Reference Guide

IMS Procedures and Protocols

The LTE User Equipment Perspective

TABLE OF CONTENTS

1. EXECUTIVE SUMMARY

This reference guide presents an overview of the procedures and protocols used in IMS-based LTE systems, from the perspective of the UE. To illustrate the concepts being discussed, several sample protocol exchanges, captured from a live network, are broken down and described in more detail.

2. INTRODUCTION

IMS represents a substantial challenge to those charged with developing LTE UEs. For one thing, the flexibility allowed in offer/answer SIP messaging represents a double-edged sword. While the advantages of flexibility are obvious, one resulting challenge is a large number of equally valid protocol flows. Unless both the intuitive intent and details of the protocols are understood, developers can be tempted to design for specific known cases rather than for all valid cases.

CORRESPONDING LITERATURE

WHITE PAPER

IMS Architecture:
The LTE User Equipment Perspective

WHITE PAPER

VoLTE Deployment and The Radio Access Network:
The LTE User Equipment Perspective

POSTERS

IMS/VoLTE Reference Guide
LTE and the Mobile Internet

Today's UE developers must deal with increased complexity on a variety of fronts. The deployment of LTE introduces a multitude of inter-RAT (Radio Access Technology) mobility scenarios, new antenna techniques such as MIMO and Quality of Service (QoS) challenges with next-generation services such as Voice over LTE (VoLTE). With IMS and its associated Session Initiation Protocol (SIP) being essential in deploying LTE services, UE developers and wireless operators continue to focus on IMS functional and SIP signaling conformance testing.

Most discussions of IMS protocols are general overviews containing a small minority of content of interest to the UE developer. This paper is an attempt to provide an intuitive introduction to IMS procedures and protocols, focusing on those concepts most relevant to the UE designer in deploying LTE services such as VoLTE.

3. IMS PROCEDURES

Any discussion of IMS protocols must start with a dialogue describing the procedures being implemented. It is important to note that there is no "one size fits all" procedural flow; IMS in LTE offers a lot of flexibility to both network equipment manufacturers and network operators. Note that the processes described here are strictly from the UE's point of view, without discussion of the many intra-network procedures required to make the system work.

The processes involved in a Voice over LTE (VoLTE) call can provide a meaningful background and a fairly typical scenario. From the UE's point of view the initial step is to "listen" for system information in the form of Master Information Blocks (MIBs) and System Information Blocks (SIBs). Once that information has been processed the UE can initiate its own processes. These processes are outlined in the next section. The graphical depiction in Figure 1 is not meant to distinguish between multiple protocol layers; it is merely an intuitive impression of the required processes.

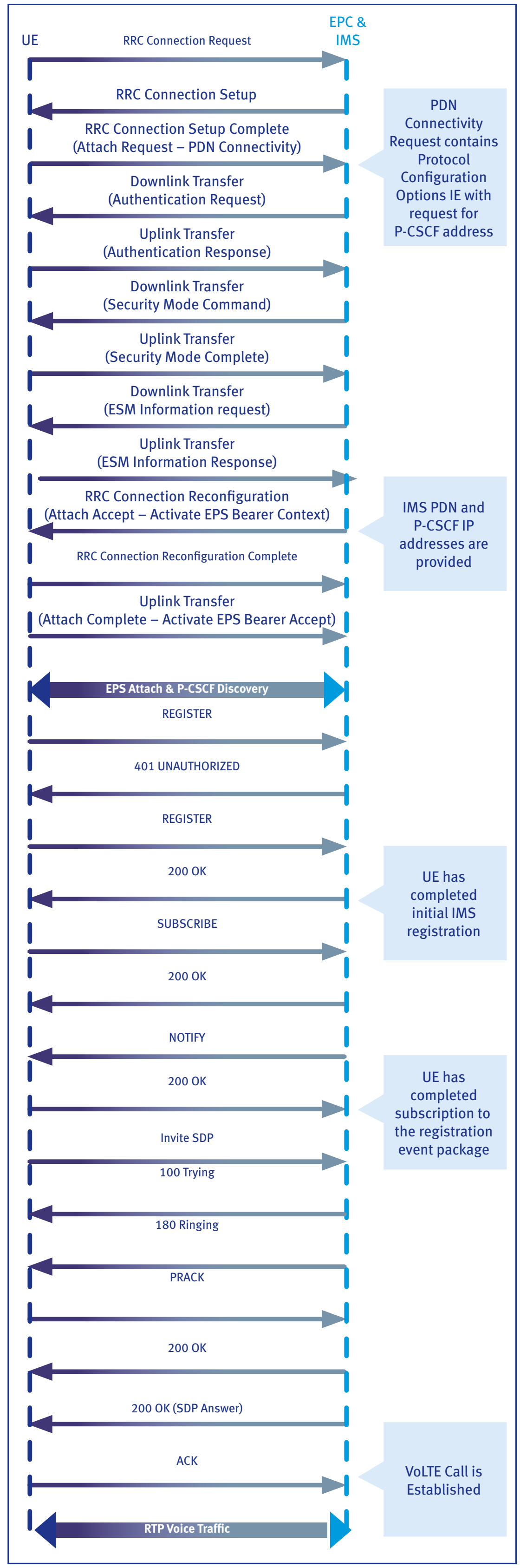
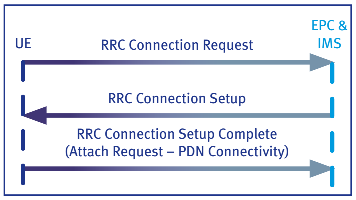


Figure 1 - Multi-layer procedural flow required for a VoLTE call

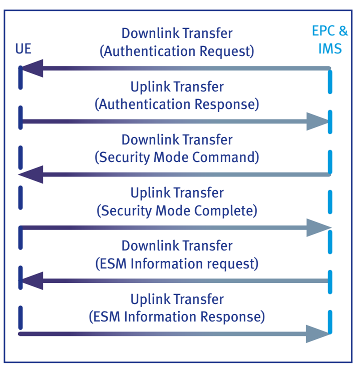
3.1. PDN Connectivity (NAS Signaling)



As in legacy 3GPP technologies, the UE starts connection by issuing a Radio Resource Control (RRC) Connection Request. Note that while either the UE or the network can trigger the connection request, it is always initiated by the UE. This request includes both the UE identity information and the call establishment cause (i.e. Mobile Originating Signaling or Emergency). Assuming there are no issues, the network responds with an RRC Connection Setup message.

The procedure thus far has established a signaling bearer and a Dedicated Control Channel (DCCH). Once in RRC Connected mode, the UE responds by sending an RRC Connection Setup Complete message which includes the Attach request for PDN connectivity. While this part of the connection is familiar to those versed in 3G technologies, it is worth noting that at this point, unlike in a legacy UMTS system, the initial NAS message has already been delivered to the Mobility Management Entity (MME). In the case of a VoLTE call this message would be an Attach Request.

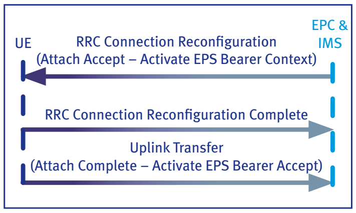
3.2. Authentication



Now that NAS signaling is established, the network initiates an Authentication Request or challenge. Once the UE's Authentication Response is deemed valid, the network sends a NAS Security Mode Command. Note that while neither the Authentication Request nor the Authentication Response is integrity-protected, the Security Mode Command is protected. The UE then sends a Security Mode Complete message, establishing protected NAS signaling.

In order to protect EPS Session Management (ESM) information, the network now sends an ESM Information Request; the UE reacts with an ESM Information response describing the now-protected protocol configuration options.

3.3. Bearer Setup and EPS Attach



At this point, additional radio bearers must be set up. The network sends an RRC Connection Reconfiguration to activate the EPS bearer. The UE confirms successful completion with an RRC Connection Reconfiguration Complete message and then finalizes the Attach procedure and accepts the activation of the EPS bearer.

It should be noted that the way a default PDN is associated to an IMS device varies per the network operator. In some networks, powering on a device will cause it to attempt to establish a connection with an Internet PDN. In this case the device will only establish IMS connectivity when an IMS application needs to be serviced. A device used on another network will, on powering up, attempt to establish a connection with an IMS PDN, and display a "No Service" message if the connection is not made.

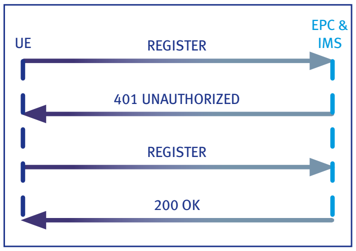
3.4. P-CSCF Discovery

Before sending any Session Initiation Protocol (SIP) requests, the UE must perform "P-CSCF Discovery", the process of identifying (by address) the correct Proxy-Call Session Control Function (P-CSCF). The P-CSCF address may be discovered in one of three different ways:

1. It may be stored in the IP Multimedia Services Identity Module (ISIM).
2. The UE may request it as part of the PDN connectivity request during the Attach process.
3. The UE may request an IP address and Fully Qualified Domain Name (FQDN) from a DHCP server and then perform a DNS query on the returned IP address and FQDN.

The next part of the procedural flow includes IMS Registration, Event Subscription and Call Connection and utilizes key IMS protocols. For a detailed explanation of these protocols, please refer to the "IMS Protocols" and "Sample Call Flows" sections in this document.

3.5. SIP Registration



After Authentication, Security and UE Capability requests, the network accepts the Attach request and activates the EPS bearer context. Once that has happened and the UE has also established a PDP context, a typical IMS SIP client registration (Figure 4) begins:

1. The IMS client attempts to register by sending a REGISTER request to the P-CSCF.
2. The P-CSCF forwards the REGISTER request to the I-CSCF.
3. The I-CSCF polls the HSS for data used to decide which S-CSCF should manage the REGISTER request. The I-CSCF then makes that decision.
4. The I-CSCF forwards the REGISTER request to the appropriate S-CSCF.
5. The S-CSCF typically sends the P-CSCF a 401 (UNAUTHORIZED) response as well as a challenge string in the form of a "number used once" or "nonce".
6. The P-CSCF forwards the 401 – UNAUTHORIZED response to the UE.
7. Both the UE and the network have stored some Shared Secret Data (SSD), the UE in its ISIM or USIM and the network on the HSS. The UE uses an algorithm per RFC 3310[1] (e.g. AKAv2-MD5) to hash the SSD and the nonce."
8. The UE sends a REGISTER request to the P-CSCF. This time the request includes the result of the hashed nonce and SSD.
9. The P-CSCF forwards the new REGISTER request to the I-CSCF.
10. The I-CSCF forwards the new REGISTER request to the S-CSCF.
11. The S-CSCF polls the HSS (via the I-CSCF) for the SSD, hashes it against the nonce and determines whether the UE should be allowed to register. Assuming the hashed values match, the S-CSCF sends 200 – OK response to the P-CSCF. At this point an IPSec security association is established by the P-CSCF.
12. The P-CSCF forwards the 200 – OK response to the UE.

1 Internet Engineering Task Force (IETF) RFC 3310: "Hypertext Transfer Protocol (HTTP) Digest Authentication. Using Authentication and Key Agreement (AKA)"

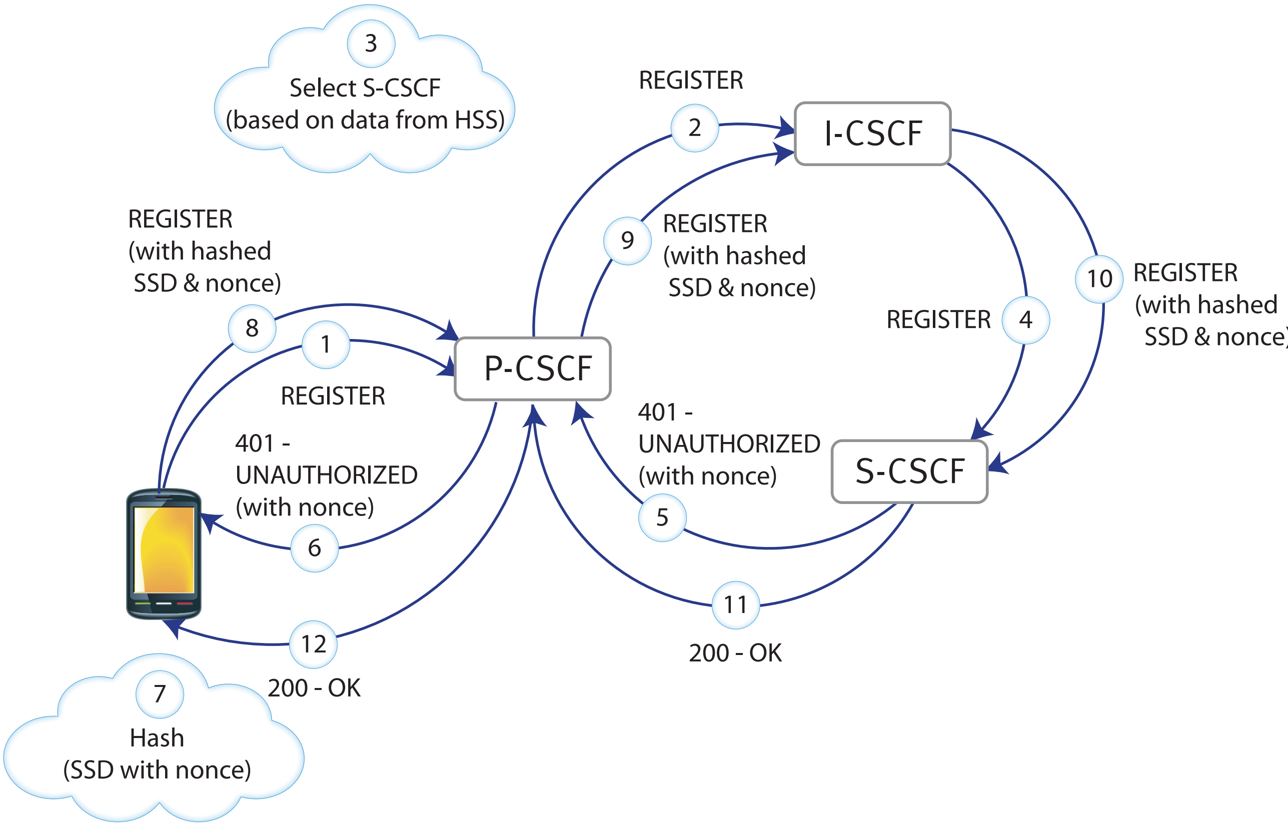
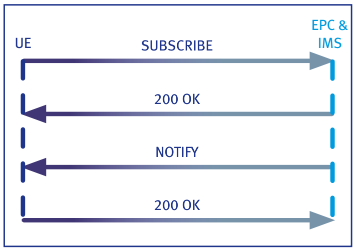


Figure 2 - SIP Client Registration

Each element described therefore has a unique set of roles in this arrangement:

- The UE initiates the registration sequence, attaches to the LTE network and activates the PDP context. It discovers which P-CSCF to use, then makes a deliberately unauthenticated registration attempt. It waits for the expected 401 response, extracts the nonce from the response and hashes it with the SSD before including the result in a second REGISTER request.
- The P-CSCF, typically resident in the visited network, acts as the UE's gateway into the UE's home network. It identifies the home IMS network, routes traffic to and from the home IMS network and establishes the IPSec security association.
- The I-CSCF, typically resident in the home network, acts as the front-end of the home IMS. It interfaces with the P-CSCF in the visited network and selects the S-CSCF (by querying the HSS).
- The S-CSCF, typically resident in the home network, handles the registration request from the I-CSCF, pulls authentication vectors from the HSS and passes them to the P-CSCF (via the I-CSCF), and authenticates the user in the second registration attempt.

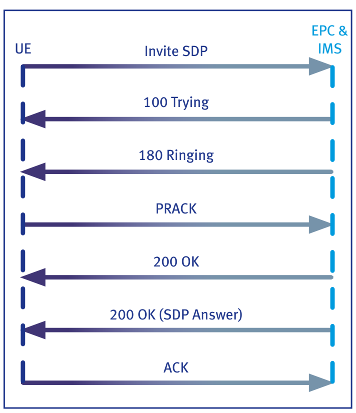
3.6. Event Subscription



Suppose the UE now intends to monitor a specific “registration event”. In this context an event may be a callback (to provide audio for a shared web event, for example) or an update to a “buddy list” or a message waiting indicator. In general, this means that the UE is asking to be notified any time there is a change in registration status and it requires cooperation between two end nodes. It is an essential part of IMS since it enables the concept of subscriber “presence”.

The UE will begin the transaction using the SUBSCRIBE method. This method, defined in RFC 3265, is one of the many SIP extensions used in IMS. This is basically a request to be notified (for a specified period of time) of a change in resource state. As is shown in the call flow section later in this document, the eventual response is a NOTIFY method indicating that there has been a change in status.

3.7. VoLTE Call



The initial stages of setting up a VoLTE call are the processes of the initial attach, P-CSCF discovery and creating the default bearer for SIP signaling (by registering with the IMS network and subscribing to a registration event package).

The first step in a VoLTE call setup is a SIP INVITE request initiated by the calling UE. Following this step, agreement is made on the media-specific parameters such as codecs (e.g. AMR or WB-AMR). After some RINGING, TRYING and OK messaging, the calling UE may respond with a Provisional ACK (PRACK) method as shown in the flow diagram above and as defined in RFC 3551. The PRACK method is used because ACK cannot safely traverse proxy servers that comply with RFC 3261. The PRACK is also forwarded to the called UE. When the called subscriber answers the call, the called UE will respond with a 200 OK before the RTP (media) messaging begins.

In a VoLTE call, the bearer is associated with a QoS Class Identifier (QCI) of 1. QCI values from the 3GPP's TS 23.203[2] are shown in Table 1. Each is generally targeted to a specific service type based on delay and packet loss requirements. For example, a video telephony call might add a second dedicated bearer for video traffic, assigning a QCI of 6 to that bearer.

QCI	Resource Type	Priority	Packet Delay Budget (ms)	Packet Error Loss Rate	Example Services
1	GBR	2	100	10^{-2}	Conversational Voice
2	GBR	4	150	10^{-3}	Conversational Video (live streaming)
3	GBR	5	300	10^{-6}	Non-conversational video (buffered streaming)
4	GBR	3	50	10^{-3}	Real-time gaming
5	Non-GBR	1	100	10^{-6}	IMS Signaling
6	Non-GBR	7	100	10^{-3}	Voice, Video (live streaming), interactive gaming
7	Non-GBR	6	300	10^{-6}	Video (buffered streaming)
8	Non-GBR	8	300	10^{-6}	TCP-based (WWW, email, FTP); privileged subscriber
9	Non-GBR	9	300	10^{-6}	TCP-based (WWW, email, FTP); non-privileged subscriber

Table 1 - QCI Values for Bearers

4. IMS PROTOCOLS

From the UE's point of view of the IMS subsystem, the critical protocols are the Session Initiation Protocol (SIP), SigComp, Real-time Transport Protocol (RTP), RTP Control Protocol (RTCP) and IP Security (IPSec). While there are other key IMS protocols (e.g. Diameter) often mentioned in the same breath as those listed here, these are the ones impacted by the UE or having direct impact on UE operation.

4.1. SIP

SIP is a protocol used to create, modify and terminate multimedia sessions, essentially negotiating a media session between two users. As a text-based client/server protocol, SIP is completely independent of underlying protocols, (e.g. TCP/IP vs. UDP or IPv4 vs. IPv6). SIP is not a transport protocol and does not actually deliver media, leaving that task to RTP/RTCP.

While SIP itself is defined in the IETF's RFC 3261[3], SIP as used for IMS includes multiple extensions. This is not without precedent in telephony; one popular implementation of Push-to-talk over Cellular (PoC) used a heavily-extended version of SIP as well. As a matter of fact, some better-known cellular SIP methods (e.g. MESSAGE, SUBSCRIBE) are actually defined in extensions beyond RFC 3261, and their usage in cellular IMS is defined in the 3GPP's TS 23.228[4].

One popular misconception is that SIP is specific to IMS. In fact, it is used in media services deployed via Internet PDN as well. Skype™ and FaceTime® are two well-known examples of non-IMS-based SIP-based applications.

2 3GPP TS 23.203: "Policy and charging control architecture"
3 Internet Engineering Task Force (IETF) RFC 3261: "SIP: Session Initiation Protocol"
4 3GPP TS 23.228: "IP Multimedia Subsystem (IMS); Stage 2"

4.2. SIP requests

SIP is a sequential (request/response) protocol similar to HTTP both in functionality and format. Every SIP request begins with a starting line that includes the name of the method (request type). Table 2 outlines request methods used in SIP.

SIP Request Method	Description	Definition
INVITE	Indicates that a client is being invited to participate in a call session	RFC 3261
ACK	Confirms that the client has received a final response to an INVITE request	RFC 3261
BYE	Terminates a call; can be sent by either the caller or the called party	RFC 3261
CANCEL	Cancels any pending request	RFC 3261
OPTIONS	Queries the capabilities of servers	RFC 3261
REGISTER	Registers the address listed in the To header field with a SIP server	RFC 3261
PRACK	Provisional acknowledgement	RFC 3262[5]
SUBSCRIBE	Subscribes to event notification	RFC 3265[6]
NOTIFY	Notifies the subscriber of a new Event	RFC 3265
PUBLISH	Publishes an event to the Server	RFC 3903[7]
INFO	Sends mid-session information that does not modify the session state	RFC 6086[8]
REFER	Asks recipient to issue a SIP request (call transfer)	RFC 3515[9]
MESSAGE	Transports instant messages using SIP	RFC 3428[10]
UPDATE	Modifies the state of a session without changing the state of the dialog	RFC 3311[11]

Table 2 - SIP Request Methods

The first line of a SIP request is followed by header information, and finally the message body. RFC 3261 not only defines SIP but includes a very reader-friendly description of the fields found in the request header. Please refer to the Appendix for a complete list of SIP Headers. The content of the message body is defined by the Session Description Protocol defined in RFC 2327[12] and described in the next section.

5 Internet Engineering Task Force (IETF) RFC 3262: “Reliability of Provisional Responses in the Session Initiation Protocol (SIP)”
6 Internet Engineering Task Force (IETF) RFC 3265: “Session Initiation Protocol (SIP)-Specific Event Notification”
7 Internet Engineering Task Force (IETF) RFC 3903: “Session Initiation Protocol (SIP) Extension for Event State Publication”
8 Internet Engineering Task Force (IETF) RFC 6086: “Session Initiation Protocol (SIP) INFO Method and Package Framework”
9 Internet Engineering Task Force (IETF) RFC 3515: “The Session Initiation Protocol (SIP) Refer Method”
10 Internet Engineering Task Force (IETF) RFC 3428: “Session Initiation Protocol (SIP) Extension for Instant Messaging”
11 Internet Engineering Task Force (IETF) RFC 3311: “The Session Initiation Protocol (SIP) UPDATE Method”
12 Internet Engineering Task Force (IETF) RFC 2327: “SDP: Session Description Protocol”

```
Request start line INVITE sip:13@10.10.1.13 SIP/2.0
Request header     Via: SIP/2.0/UJP 10.10.1.99:5060;branch=z9hG4bK343b:628;rport
                   From: "Test 15" <sip:15@10.10.1.99>tag=as58f4201b
                   To: <sip:13@10.10.1.13>
                   Contact : <sip:15@10.10.1.99>
                   Call-ID: 326371826c80e17e6c:6c29861eb2933@10.10.1.99
                   CSeq: 102 INVITE
                   User-Agent : Asterisk PBX
                   Max-Forwards : 70
                   Date: Wed, 06 Dec 2009 14 :12 :45 GY.T
                   Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE,
                   NOTIFY
                   Supported: replaces
                   Content-Type : application/adp
                   Content-Length: 258
<blank line>
Message body       v=0
(SDP message)      o=Joe Spirent 1821 1821 IN IP4 10.10.1.99
                   s=Spirent Seminar : IMS & VoLTE
                   c=IN IP4 10.10.1.99
                   t=0 0
                   m=audio 11424 RTP/AVP 0 8 101
                   a=rtpmap:0 PCMU/8000
                   a=rtpmap:8 PCMA/8000
                   a=rtpmap:101 telephone-event/8000
                   a=fmtp:101 0-16
                   a=silenceSupp:off - - - -
                   a=ptime:20
                   a=sendrecv
```

Table 3 - Sample SIP request

4.3. Session Description Protocol (SDP)

The definition of SDP in RFC 2327 was cast in the late 1990's and was originally intended for use in describing multimedia (e.g. audio, video) sessions on an Internet backbone. At a minimum, a multimedia session requires the following information to be shared between the sender and the receiver: the name of the session, the time(s) at which the session is active, information regarding the media and information required to receive the media (i.e., addresses, ports, formats, etc.) SDP information may also include contact information and information about bandwidth requirements for the session.

While RFC 2327 defines the fields used in SDP, the protocol mechanism or negotiation is defined in RFC 3264[13]. This basic mechanism itself is familiar to the cellular world, with one participant suggesting a common basis for communication and another responding with a suggestion suited to its own capabilities. At a minimum this "offer/answer" mechanism is used to negotiate media formats and transport addresses. It may also be used to exchange cryptographic keys and algorithms.

In Table 2, the SDP message body describes the owner ("Joe Spirent"), the session ("Spirent Seminar: IMS & VoLTE"), some connection information (IP4 10.10.1.99), the media (audio) and some suggested attributes of the media (PCMU, PCMA, etc.).

13 Internet Engineering Task Force (IETF) RFC 3264: "An Offer/Answer Model with the Session Description Protocol (SDP)"

4.4. SIP Responses

SIP Responses are maintained in an IANA list called *Session Initiation Protocol (SIP) Parameters*[14]. They always begin with a Response Code, which falls into one of the following categories:

Informational/Provisional (1xx): Request received and being processed – Examples: 100 Trying, 180 Ringing

Successful (2xx): The action was successfully received, understood, and accepted – Examples: 200 OK, 202 Accepted

Redirection (3xx): Further action needs to be taken (typically by the sender) to complete the request – Examples: 301 Moved Permanently, 302 Moved Temporarily

Client Failure (4xx): The request contains bad syntax or cannot be fulfilled at the server – Examples: 401 Unauthorized, 403 Forbidden

Server Failure (5xx): The server failed to fulfill an apparently valid request – Examples: 500 Server Internal Error, 504 Server Time-out

Global Failure (6xx): The request cannot be fulfilled at any server – Examples: 600 Busy Everywhere, 604 Does Not Exist Anywhere

Please refer to the Appendix for a complete list of SIP Codes.

4.5. SigComp (Signaling Compression)

SIP is, like HTTP, a text-based protocol. While this can make for easy debugging it is inefficient when used in its native text form. The compression mechanism used is SigComp, defined in RFC 3320[15]. SigComp is not specific to IMS and, contrary to popular belief, does not define a specific algorithm. Rather it defines an architecture in which to deploy a compression/decompression algorithm, including the definition for a Universal Decompressor Virtual Machine (UDVM). While this architecture enables virtually any available lossless compression algorithm, IMS centers on using either the DEFLATE algorithm or the well-known Lempel-Ziv-Storer-Szymanski (LZSS) algorithm. While both DEFLATE and LZSS started their lives as commercial products, the patents on DEFLATE have expired and the algorithm has since been codified in an IETF document (RFC 1951[16]).

Two noteworthy points: first, SigComp is only implemented between a UE and the network's P-CSCF. Secondly, SMS-only IMS devices do not use SigComp.

14 http://www.iana.org/assignments/sip-parameters
15 Internet Engineering Task Force (IETF) RFC 3320: "Signaling Compression (SigComp)"
16 Internet Engineering Task Force (IETF) RFC 1951: "DEFLATE Compressed Data Format Specification"

4.6. The Real-time Transport Protocol (RTP) and RTP Control Protocol (RTCP)

It was noted earlier that while SIP is the most commonly mentioned protocol when discussing IMS, SIP is not a media transport protocol. IMS uses RTP as the media data transfer protocol. Both RTP and RTCP are defined in RFC 3550[17].

Despite the protocol's name, neither RTP nor RTCP make any attempt to guarantee timeliness of data delivery. On the contrary, the phrase "real-time" is used because a pre-requisite for RTP is an architectural framework whose lower layers can deliver real-time data.

In an IMS scenario, RTCP is used to provide statistical Quality-of-Service (QoS) information and aid in synchronizing streams. While the protocol can be used to provide other rudimentary connection information, an IMS subsystem uses SDP for this purpose.

RTP and RTCP are always paired in port assignments. An even-numbered port will become an RTP port, and the next highest-number port will be the associated RTCP port.

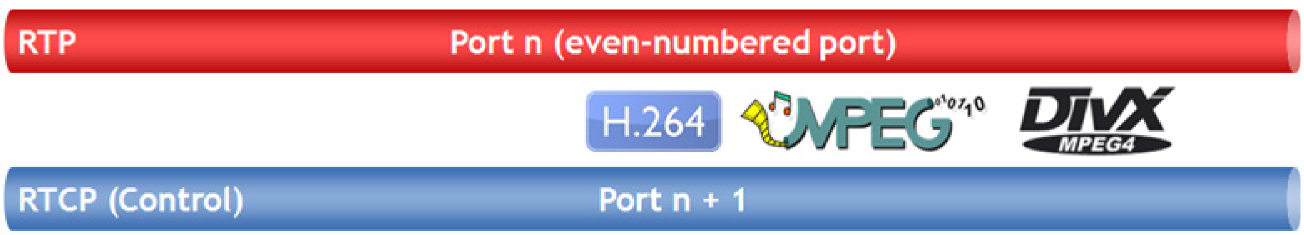


Figure 3 - IMS media is transported by RTP/RTCP

5. IMS CLIENT-RELATED SECURITY

IMS clients are challenged at various points by the network: on initial registration, on de-registration, and on certain session requests (e.g. SIP INVITE). The mechanism used is Authentication and Key Agreement (IMS AKA) with IPsec.

In terms of *access security* (managed in part by the UE or UE-hosted elements), of the five documented security associations in the 3GPP's TS 33.203[18] document, two are related to direct connections between the UE and the IMS subsystem. Note that the topic of network security (security between nodes in the network) is beyond the scope of this document. While there are other security associations related to the UE, these are meant to protect nodes within the subsystem.

From a more macroscopic point of view, the security associations discussed here are independent of those required by legacy networks and non-IMS packet data systems.

17 Internet Engineering Task Force (IETF) RFC 3550: "RTP: A Transport Protocol for Real-Time Applications"
18 3GPP TS 33.203: "Technical Specification Group Services and System Aspects; 3G security; Access security for IP-based services"

5.1. Security association between the User Agent and a P-CSCF

This security association occurs on the Gm reference point defined in TS 23.002[19]. The mechanism call flow is outlined in Figure 3 and described in detail in the document section titled Sample SIP Call Flows starting on page 15. This initial call flow uses an unprotected port on the network side.

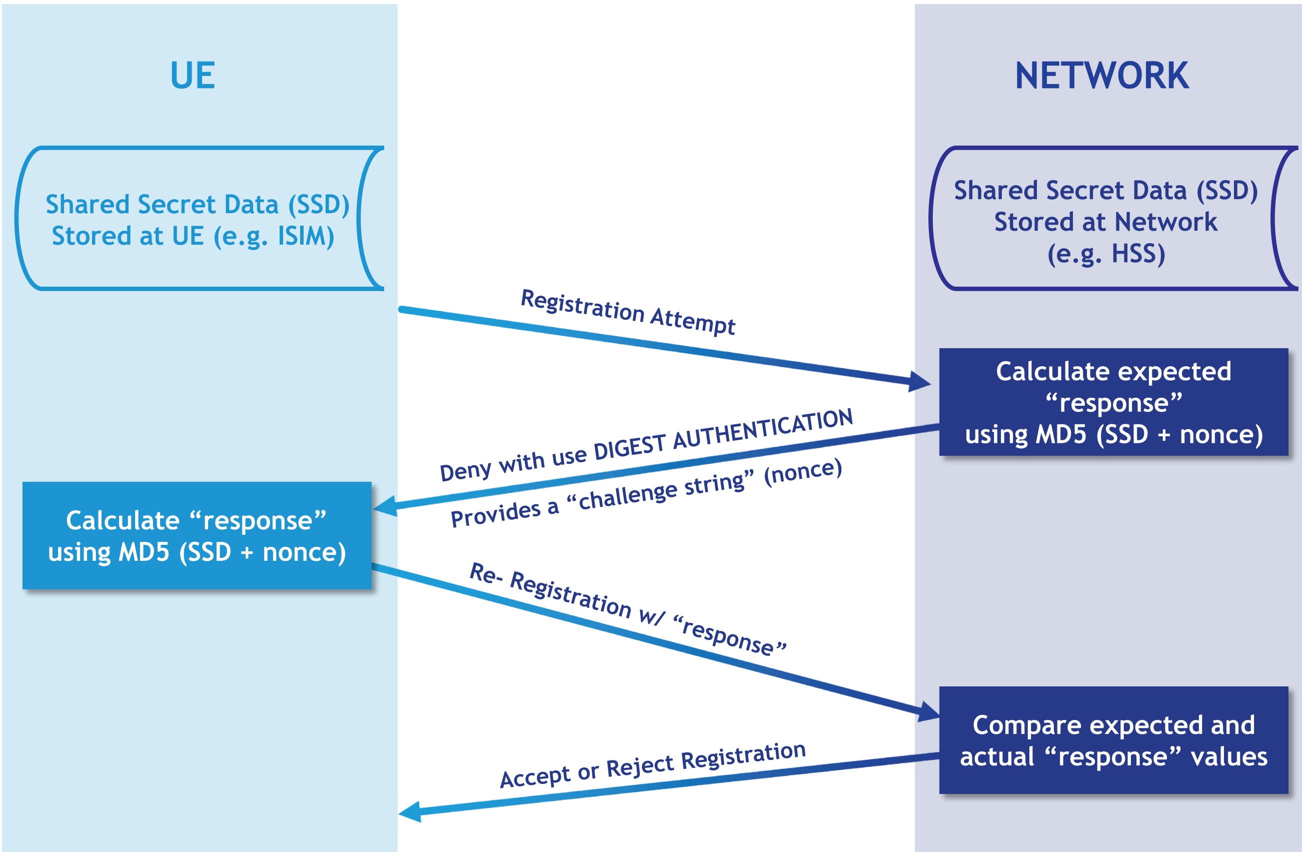


Figure 4 - IMS Authentication

In transport mode, data traffic between the UE and the P-CSCF is protected by IPsec Encapsulating Security Payloads (ESP).

5.2. Security association between the ISIM and the HSS

The second security association discussed here is between the ISIM and the HSS. This association uses IMS Authentication and Key Agreement (IMS-AKA) to provide mutual authentication between the ISIM and the home network. Note that the User Agent ⇔ P-CSCF association does not use IMS-AKA since no key is shared; that mechanism assumes that shared secret data is stored on both the network and the UE.

19 3GPP TS 23.002: "Technical Specification Group Services and System Aspects; Network Architecture"

6. SAMPLE SIP CALL FLOWS

The following section illustrates the above with some examples as seen from the UE's perspective.

6.1. Registration

First, the User Agent (UA) on the UE attempts to register with the IMS subsystem using an unauthenticated registration attempt. Here, sip:spirentims.com is the Request-URI. Note that the client uses valid abbreviations for the 'from' ('f') and to ('t') parameters. Note also that the addresses in these two fields are identical. This is, in fact, usually the case. Finally, take note that SIP header abbreviations are not always as intuitive as they are for 'from' and 'to'. For example, 'k' abbreviates 'Supported' and the abbreviation for 'Identity' is 'y'. In multiple designs this relatively simple detail has raised issues that were not discovered until interoperability testing.

```
REGISTER sip:spirentims.com

f: <sip:+17325449180@spirentims.com>;tag=4182491880
t: <sip:+17325449180@spirentims.com>
CSeq: 961266357 REGISTER
i: 4182491830_60060904@2600:1000:800a:92e0:0:2:c33c:b501
v: SIP/2.0/UDP [2600:1000:800a:92e0:0:2:c33c:b501]:5060;branch=z9hG4bK501773842
Max-Forwards: 70
m: <sip:+17325449180@[2600:1000:800a:92e0:0:2:c33c:b501]:5060>
P-Access-Network-Info: 3GPP-E-UTRAN-FDD; utran-cell-id-3gpp=025B2816401
l: 0
Authorization: Digest uri="sip:spirentims.com",username="311480000224201@spirentims.com",response="",realm=\
"spirentims.com",nonce=""
Expires: 3600
```

The 'from' and 'to' fields show examples of SIP URIs, including 10-digit MINs built from the UE's public identities.

The network's response (below) is the expected 401 response. It contains the nonce (="C/0d2Rb…") that will be hashed with the SSD by the UE. The response also specifies the algorithm to be used, in this case AKAv2 (defined in RFC 4169[20]) with MD5 hashing. Note also that the network is not using abbreviations for 'from' and 'to'.

```
401 Unauthorized

From: <sip:+17325449180@spirentims.com>;tag=4182491880
To: <sip:+17325449180@spirentims.com>;tag=1773611254
CSeq: 961266357 REGISTER
Call-ID: 4182491830_60060904@2600:1000:800a:92e0:0:2:c33c:b501
Via: SIP/2.0/UDP [2600:1000:800a:92e0:0:2:c33c:b501]:5060;branch=z9hG4bK501773842
WWW-Authenticate: Digest realm="spirentims.com",nonce="C/0d2RbSENwLBtfXG2d+EoZTHcoQtAAAM1EyTNicLIMyM
DJiMTExAA==",\
algorithm=AKAv2-MD5,qop="auth"
Content-Length: 0
```

20 Internet Engineering Task Force (IETF) RFC 4169: "Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA) Version-2"

The client replies with a response that includes the hashed value ("response") and includes an echo of the nonce.

```
REGISTER sip:spirentims.com SIP/2.0

f: <sip:+17325449180@spirentims.com>;tag=4182491880
t: <sip:+17325449180@spirentims.com>
CSeq: 961266358 REGISTER
i: 4182491830_60060904@2600:1000:800a:92e0:0:2:c33c:b501
v: SIP/2.0/UDP [2600:1000:800a:92e0:0:2:c33c:b501]:5060;branch=z9hG4bK133348912
Max-Forwards: 70
m: <sip:+17325449180@[2600:1000:800a:92e0:0:2:c33c:b501]:5060>
P-Access-Network-Info: 3GPP-E-UTRAN-FDD; utran-cell-id-3gpp=025B2816401
l: 0
Authorization: Digest username="311480000224201@spirentims.com",\ realm="spirentims.com",uri="sip:spirentims.
com",qop=auth,\
nonce="C/0d2RbSENwLBtfXG2d+EoZTHcoQtAAAM1EyTNicLIMyMDJiMTExAA==",nc=00000001,cnonce="11259375",\
algorithm=AKAv2-MD5,response="ae1cbf6463baa6dfb7dc59a7fdea8ad"
Expires: 3600
```

The network, having checked the hashed response against the result of its own hashing, sends a 200 response:

```
200 OK

From: <sip:+17325449180@spirentims.com>;tag=4182491880
To: <sip:+17325449180@spirentims.com>;tag=1246742606
CSeq: 961266358 REGISTER
Call-ID: 4182491830_60060904@2600:1000:800a:92e0:0:2:c33c:b501
Via: SIP/2.0/UDP [2600:1000:800a:92e0:0:2:c33c:b501]:5060;branch=z9hG4bK133348912
Contact: <sip:+17325449180@[2600:1000:800a:92e0:0:2:c33c:b501]:5060>;expires=3600
P-com.siemens.maximum-chat-size: 1300
P-com.siemens.maximum-IM-size: 1300
P-com.siemens.chat: direct
P-Associated-URI: <sip:+17325449180@spirentims.com>
P-Associated-URI: <tel:+17325449180>
Content-Length: 0
```

Initial IMS registration is now complete.

6.2. Event Subscription

Here, the type of event is a “reg” event. The abbreviation ‘o’ as a header field means ‘Event’… yet another example of a non-intuitive header field abbreviation. Note the “Expires” field setting up the subscription for 600,000 seconds.

```
SUBSCRIBE sip:+17325449180@spirentims.com SIP/2.0

f: <sip:+17325449180@spirentims.com>;tag=4182493644
t: <sip:+17325449180@spirentims.com>
CSeq: 961268047 SUBSCRIBE
i: 4182493519_60077872@2600:1000:800a:92e0:0:2:c33c:b501
v: SIP/2.0/UDP [2600:1000:800a:92e0:0:2:c33c:b501]:5060;branch=z9hG4bK299099096
Max-Forwards: 70
m: <sip:+17325449180@[2600:1000:800a:92e0:0:2:c33c:b501]:5060>
P-Access-Network-Info: 3GPP-E-UTRAN-FDD; utran-cell-id-3gpp=025B2816401
o: reg
l: 0
Route: <sip:[2001:4888:2:fff0:a0:104:0:37]:5060;lr>
P-Preferred-Identity: <sip:+17325449180@spirentims.com>
Expires: 600000
```

The network replies with a 200 (OK) response:

```
200 OK

From: <sip:+17325449180@spirentims.com>;tag=4182493644
To: <sip:+17325449180@spirentims.com>;tag=647050200
CSeq: 961268047 SUBSCRIBE
Call-ID: 4182493519_60077872@2600:1000:800a:92e0:0:2:c33c:b501
Via: SIP/2.0/UDP [2600:1000:800a:92e0:0:2:c33c:b501]:5060;branch=z9hG4bK299099096
Expires: 86400
Contact: <sip:njbbims1scscf040.spirentims.com:5090;lskpmc=S20>
Record-Route: <sip:[2001:4888:2:fff0:a0:104:0:37];routing_id=pcscf_a_side;lskpmc=P12;lr;serv_user=[2600:1000:800a:92e0:
0:2:c33c:b501]:5060>
Content-Length: 0
```

The network now wants to notify the UA of a change in registration status, using the NOTIFY method.

```
NOTIFY sip:+17325449180@[2600:1000:800a:92e0:0:2:c33c:b501]:5060 SIP/2.0

Via: SIP/2.0/UDP [2001:4888:2:fff0:a0:104:0:37]:5060;branch=z9hG4bK57c9c140bcda4a610df85cd53f7a754b;lskpmc=P12
Record-Route: <sip:[2001:4888:2:fff0:a0:104:0:37];routing_id=pcscf_a_side;lskpmc=P12;lr>
From: <sip:+17325449180@spirentims.com>;tag=647050200
To: <sip:+17325449180@spirentims.com>;tag=4182493644
Event: reg
Call-ID: 4182493519_60077872@2600:1000:800a:92e0:0:2:c33c:b501
Subscription-State: active
CSeq: 1 NOTIFY
Content-Type: application/reginfo+xml
Contact: <sip:njbbims1scscf040.spirentims.com:5090;lskpmc=S20>
Max-Forwards: 68
Content-Length: 613
    Message Body
eXtensible Markup Language
```

Extracting the XML message body reveals two separate addresses of record in the lines beginning with "aor=". The first is the sip-uri (defined in RFC 3261) originally used in the registration. The second is a tel-uri (defined in RFC 3966[21]). In this case the information provided seems redundant, but there is a reason for this distinction. If a PSTN user needs to call the UE, the device connected to the PSTN probably has no concept of SIP or its usage. It will, however, be able to call using the standard 10-digit E.164 telephone number provided in the tel-uri. This allows a circuit-switched device to communicate with the UE.

The CSCF initiated this action (creating the telephone number) and then notified the UA because the UA had SUBSCRIBEd to being notified of changes in registration status.


```
<?xml
    version="1.0"
    ?>
<reginfo
    xmlns="urn:ietf:params:xml:ns:reginfo"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    version="0"
    state="full">
    <registration
        aor="sip:+17325449180@spirentims.com"
        id="ecc0150020253091"
        state="active">
        <contact
            id="20253091"
            state="active"
            event="registered">
            <uri>
                sip:+17325449180@[2600:1000:800a:92e0:0:2:c33c:b501]:5060
                </uri>
            </contact>
        </registration>
    <registration
        aor="tel:+17325449180"
        id="575a5d0a20253091"
        state="active">
        <contact
            id="20253091"
            state="active"
            event="created">
            <uri>
                sip:+17325449180@[2600:1000:800a:92e0:0:2:c33c:b501]:5060
                </uri>
            </contact>
        </registration>
    </reginfo>
```


21 Internet Engineering Task Force (IETF) RFC 3966: "The tel URI for Telephone Numbers"

Finally, the UA sends its own 200 (OK) response and the exchange is complete:

```
200 OK

Via: SIP/2.0/UDP [2001:4888:2:fff0:a0:104:0:37]:5060;branch=z9hG4bK57c9c140bcda4a610df85cd53
f7a754b;lskpmc=P12
Record-Route: <sip:[2001:4888:2:fff0:a0:104:0:37];routing_id=pcscf_a_side;lskpmc=P12;lr>
From: <sip:+17325449180@spirentims.com>;tag=647050200
To: <sip:+17325449180@spirentims.com>;tag=4182493644
Call-ID: 4182493519_60077872@2600:1000:800a:92e0:0:2:c33c:b501
CSeq: 1 NOTIFY
l: 0
P-Access-Network-Info: 3GPP-E-UTRAN-FDD; utran-cell-id-3gpp=025B2816401
```

6.3. VoLTE Call

In this example, one user will invite another UE to a VoLTE call with a SIP INVITE request containing the SDP offer (starting after the blank line) in its body:

```
INVITE sip:+1102@fd00:0:20:1:0:0:1:2 SIP/2.0
Via: SIP/2.0/UDP [fd00:0:0:1::1]:5060;branch=z9hG4bK3400253307smg;transport=UDP
Supported: 100rel,timer
Allow: INVITE, ACK, CANCEL, UPDATE, BYE
P-Access-Network-Info: 3GPP-E-UTRAN-FDD;utran-cell-id-3gpp=0000000000000002
P-com.HDVVServiceType: VZW2012
User-Agent: SP VOIP IMS 2.0
Session-Expires: 1800;refresher=uac
Content-Type: application/sdp
Route: <sip:[fd00:0:20:1:0:0:1:2]:5060;lr>
Accept-Contact: *;+g.3gpp.icsi-ref="urn%3Aurn-7%3A3gpp-service.ims.icsi.mmtel"
From: <sip:+1732549822@spirentims.com>;tag=3257031038
To: <sip:+1102@fd00:0:20:1:0:0:1:2>
Call-ID: 2369393125@fd00:0:0:1::1
CSeq: 1 INVITE
Max-Forwards: 70
Contact: <sip:[fd00:0:0:1::1]:5060;transport=UDP>;+g.3gpp.icsi-ref="urn%3Aurn-7%3A3gpp-service.ims.
icsi.mmtel"
Content-Length: 396

v=0
o=IMS-UE-FOR-SPIRENT 1234562 0 IN IP6 fd00:0:0:1::1
s=-
i=A VOIP Session
c=IN IP6 fd00:0:0:1::1
t=0 0
m=audio 10040 RTP/AVP 107 97 110
b=AS:49
b=RS:800
b=RR:2400
a=ptime:20
a=maxptime:20
a=rtpmap:107 AMR-WB/16000
a=fmtp:107 octet-align=1; mode-set=2
a=rtpmap:97 AMR/8000
a=fmtp:97 octet-align=1; mode-set=7
a=rtpmap:110 telephone-event/8000
a=fmtp:110 0-15
a=mid:0
a=sendrecv
```

Here the UE offers a number of media and codec options to use during the call. Some of the details are described below.

Some static RTP payload type values are assigned standard values defined in RFC 3551[22], but most “interesting” codecs are newer than the standard and therefore rely on the use of dynamic RTP payload type assignments. Dynamically assigned payload type values can be instantly recognized… their values are greater than 96. This sometimes causes confusion. Some implementations will consistently use a specific payload type code for a specific codec, leading to the belief that all payload type values are standardized.

v=	Version	v=0 (at the time of the writing of this document, 0 is the only valid value
o=	Session owner & ID	o=‹username› ‹session id› ‹version› ‹network type› ‹address type› ‹address›
s=	Session name	s=‹session name›
i=	A VOIP Session	i=‹session description›
c=	Connection information	c=‹nettype› ‹addrtype›‹connection-address›
t=	Time the session is active	t=‹starttime› ‹stoptime› - non-zero for scheduled events
m=	media type, format and transport address	m=‹media› ‹port› ‹transport› ‹format list› ‹media› is “audio” or “video” (two m= lines for both). This is a prioritized list, where the first media type is the preferred type.
b=	AS:49	b=‹bandwidth type›‹bandwidth›
a=	session attributes	a=‹attribute› or a=‹attribute› ‹value›

Table 4 - Details on the SIP INVITE SDP

ptime	a=ptime:‹packet time› Length (in ms) carried in one RTP packet
rtpmap	a=rtpmap:‹payload type› ‹encoding name›/‹clock rate› [/‹encoding parameters›] Mapping from RTP payload codes (from the ‹format list› in the “m=“ field) to a codec name, clock rate and other encoding parameters
fmtp	a=fmtp:‹format› ‹format specific parameters›Defines parameters that are specific to a given format code
mid	a=mid:‹identification-tag› Normally used when media lines have to be typed together to indicate interaction between media types (e.g. audio and video). Defined in RFC 3388[23]
sendrecv	a=sendrecv (or “sendonly”, “recvonly”, “inactive”, “broadcast”)

Table 5 - Details on Session Attributes

22 Internet Engineering Task Force (IETF) RFC 3551: “RTP Profile for Audio and Video Conferences with Minimal Control”
23 Internet Engineering Task Force (IETF) RFC 3388: “Grouping of Media Lines in the Session Description Protocol (SDP)”

From the network's point of view, the next step is for the CSCF (which has received the INVITE request) to forward the request to the UE the caller is attempting to reach. That UE may first reply with a 100 TRYING response, then with a 180 RINGING response, both of which the CSCF forwards to the calling UE:

```
100 Trying

Via: Via: SIP/2.0/UDP [fd00:0:0:1::1]:5060;branch=z9hG4bK3400253307smg;transport=UDP
To: <sip:+1102@fd00:0:20:1:0:0:1:2>
From: <sip:+1732549822@spirentims.com>;tag=3257031038
Call-ID: 2369393125@fd00:0:0:1::1
CSeq: 1 INVITE
User-Agent: SP VOIP IMS 2.0
Content-Length: 0

180 Ringing

Via: SIP/2.0/UDP [fd00:0:0:1::1]:5060;branch=z9hG4bK3400253307smg;transport=UDP
Contact: <sip:[fd00:0:0:1::1]:5060;transport=UDP>
To: <sip:+1101@fd00:0:20:1:0:0:1:2>;tag=0161656c
From: <sip:+1732549822@spirentims.com>;tag=3257031038
Call-ID: 2369393125@fd00:0:0:1::1
CSeq: 1 INVITE
User-Agent: SP VOIP IMS 2.0
Content-Length: 0
```

Once the called subscriber answers the call, the called UE will respond with a 200 (OK):

```
200 OK

Via: SIP/2.0/UDP [fd00:0:0:1::1]:5060;branch=z9hG4bK3400253307smg;transport=UDP
Contact: <sip:[fd00:0:0:1::1]:5060;transport=UDP>
To: <sip:+1101@fd00:0:20:1:0:0:1:2>;tag=0161656c
From: <sip:+1732549822@spirentims.com>;tag=3257031038
Call-ID: 2369393125@fd00:0:0:1::1
CSeq: 1 INVITE
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REGISTER, SUBSCRIBE, NOTIFY, REFER, INFO, MESSAGE
Content-Type: application/sdp
Supported: replaces
User-Agent: SP VOIP IMS 2.0
Content-Length: 407

v=0
s=-
i=A VOIP Session
t=0 0
m=audio 4900 RTP/AVP 107 97 110
b=AS:49
b=RS:800
b=RR:2400
a=ptime:20
a=maxptime:20
a=rtpmap:107 AMR-WB/16000
a=fmtp:107 octet-align=1; mode-set=2
a=rtpmap:97 AMR/8000
a=fmtp:97 octet-align=1; mode-set=7
a=rtpmap:110 telephone-event/8000
a=fmtp:110 0-15
a=mid:0
a=sendrecv
```

From this point forward VoLTE traffic is transacted in the form of RTP messages and associated ACK/NACK signaling.

What has happened from the network's point of view is that one UE, which may have already been using the Internet PDN as a default bearer (per the operator's preference), issued an INVITE (via the default bearer) to IMS. The called UE was contacted, answered and issued an SDP answer. This caused the S-CSCF to request that the PCRF establish a dedicated IMS bearer to transport RTP traffic.

6.4. SMS

Suppose the UE initiates a text message. The UA initiates the transaction using the MESSAGE method, an extension defined in RFC 3428 . The 'to' field now includes the URI for the intended recipient UE. The message body is an IS-637-A message, the same payload data (not shown here) as might be found in a 1X text message. The payload could have just as easily been formatted as per a GSM text message.

```
MESSAGE tel:8177346764;phone-context=spirentims.com SIP/2.0

f: "UML290" <sip:+17325449180@spirentims.com>;tag=4182579147
t: <tel:8177346764;phone-context=spirentims.com>
CSeq: 961353644 MESSAGE
i: 4182579116_60098040@2600:1000:800a:92e0:0:2:c33c:b501
v: SIP/2.0/UDP [2600:1000:800a:92e0:0:2:c33c:b501]:5060;branch=z9hG4bK347680619
Max-Forwards: 70
P-Access-Network-Info: 3GPP-E-UTRAN-FDD; utran-cell-id-3gpp=025B2816401
Route: <sip:[2001:4888:2:fff0:a0:104:0:37]:5060;lr>
c: application/vnd.3gpp2.sms
Allow: MESSAGE
Request-Disposition: no-fork
User-Agent: QC User Agent
l: 62
ANSI IS-637-A (SMS) Transport Layer - Point-to-Point
ANSI IS-637-A (SMS) Teleservice Layer - CDMA Cellular Messaging Teleservice (4098)
```

Here, the message body is broken down to show the IS-637-A fields, including the encoded user data (in bold):

```
ANSI IS-637-A (SMS) Transport Layer - Point-to-Point
    Teleservice Identifier - CDMA Cellular Messaging Teleservice (4098)
        Transport Param ID: Teleservice Identifier (0)
        Length: 2
        CDMA Cellular Messaging Teleservice (4098)
    Destination Address
        Transport Param ID: Destination Address (4)
        Length: 7
        0... .... :  Digit mode: 4-bit DTMF
        .0.. .... :  Number mode: ANSI T1.607
        ..00 0010 :  Number of fields (MSB): (10)
        10.. .... :  Number of fields (LSB)
        Number: 8177346764
        ..00 0000 :  Reserved
    Bearer Data
        Transport Param ID: Bearer Data (8)
        Length: 46
        Bearer Data
ANSI IS-637-A (SMS) Teleservice Layer - CDMA Cellular Messaging Teleservice (4098)
    Message Identifier
        Teleservice Subparam ID: Message Identifier (0)
        Length: 3
        0010 .... .... .... .... .... = Message Type: Submit (mobile-originated only) (2)
        .... 0110 0110 0111 1000 .... = Message ID: 26232
        .... .... .... .... .... 0000 = Reserved: 0
    User Data
        Teleservice Subparam ID: User Data (1)
        Length: 36
        0001 0... :  Encoding: 7-bit ASCII
        .... .001 :  Number of fields (MSB): 39
        0011 1... :  Number of fields (LSB)
        .... .101 :  Most significant bits of first field
        Encoded user data: Spirent's IMS Solution (2nd to None!!!)
        .... ..00 :  Reserved
    Validity Period - Relative
        Teleservice Subparam ID: Validity Period - Relative (5)
        Length: 1
        Days
```

The CSCF now sends a 200 (OK) to indicate that it has received the SIP request. Note that this does not reflect any information about whether the message was delivered, read or received.

```
200 OK

Via: SIP/2.0/UDP [2600:1000:800a:92e0:0:2:c33c:b501]:5060;branch=z9hG4bK347680619
To: <tel:8177346764;phone-context=spirentims.com>;tag=notag
From: "UML290" <sip:+17325449180@spirentims.com>;tag=4182579147
Call-ID: 4182579116_60098040@2600:1000:800a:92e0:0:2:c33c:b501
CSeq: 961353644 MESSAGE
Allow: INVITE,ACK,CANCEL,BYE,INFO,UPDATE,MESSAGE,NOTIFY
Content-Length: 0
```

7. CONCLUSION

The IMS subsystem is a critical factor in the deployment of next-generation services. UE development today requires an understanding of the essential mechanisms used to interface with the subsystem. This paper presented the key protocols and procedures used by an LTE-capable UE when interfacing with an IMS-based LTE network. Much of the focus was on SIP and its use in registration, event subscription and VoLTE call connection. Some detailed protocol exchanges, captured from a live network, were used to illustrate the concepts.

The designer of a modern UE faces challenges on several fronts, not the least of which is an interface to an entirely new subsystem. As a global leader in LTE device testing, Spirent is well prepared to assist the UE developer address the many IMS/VoLTE test challenges and to support the industry in successful deployment of IMS/VoLTE.

Please see the Spirent website (www.spirent.com) for other free white papers, recorded seminars, posters and other resources that may be helpful to the UE developer.

8. APPENDIX

8.1. SIP Headers

Header field	Abbreviation	Reference
Accept		RFC3261
Accept-Contact	a	RFC3841
Accept-Encoding		RFC3261
Accept-Language		RFC3261
Accept-Resource-Priority		RFC4412
Alert-Info		RFC3261
Allow		RFC3261
Allow-Events	u	RFC3265
Answer-Mode		RFC5373
Authentication-Info		RFC3261
Authorization		RFC3261
Call-ID*	i	RFC3261
Call-Info		RFC3261
Contact	m	RFC3261
Content-Disposition		RFC3261
Content-Encoding	e	RFC3261
Content-Language		RFC3261
Content-Length	l	RFC3261
Content-Type	c	RFC3261
CSeq*		RFC3261
Date		RFC3261
Encryption**		RFC3261
Error-Info		RFC3261
Event	o	RFC3265
Expires		RFC3261
Flow-Timer		RFC5626
From*	f	RFC3261
Hide**		RFC3261
History-Info		RFC4244 RFC6044
Identity	y	RFC4474
Identity-Info	n	RFC4474
In-Reply-To		RFC3261
Join		RFC3911
Max-Breadth		RFC5393
Max-Forwards*		RFC3261
MIME-Version		RFC3261
Min-Expires		RFC3261
Min-SE		RFC4028
Organization		RFC3261
P-Access-Network-Info		RFC3455
P-Answer-State		RFC4964
P-Asserted-Identity		RFC3325
P-Asserted-Service		RFC6050
P-Associated-URI		RFC3455
P-Called-Party-ID		RFC3455
P-Charging-Function-Addresses		RFC3455

* Mandatory
** Deprecated

Header field	Abbreviation	Reference
P-Charging-Vector		RFC3455
P-DCS-Billing-Info		RFC5503
P-DCS-LAES		RFC5503
P-DCS-OSPS		RFC5503
P-DCS-Redirect		RFC5503
P-DCS-Trace-Party-ID		RFC3603
P-Early-Media		RFC5009
P-Media-Authorization		RFC3313
P-Preferred-Identity		RFC3325
P-Preferred-Service		RFC6050
P-Profile-Key		RFC5002
P-Refused-URI-List		RFC5318
P-Served-User		RFC5502
P-User-Database		RFC4457
P-Visited-Network-ID		RFC3455
Path		RFC3327
Permission-Missing		RFC5360
Policy-Contact		
Policy-ID		
Priority		RFC3261
Priv-Answer-Mode		RFC5373
Privacy		RFC3323
Proxy-Authenticate		RFC3261
Proxy-Authorization		RFC3261
Proxy-Require		RFC3261
RAck		RFC3262
Reason		RFC3326
Record-Route		RFC3261
Refer-Sub		RFC4488
Referred-By		RFC3892
Replaces		RFC3891
Resource-Priority		RFC4412
Response-Key**		RFC3261
Retry-After		RFC3261
Route		RFC3261
RSeq		RFC3262
Security-Client		RFC3329
Security-Server		RFC3329
Security-Verify		RFC3329
Server		RFC3261
Service-Route		RFC3608
Session-Expires	x	RFC4028
SIP-ETag		RFC3903
SIP-If-Match		RFC3903
Subject	s	RFC3261
Subscription-State		RFC3265
Supported	k	RFC3261
Suppress-If-Match		RFC5839

** Deprecated

Header field	Abbreviation	Reference
Target-Dialog		RFC4538
Timestamp		RFC3261
To*	t	RFC3261
Trigger-Consent		RFC5360
Unsupported		RFC3261
User-Agent		RFC3261
Via*	v	RFC3261
Warning		RFC3261
WWW-Authenticate		RFC3261

8.2. SIP Codes

Code	Description	Reference
100	Trying	
180	Ringing	
181	Call Is Being Forwarded	
182	Queued	
183	Session Progress	
199	Early Dialog Terminated	RFC6228
200	OK	
202	Accepted	RFC3265
204	No Notification	RFC5839
300	Multiple Choices	
301	Moved Permanently	
302	Moved Temporarily	
305	Use Proxy	
380	Alternative Service	
400	Bad Request	
401	Unauthorized	
402	Payment Required	
403	Forbidden	
404	Not Found	
405	Method Not Allowed	
406	Not Acceptable	
407	Proxy Authentication Required	
408	Request Timeout	
410	Gone	
412	Conditional Request Failed	RFC3903
413	Request Entity Too Large	
414	Request-URI Too Long	
415	Unsupported Media Type	
416	Unsupported URI Scheme	
417	Unknown Resource-Priority	RFC4412
420	Bad Extension	
421	Extension Required	
422	Session Interval Too Small	RFC4028
423	Interval Too Brief	
424	Bad Location Information	RFC6442
428	Use Identity Header	RFC4474

* Mandatory

Code	Description	Reference
422	Session Interval Too Small	RFC4028
423	Interval Too Brief	
424	Bad Location Information	RFC6442
428	Use Identity Header	RFC4474
429	Provide Referrer Identity	RFC3892
430	Flow Failed	RFC5626
433	Anonymity Disallowed	RFC5079
436	Bad Identity-Info	RFC4474
437	Unsupported Certificate	RFC4474
438	Invalid Identity Header	RFC4474
439	First Hop Lacks Outbound Support	RFC5626
440	Max-Breadth Exceeded	RFC5393
469	Bad Info Package	RFC6086
470	Consent Needed	RFC5360
480	Temporarily Unavailable	
481	Call/Transaction Does Not Exist	
482	Loop Detected	
483	Too Many Hops	
484	Address Incomplete	
485	Ambiguous	
486	Busy Here	
487	Request Terminated	
488	Not Acceptable Here	
489	Bad Event	RFC3265
491	Request Pending	
493	Undecipherable	
494	Security Agreement Required	RFC3329
500	Server Internal Error	
501	Not Implemented	
502	Bad Gateway	
503	Service Unavailable	
504	Server Time-out	
505	Version Not Supported	
513	Message Too Large	
580	Precondition Failure	RFC3312
600	Busy Everywhere	
603	Decline	
604	Does Not Exist Anywhere	
606	Not Acceptable	

9. ACRONYMS

ACK	ACKnowledge
CSCF	Call Session Control Function
DCCH	Dedicated Control Channel
DHCP	Dynamic Host Configuration Protocol
EPS	Evolved Packet System
ESM	EPS Session Management
FQDN	Fully Qualified Domain Name
GBR	Guaranteed Bit Rate
HSS	Home Subscriber Server
IANA	Internet Assigned Numbers Authority
I-CSCF	Interrogating Call Session Control Function
IMS	IP Multimedia Subsystem
IMS AKA	IMS Authentication and Key Agreement
Inter-RAT	Inter-Radio Access Technology
IPSec	IP Security
ISIM	IP Multimedia Services Identity Module
LZSS	Lempel-Ziv-Storer-Szymanski
MIB	Master Information Block
MME	Mobility Management Entity
NAS	Non-Access Stratum
P-CSCF	Proxy- Call Session Control Function
PDN	Packet Data Network
PRACK	Provisional ACK
QCI	QoS Class Identifiers
QoS	Quality-of-Service
RRC	Radio Resource Control
RTCP	RTP Control Protocol
RTP	Real-time Transport Protocol
S-CSCF	Serving Call Session Control Function
SDP	Session Description Protocol
SIB	System Information Block
SIP	Session Initiation Protocol
SMS	Short Message Service
SSD	Shared Secret Data
UA	User Agent
UDVM	Universal Decompressor Virtual Machine
UE	User Equipment
URI	Uniform Resource Identifier
USIM	UMTS Subscriber Identity Module
VoLTE	Voice over LTE

AMERICAS 1-800-SPIRENT | +1-818-676-2683 | sales@spirent.com
EUROPE AND THE MIDDLE EAST +44 (0) 1293 767979 | emeainfo@spirent.com
ASIA AND THE PACIFIC +86-10-8518-2539 | salesasia@spirent.com

Rev B. 03/14