the “nonce” header field parameter, set to an empty value; and
v. the “response” header field parameter, set to an empty value.

[R.17]. The UE shall accept Authentication challenges contained in 401 Responses

[R.18]. The UE shall respond to Authentication challenges by resending the REGISTER Method including the `Authorization` header, which shall contain the Authentication Response computed according to the hash MD5 algorithm (more details are contained in “22 Usage of HTTP Authentication” – RFC3261 [DOC1] and RFC2617 [DOC7])

[R.19]. The UE shall use the NC (nonce count) in order to synchronize UE and network as regards Authentication Challenges/Responses and avoid unnecessary challenges.

[R.20]. The `Authorization` header, in response to 401 Challenges, shall contain the following information:

- `Digest username`: authentication username (private user identity)
- `nonce`: provided by network in 401
- `cnonce`: generated from UE
- `nc`: nonce count, used to compute responses; it states the number of requests performed by the UE using the same value of *nonce*
- `realm`: provided by network in 401
- `uri`: suggested `sip:telecomitalia.it`
- `qop`: provided by network in 401; TIM Network uses `qop=”auth”`, hence the UE is expected to behave coherently, according to RFC 2617
- `Algorithm:` provided by network in 401; TIM uses `MD5`
- `response:` shall be computed, based on MD5 algorithm, from the following parameters: `nonce`, `cnonce`, `nc`, `realm`, SIP password (Authentication Password)

[R.21]. As per RFC 3261 and 2617, the UE shall NEVER send the Authentication Password in any message to the network.

[R.22]. After the first successful authentication, the UE can compute the following authentication responses, using the same parameters exchanged at the first authentication request, by simply incrementing the nonce count (NC). Please note that the NC is in exadecimal format.

[Q.9]. In order to avoid signalling overload the UE should support `Authentication-Info` header provided by the network in 200 OK response to Digest challenge. In particular if `Authentication-Info` contains a NONCE value, the UE should use this NONCE to fill in the `Authorization` Header of the next message to be sent to the network; if the `Authentication Info` does not contain a NONCE value, the UE should reuse the same the NONCE already used since it's still valid and must increment nonce count (nc=nc+1).

5.2.3 Digest Authentication Failure Management

[R.23]. The digest response authentication can fail for two reasons:

1. Nonce expiration
The network sends 401 with header **"stale=true"** indicating that the previous request from the client was rejected because the nonce value was stale.
The UAC must retry the authentication with new credential. In this way the UAC and UAS synchronize "nc=1" and new nonce, Cnonce

2. Wrong digest credential
The network sends 401 with header **"stale=false"** indicating that the UAC credential are wrong (wrong password or wrong algorithm)
The UAC must retry the authentication using the time shows in "`Rety-After`" header build in 401 network message. If the "`Retry-After`" header is empty, the default parameter shall be used (600000s).

5.2.4 Autorizathion

[Q.10]. In order to prevent VoIP nomadism, the network perform a specific control to check if the REGISTER and the INVITE sent from the UE, is coming from the IP Address assigned dynamically by the network to the UE. In case this check fails, the network responds to INVITE or REGISTER methods, with a specific Response Code (403 No Roaming Agreement).

5.2.5 Registration

[R.24]. The UE shall perform Registration request for each configured SIP identity.

[R.25]. In order to improve user Experience, the UE shall support Retry-after header.

[R.26]. In case of Failure when the transaction layer times out without ever having received any response, provisional or final (i.e., timer B or timer F in RFC 3261 [1] fires), the UE shall try a new registration sent to the next element in the list obtained in resolution of the FQDN of P-CSCF, as per RFC3263 (see [R.9])

[R.27]. Registration state has a validity defined by the Expiration timer. The UE shall comply to this Expire Time and to the registration states defined in RFC 3261 and 3GPP 24.229, as regards the policy for registration refresh (in case of successful registration) and retries (in case of failed registrations):

Specs	200 Ok	4xx, 5xx, 6xx with Retry-After	401 stale=true	401 stale=false	4xx, 5xx, 6xx	Timer F Expiry
[DOC36]	If Exp_{time} > 1200 Exp_{time} – 600 If Exp_{time} < 1200 Exp_{time} /2	Retry-after time	0 seconds (immediately)	retry-after time or default (600000 s)	See 3GPP 24.229 par. 5.1.1.2.1 and RFC5626 par. 4.5	

Table 3

Note: in the Table above, Timer F Expiry refers to the case of final failure after all the P-CSCF choices listed in FQDN resolution, have failed.

[Q.11]. The UE should support Registration Event Package according to 3GPP TS 24.229 and RFC3680.

[Q.12]. The UE should support P-Associated-URI as defined in 3GPP TS 24.229.

5.2.6 Authentication with Digest and Sychronization for Non-Registration (INVITE)

[R.28]. After successful Registration, the UE shall send all Requests to the P-CSCF discovered by the registration process.

[R.29]. In case of failed registration, the UE shall try to send Requests to the P-CSCF resolved in [R.9].

[R.30]. Based of 3GPP 24.229, par. 4.14.2, when the UE originates a session it can detect that a P-CSCF is not reachable based on no response from the P-CSCF in which case the UE selects another P-CSCF if possible and performs a new initial registration, as per [R.9].

[R.31]. The UE shall accept Authentication challenges to non-REGISTER methods contained in 407 Responses

[R.32]. The UE shall respond to Authentication Request by resending the INVITE Method including the `Proxy-Authorization` header, which shall contain the Authentication Response with the computed according to the hash MD5 algorithm (more details are contained in "22 Usage of HTTP Authentication" – RFC3261 [DOC1] and RFC2617 [DOC7]).

[R.33]. The UE shall use the NC (nonce count) in order to synchronize UE and network as regards Authentication Challenges/Responses and avoid unnecessary challenges.

[R.34]. The `Proxy-Authorization` header, in response to 407 Challenges, shall contain the following information:

- `Digest username`: authentication username (private user identity)
- `nonce`: provided by network in 407
- `cnonce`: generated from UE
- `nc`: nonce count, used to compute responses; it states the number of requests performed by the UE using the same value of *nonce*
- `realm`: provided by network in 407
- `uri`: suggested [`sip:telecomitalia.it`](sip:telecomitalia.it)
- `qop`: provided by network in 407; TIM Network uses `qop="auth",` hence the UE is expected to behave coherently, according to RFC 2617
- `Algorithm:` provided by network in 407; TIM uses `MD5`
- `response:` shall be computed, based on MD5 algorithm, from the following parameters: `nonce, cnonce, nc, realm,` SIP password (Authentication Password)

[R.35]. After the first successful authentication, the UE can compute the following authentication responses, using the same parameters exchanged at the first authentication request, by simply incrementing the nonce count (NC). Please note that the NC is in exadecimal format.

5.3 BASIC CALL

[R.36]. The UE must be compliant with the following RFCs:

- RFC3261 – SIP protocol ([DOC1])
- RFC3262 – Reliability of Provisional Responses (100rel Support/PRACK) ([DOC2])
- RFC3264 – the Offer/Answer Model (SDP) ([DOC4])
- RFC3311 – the UPDATE method ([DOC5])

[R.37]. The UE must be compliant to 3GPP TS 24.229 ([DOC37]) as amended by TIM.

[Q.13]. The UE may insert a P-Preferred-Identity header in any initial request for a dialog or request for a standalone transaction as a hint for creation of an asserted identity, as per 3GPP 24.229 and RFC3325 ([DOC13]).

[R.38]. The UE must must be able to accept incoming INVITE without SDP, in this case the UE shall perform the SDP offer in the first 1xx or 200 Response, as specified in RFC3264 and RFC3262 ([DOC2]).

[R.39]. For incoming signalling, the UE must support both SIP-URI and tel-URI.

[Q.14]. For UE equipped with FXS port(s), the vendor should provide information about the possibility to send a “forced” SIP Registration when off-hook condition is detected on the FXS ports and, consequently, to send out to the network an outgoing INVITE if the user has dialled a phone number regardless to the answer provided by the network to the previous “forced” SIP Registration. In case this INVITE is refused by the network with a 403 answer, no other INVITE has to be sent.

5.3.1 CODEC

[R.40]. The UE must support the audio codecs compliant to the ITU-T recommendations G.729 ([DOC40]) and G.711 A-law ([DOC39]). These codecs shall be offered in SDPs in the following priority order:

- G.729
- G.711 A-law

[R.41]. Annex b. of G.729 and G.711 µ-Law are not supported and should not be offered in SDP.

[R.42]. The packetization period for all audio codecs shall be 20 ms.

[R.43]. The UE must send and receive DTMF tones complying with RFC2833/RFC4733 [DOC8]/[DOC9], with the following sdp attribute required:

```
a=fmtp:<format> 0-15
```
or
```
a=fmtp:<format> 0-16
```

[Q.15]. In order to improve customer experience, the UE can support wide-band audio codec compliant to the ITU-T recommendation G722 ([DOC41]). In case of support of such codec, the codecs shall be offered in SDPs in the following priority order:

- **G.722**
- G.729
- G.711 A-law

[R.44]. Other audio codecs than those mentioned above are not supported and should not be offered.

[R.45]. Voice Activity Detection should be disabled.

[R.46]. The UE must support an echo canceller compliant to ITU-T G.131, for managing delays less than 150 ms.

5.3.2 RTP

[R.47]. The UE must support RFC 3550 (RTP) [DOC32], RFC 3551 (RTP Profile for Audio and Video Conferences with Minimal Control) [DOC33], RFC 3605 (RTCP) [DOC34], RFC 2198 (RTP Payload for Redundant Audio Data) [DOC35].

[R.48]. The UE shall use Symmetric RTP and RTCP, i.e. the UE shall transmit RTP/RTCP packets using the same UDP port used for receiving RTP/RTCP packets, as stated in RFC4961 ([DOC28]).

5.3.3 Early Media and Ringing Tone Generation

[R.49]. The UE, for Early Media and Ringing Tone Generation, must be compliant, in alternative, to:

- RFC5009 ([DOC29]) , about P-Early-Media header;
- RFC3960 [DOC6], in particular with the “Gateway Model”.

[R.50]. When a UE has sent the SDP offer, it must be prepared to receive media for any streams described by that offer, as described in RFC3264 [DOC4], even before receiving any SIP provisional response (this requirement is needed to avoid media clipping).

[Q.16]. The vendor should provide, in any case, detailed information about the current or future support of P-Early-Media header, as specified in RFC5009 ([DOC29]).

[Q.17]. In case the UE is compliant to RFC3960, the UE, for ringing tone generation, should implement the following local policy, derived from the example contained in RFC3960:

1. Unless a 180 (Ringing) response is received, never generate local ringing.
2. If a 180 (Ringing) has been received but there are no incoming media packets or incoming media packets containing silence, generate local ringing.
3. If a 180 (Ringing) has been received and there are incoming media packets, not containing silence, play them and do not generate local ringing.

5.3.4 Use of RE-INVITE and UPDATE

[R.51]. The support of RE-INVITE and UPDATE methods is required, as many service scenarios foresee the use of such methods.

[R.52]. The use of UPDATE method must be accompanied by 100rel/PRACK (see §5.3.5).

5.3.4.1 reINVITE/UPDATE synchonization and 491 response

[R.53]. The reINVITE/UPDATE synchronization within an existing dialog must be handled through the 491 Request Pending Response, as specified in RFC3261.

5.3.5 Reliability of Provisional Responses (100rel / PRACK)

[R.54]. UE must support the Reliability of Provisional Responses as defined in RFC3262 [DOC2]. The UE must insert the following header in INVITEs:
`Supported:100rel`

[R.55]. UE must support also “The Offer/Answer Model” which enables the SDP exchange in PRACK request and response (ref §5 in RFC3262).

5.3.6 CALLER PREFERENCES (RFC3841)

[Q.18]. In order to improve user experience, the UE should support the Caller Preferences (RFC3841 [DOC12]) in order to remark in `INVITE` the type of session originated by means of header `Accept-Contact`. If the `Accept-Contact` header is present, the following Tags must be present:

```
*; audio; +g.3gpp.icsi-ref="urn%3Aurn-7%3A3gpp-service.ims.icsi.mmtel"
```

5.4 FAX/POS/MODEM SUPPORT

[R.56]. If the UE is supporting a FXS interface, then it must support FAX transmission, at least by means of upspeed to G.711.

[R.57]. If the UE is supporting a FXS interface, then it must support modem and POS transmission, by means of upspeed to G.711.

[Q.19]. The called UE should send the ReINVITE (upspeed to G.711), when it detects the CED/ANSam in case of FAX; in case of modem/POS, the called UE should send the ReINVITE (upspeed to G.711), when it detects the modem carrier signal. Hence, a calling UE should not send a ReINVITE.

[R.58]. In case of a race condition due to simultaneous ReINVITE from both UE, the procedure mentioned in §5.3.4.1 shall be applied.

[Q.20]. The UE should support T.38, as specified in ITU-T T.38 (09/2010) ([DOC42]) and RFC 3407 ([DOC30]). In particular:

a. The UE should include, in the SDP Offer of the INVITE, the line `a=cdsc:1 image udptl t38`
b. The called UE should perform an upspeed to T.38, by sending a ReINVITE, if in the received INVITE is present the line `a=cdsc:1 image udptl t38`. The called UE should send the ReINVITE (upspeed to T.38), when it detects the V.21 preamble.

[Q.21]. The UE can support the capabilities for T.38 defined by 3GPP 24.229, ITU-T T.38 and RFC5939 ([DOC31]).

[R.59]. In case a ReINVITE fails, for example because the remote party is unable to perform upspeed (488 Not Acceptabe Here Response), the UE shall continue the session using the previously negotiated codec(s). In this case, the UE can send a ReINVITE to confirm again to the remote party the previously negotiated codecs.

5.5 COMMUNICATION QUALITY MEASUREMENTS

Will be defined in next revisions of the document.

5.6 MISCELLANEOUS SECURITY REQUIREMENTS

[Q.22]. The UE should discard silently any SIP ot RTP packet coming from IP source addresses different from the IP Address of the P-CSCF discovered by the Registration Procedure (see §5.1.4).

------------%%%%%%%-----------