SIPPING Working Group
Internet-Draft
Expires: April 11, 2003

M. Garcia-Martin
Ericsson

October 11, 2002

3rd-Generation Partnership Project (3GPP) Release 5 requirements on the Session Initiation Protocol (SIP)

draft-ietf-sipping-3gpp-r5-requirements-00.txt

Status of this Memo

Copyright Notice

Abstract

The 3rd Generation Partnership Project (3GPP) has selected SIP [2]as the session establishment protocol for the 3GPP IP Multimedia Core Network Subsystem (IMS). IMS is part of the Release 5 of the 3GPP specifications. Although SIP is a protocol that fulfills most of the requirements to establish a session in an IP network, SIP has never been evaluated against the specific 3GPP requirements for operation in a cellular network. In this document we express the requirements identified by 3GPP to support SIP for the Release 5 of the 3GPP IMS in cellular networks.

Table of Contents

1. Conventions

This document does not specify any protocol of any kind. Therefore, the usage of the key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document, as described in RFC-2119 [1], does not apply.

2. Introduction

3GPP has selected SIP [2]as the protocol to establish and tear down multimedia sessions in the IP Multimedia Subsystem (IMS). A description of the IMS can be found in 3GPP Technical Specification 23.228 [31]. A comprehensive set of session flows can be found in 3GPP Technical Specification 24.228 [32].

This document is an effort to define the requirements applicable to the usage of the SIP protocol suite in cellular networks, and particularly in the 3GPP IMS, and in particular, to the Release 5 of the 3GPP specifications. Further releases of the 3GPP specifications may contain additional requirements to SIP. This document focuses on the requirements identified for the 3GPP Release 5 IMS.

The rest of this document is structured as follows:

- Section 3 offers an overview of the 3GPP IMS. Readers who are not familiar with it should carefully read this section.

- o Section 4 contains the 3GPP requirements to SIP. Requirements are grouped by categories. Some requirements include a statement on possible solutions that would be able to fulfill the requirement. Note also that, as a particular requirement might be fulfilled by different solutions, not all the solutions might have an impact on SIP.

3. Overview of the 3GPP IMS

This section gives the reader an overview of the 3GPP IM CN Subsystem (IMS). It is not intended to be comprehensive. But it provides enough information to understand the basis of the 3GPP IMS. Readers are encouraged to find a more detailed description in the 3GPP Technical Specifications 23.060 [30], 23.228 [31] and 24.228 [32].

For a particular cellular device, the 3GPP IMS network is further decomposed in a home network and a visited network.

An IMS subscriber belongs to his or her home network. Services are

triggered and may be executed in the home network. One or more SIP servers are deployed in the SIP home network to support the IP Multimedia Subsystem. Among those SIP servers, there is a SIP serving proxy, which is also acting as a SIP registrar. Authentication/Authorization servers may be part of the home network as well. Users are authenticated in the home network.

A SIP outbound proxy is provided to support the UA. The SIP outbound proxy is typically located in the visited network, although it may located in the home network as well. The SIP outbound proxy maintains security associations between itself and the terminals, and interworks with the resource management in the packet network.

The SIP outbound proxy is assigned after the mobile device has connected to the access network. Once this proxy is assigned, it does not change while the mobile remains connected to the access network. Thus the mobile can move freely within the access network without SIP outbound proxy reassignment.

The home network may support also one or more SIP edge proxies. These nodes may act as the first entry point for SIP signaling to the

home network and may decide (with the help of location servers) which SIP registrar server to assign to a particular user. Typically the address of the home network SIP edge proxy is configured in DNS in the form of a DNS NAPTR and SRV records for SIP.

Additionally, home and visited networks may deploy, if required, a SIP hiding proxy. The main purpose of the SIP hiding proxy is to hide the network configuration.

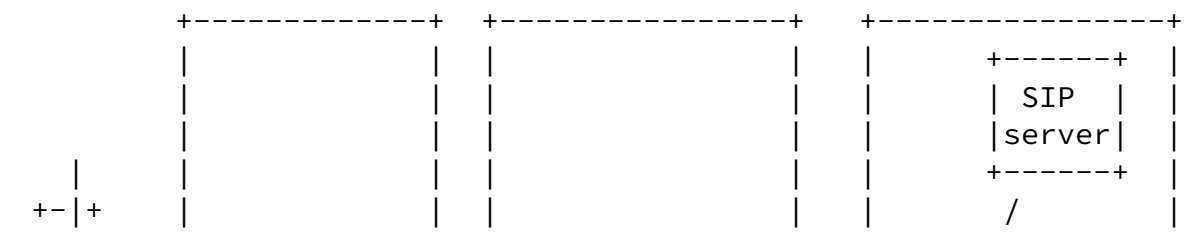
The 3GPP IM CN Subsystem is designed to be access independent. Access is granted from 3GPP cellular terminals or from other terminals that use other accesses out of the scope of 3GPP.

3GPP cellular IP Multimedia terminals use the existing General Packet Radio Service (GPRS) [30] as a transport network for IP datagrams. The terminals first connect to the GPRS network to get an IPv6 prefix. In order to do this, the terminals must perform a (GPRS) Attach procedure followed by a (GPRS) PDP Context Activation procedure. These GPRS procedures are required to be completed before any IP Multimedia session can be established.

As a result of the above-mentioned GPRS procedures, the terminal has built an IPv6 address. The IPv6 address belongs to the same network address space as the SIP outbound proxy. The address does not change as the mobile terminal moves while still attached to the same network address space.

If the terminal moves from a GPRS access to another GPRS access, the above-mentioned GPRS procedures needs to start from the beginning to allocate an IPv6 address to the terminal.

Figure 1 shows an overview of the 3GPP architecture for IM CN Subsystem.



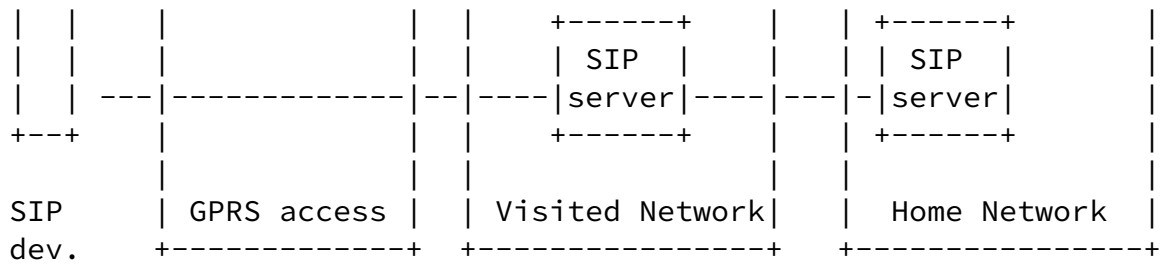


Figure 1: Overview of the 3GPP IMS architecture

Another possible future configuration is depicted in Figure 2. In that case, a general-purpose computer (e.g., a laptop computer) is connected to a GPRS terminal. The computer hosts the Multimedia application (comprising SIP, SDP, RTP, etc.). The GPRS terminal handles the radio access and the GPRS connectivity. Note that, for the sake of clarity, in this example the home network has not been depicted in the figure.

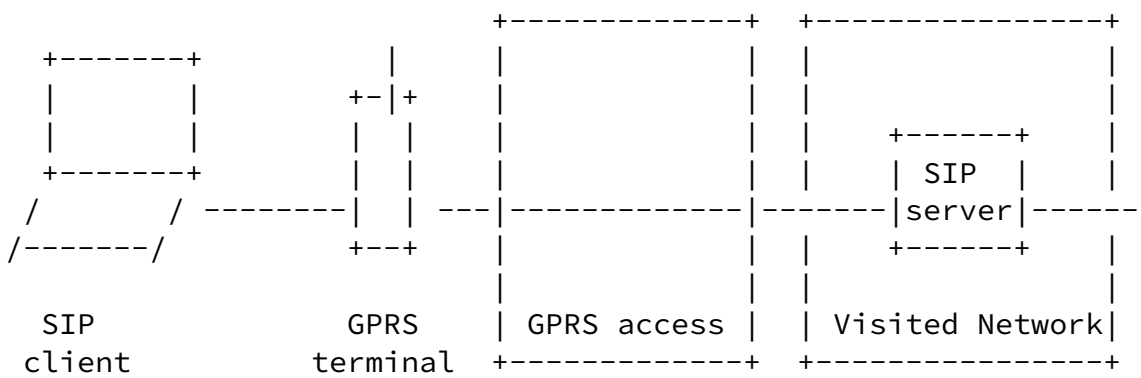


Figure 2: A computer connected to a GPRS terminal

Services are typically executed in an application server. The interface between the SIP server and the application server is based on SIP. However, certain operators may want to reuse the existing

technology, and therefore, they may need to interoperate SIP with protocols like CAMEL/Intelligent-Network or Open services Architecture (OSA).

4. 3GPP Requirements on SIP

4.1 General requirements

This section does not specify any particular requirement to SIP. However, it includes a list of general requirements that must be considered when developing solutions to particular requirements.

4.1.1 Efficient use of the radio interface

The radio interface is a scarce resource. As such, the exchange of signaling messages between the mobile terminal and the network should be minimized. All the mechanisms developed should make an efficient use of the radio interface.

See also the related requirements in Section 4.4

4.1.2 Minimum session setup time

All the procedures and mechanisms should have a minimum impact on the session setup time as perceived by the user. When there is a choice between performing tasks at session establishment and in transactions prior to session establishment, then the tasks should be performed prior to session establishment.

See also the related requirements in Section 4.4

4.1.3 Minimum support required in the terminal

As terminals could be rather small devices, memory requirements, power consumption, processing power, etc. should be kept to a minimum. Mandating support for additional protocols in the terminal must meet this requirement.

4.1.4 Roaming and non-roaming

All the requirements must be met for both roaming and non-roaming scenarios. There should not be a significant change in the signaling procedures between roaming and non-roaming scenarios.

4.1.5 Terminal mobility management

As terminal mobility is managed by the access network, there is no need to support terminal mobility management in SIP.

4.1.6 IP version 6

3GPP IMS is solely designed to use IP version 6. As a consequence, all protocols must support IPv6 addesses.

4.2 SIP outbound proxy

4.2.1 SIP outbound proxy

A SIP outbound proxy is provided to support both roaming and non-roaming scenarios. The SIP outbound proxy may be located either in the home network or in the visited network.

4.2.2 Discovery of the SIP outbound proxy

There must be a general mechanism so that the mobile device (UA) learns the SIP outbound proxy address.

The Internet Draft DHCPv6 option for SIP servers [22] seems to fulfill the requirement.

In addition to the above expressed requirement, the 3GPP access network may provide the SIP outbound proxy address during access network bearer establishment. This is considered a less general mechanism though.

4.3 Registration

The home network must maintain one or more SIP registrars. The SIP registrar authenticates the user and registers the IP address where the user can be located.

Once the terminal is switched on, the mobile device UA reads its configuration data. This data may be stored in a SIM card or any other memory device. The configuration data contains an identification of the home network. The device finds the SIP registrar address from the home network domain name. The terminal sends the registration through the SIP outbound proxy.

In order to support the search of the registrar, the home network contains one or more SIP servers that may be configured in DNS with the NAPTR/SRV record of SIP. These are the home network edge proxies. Their mission is to serve as a first point of contact in the home network, and decide (with the help of location servers) which SIP registrar server to assign to a particular user.

The procedures specified in RFC 3263 [11] applied to a REGISTER message seems to be sufficient to meet this requirement.

4.3.1 Registration required

A user must register to the IMS before he/she can receive any invitation to any sessions. In addition, it is desirable for the user to register before initiating any sessions. The rationale behind this is that:

1. The SIP serving proxy in the home network needs to know when the user is available and from which terminal, in order to route received SIP requests for sessions and services.

2. The user can be pre-authenticated early, so that authentication does not contribute to post-dial delay. The procedure should not have a penalty on the session setup time (see also the requirement stated in Section 4.1.2).

3. The user is assigned a particular serving proxy. The serving proxy downloads the service profile for that user to trigger services.

Therefore, 3GPP has mandated the mobile device UA to register before the mobile device UA initiates any session.

4.3.2 Location of the SIP Registrar

4.3.3 Efficient registration

Due to the scarce radio interface resource, a single registration must be sufficient to insure that the mobile UA is reachable from both the home and visited networks.

A single REGISTER message, addressed to the registrar, may traverse the SIP outbound proxy. This can install, if needed, soft registration states in the SIP outbound proxy.

4.3.4 Registration for roaming and non-roaming cases

Independently of whether the UA is roaming or not, it is desirable for the registration procedure to be the same.

4.3.5 Visited domain name

The home network must be able to validate the existence of a roaming

agreement between the home and the visited network. The home network needs to validate that the user is allowed to roam to such a visited network. Therefore, there must be a mechanism so that the visited network identity is known at registration time at the home network.

It is acceptable to represent the visited network identity either as a visited network domain name or as a string.

4.3.6 De-registration

4.3.6.1 De-registration of users

There must be a procedure for a user to de-register from the network. This procedure may be used, e.g., when the user deactivates the terminal.

We believe that a REGISTER with an expiration timer of 0 will meet the requirement.

4.3.6.2 Network initiated de-registration or re-registration

There are a number of situations where the network needs to de-register or trigger a re-registration of a previously registered UA. Examples of usage are described in Section 4.3.6.3, Section 4.3.6.4 and Section 4.3.6.5.

This implies a need for a notification mechanism whereby the UA can be notified of the de-registration, or a request for re-registration.

We believe this requirement is met by the SIP-specific event notification [13] and a registration event package [16].

4.3.6.3 Network initiated de-registration, network maintenance

There might be cases when the SIP serving proxy has to shutdown, e.g., due to maintenance operation. Although this situation is not likely to happen in everyday situations, still it is desirable to have a mechanism to inform the UA that his current registration is being cancelled. The UA may initiate another registration process, that will lead to the selection of a new SIP serving proxy.

4.3.6.4 Network initiated de-registration, network/traffic determined

The system must support a mechanism to avoid inconsistent information storage and remove any redundant registration information. This case will occur when a subscriber roams to a different network without a prior de-registration. This case occurs in normal mobility procedures when the user roams from one access network to another one, or when imposing new service conditions to roamers.

4.3.6.5 Network initiated de-registration, administrative

For different reasons (e.g., subscription termination, stolen

terminal, etc.) a home network administrative function may determine a need to clear a user's SIP registration. It is desirable to have a mechanism whereby the SIP serving proxy can inform the UA that his registration is being cancelled.

There must be a procedure for a the SIP serving proxy to de-register users. The de-registration information must be available at all the proxies that keep registration state and the UA.

We believe that a procedure based on SIP-specific event notification [13] and a registration event package [16].

4.4 SIP Compression

The radio interface is a scarce resource and typically, the available bandwidth over the radio interface is limited. These two factors seem to limit the transport of possibly large SIP messages over the air interface. Particularly, the session setup time might be extended, due to the time needed to transport SIP messages over a limited bandwidth channel.

On the other hand, the number and size of certain SIP header values, such as Via or Record-Route, seems to not be limited. A mobile device UA may present limitations in the available memory to store this kind of information.

Therefore, there must be a mechanism to efficiently transport SIP signaling packets over the radio interface, by compressing the SIP messages between the mobile device UA and the SIP outbound proxy, and

between the SIP outbound proxy and the mobile device UA. Note that compression of IP and transport layer protocol headers that carry these SIP messages is also a requirement, although we believe that does not have an impact on SIP.

4.4.1 Compression algorithm independency

The chosen solution(s) must be able to allow the operation under several different compression algorithms.

4.4.2 Extensibility of the SIP compression

The chosen solution(s) must be extensible to facilitate the incorporation of new and improved compression algorithms in a backward compatible way, as they become available.

4.4.3 Minimal impact of SIP compression on the network

Application specific compression must minimize impacts on existing

3GPP access networks (such as base stations transceivers). On the other hand, the compression mechanism should be independent of the access, e.g., the compression must be defined between the mobile device UA and the outbound SIP proxy.

4.4.4 Optionality of SIP compression

It must be possible to leave the usage of compression for SIP signaling optional. To facilitate mobile terminal roaming between networks which are using compression, the mobile terminal should always support ability to compress SIP signaling. If compression is not supported, communication may continue without compression, depending on the local policy of the visited network.

4.4.4.1 Compression reliability

The compression mechanism should be reliable and be able to recover automatically from errors generated during the decompression.

4.5 QoS requirements related to SIP

4.5.1 Independence between QoS signaling and SIP

The selection of QoS signaling and resource allocation schemes must be independent of the selected session control protocols. This allows for independent evolution of QoS control and SIP.

4.5.2 Coordination between SIP and QoS/Resource allocation

4.5.2.1 Allocation before alerting

In establishing a SIP session, it must be possible for an application to request that the resources needed for bearer establishment are successfully allocated before the destination user is alerted. Note, however, that it must be also possible for an SIP application in a terminal to alert the user before the radio resources are established (e.g., if the user wants to participate in the media negotiation).

We believe this requirement is met by Integration of Resource Management and SIP [17].

4.5.2.2 Destination user participates in the bearer negotiation

In establishing a SIP session, it must be possible for a terminating application to allow the destination user to participate in determining which bearers shall be established. Although it must be possible to establish the SIP session without user intervention.

We believe this requirement is met by the standard SDP negotiation described in SIP [2] and the SDP offer/answer model [12] and the extensions described in Integration of Resource Management and SIP [17].

4.5.2.3 Successful bearer establishment

Successful bearer establishment must include the completion of any required end-to-end QoS signaling, negotiation and resource allocation.

We believe this requirement is met by the procedures described in the Integration of Resource Management and SIP [17] .

4.6 Prevention of theft of service

Users are typically allocated QoS resources. There is an admission control mechanism that prevents users to exceeds the limits negotiated with the network. The network must prevent unauthorized users to make usage of non-authorized resources. For instance, the network must provide mechanism to prevent a user to use the resources allocated to a second user, and for which this second user may be paying.

We believe this requirement may be met by the procedures described in the Private SIP extensions for Media Authorization [18].

4.7 Radio resource authorization

As radio resources are very valuable the network must be able to manage these in a controlled manner. The network must be able to identify who is using these resources and be able to authorize their usage. For example, a mobile device terminal could execute an unlimited and uncontrolled resorce reservation procedure if the network does not supervise the usage of radio resources.

We believe this requirement is met by the procedures described in the Private SIP extensions for Media Authorization [18]..

4.8 Prevention of malicious usage

The 3GPP IMS must prevent mobile devices for making a malicious usage of the network. For instance, a malicious UA could not follow the Record-Route procedures, so that subsequent request bypass proxies which recorded route.

4.9 Prevention of denial of service

The risk of a proxy to receive a denial of service attack shall be minimized. For instance, a malicious mobile device could learn a SIP proxy IP address and port number (e.g., in a Record-Route header value) and establish an attack to that proxy.

4.10 Identification of users

4.10.1 Private user identity

In order to use the 3GPP IMS, a user is assigned a private user identity. The home network operator assigns the private user identity, which is used to uniquely identify the user from a network perspective. The private user identity is used, for example, for authentication, authorization, administration, and possibly accounting purposes. Note that the private user identity is not used for routing of SIP messages.

The private user identity is a unique global identity defined by the Home Network Operator. The identity takes the form of a Network Access Identifier (NAI) as defined in RFC 2486 [7].

The end user does not have access to the private user identity. Typically the identity is stored in a Subscriber Identity Module card.

The private user identity is permanently allocated to a user (it is not a dynamic identity), and is valid for the duration of the user's business subscription with the home network.

4.10.1.1 Private user ID in registrations

The mobile UA must deliver the private user identity to the SIP outbound proxy and the registrar at registration time.

The private user identity is used as the basis for authentication during registration of the mobile user. The term authentication is used in this document with the same meaning as it is defined in RFC 2828 [8].

We believe that this requirement is met by populating the username field of the Authorization: header value of the REGISTER request with the private user identity.

4.10.2 Public user identities

In order to use the 3GPP IMS, a user is assigned one or more public

user identities. The user will make use of the public user identity/

identities when requesting communication to other users. For example, the public user identity might be included on a business card.

Different public user identities may be grouped into a user profile. A user may have different profiles, each one containing different public user identities. A public user identity can be part of a single user profile.

The user may need to register one or more public user identities prior to receiving communications addressed to that public user identity.

We believe this requirement is met by populating the From: and To: header values of a REGISTER message with the public user identity.

4.10.2.1 Format of the public user identities

The public user identity/identities must take the form of a SIP URI (as defined in RFC 3261 [2] and RFC 2396 [4]) or the form of a E.164 [37]number.

We believe this requirement is met by using SIP URLs and telephone numbers represented in SIP URLs as described in SIP [3]. In addition, tel: URLs as specified in [13] can be used to fulfill the requirement.

4.10.2.2 Registration of public user IDs

It must be possible to register globally (i.e., through one single UA request) a user that has more than one public identity that belongs to the same user profile, via a mechanism within the IMS. In this case, the user will be registered with all the public identities associated to a user profile.

We believe this requirement may be accomplished by external procedures. For example, the user's profile may contain a list of alias identities that the registrar considers active if the primary identity is registered. The user may get informed of the automatically registered public user IDs by subscribing to its own registration state.

4.10.2.3 Authentication of the public user ID

Public user identities are not authenticated by the 3GPP IMS. However the network authorizes that the public user identity is associated to the registered private user identity.

There is a list of public user identities that are associated with each private user ID within the IMS. IMS will reject attempts to use other public identities with this private user ID.

4.10.3 Delivery of the dialed public user ID

Typically a UA will be registered under a set of different public user IDs. As such, sessions destined to the user can be placed to any of the registered public user IDs. The serving proxy, application server(s) in the termination network may apply certain filtering rules or services based on the public user ID contained in the Request-URI. The UA may also apply certain filtering rules or services based on the called public user ID.

As such, it must be possible, for all sessions, to deliver the dialed public user ID to the terminating entities, such as the serving proxy, application servers and the terminating UA.

4.11 Identifiers used for routing

Routing of SIP signaling within IMS must use SIP URLs as defined in SIP [2]. E.164 [37] format public user identities must not be used for routing within IMS, and session requests based upon E.164 format public user identities will require conversion into SIP URI format for internal IMS usage.

We believe that this requirement is achieved by translating E.164 numbers into SIP URIs. A database, such as ENUM [10] might do the job.

4.12 Hiding requirements

Although the requirements included in this section are not optional, the hiding feature is an optional to use through configuration. This means that a network operator can, at his desire, switch the hiding functionality on or off.

4.12.1 Hiding of the network structure

A network operator need not be required to reveal the internal network structure to another network (in Via, Route, or other headers) that may contain indication of the number of SIP proxies, domain name of the SIP proxies, capabilities of the SIP proxies or capacity of the network.

4.12.2 Hiding of IP addresses

A network need not be required to expose the explicit IP addresses of

the nodes within the network (excluding firewalls and border gateways).

4.12.3 SIP hiding proxy

In order to support the hiding requirements, a SIP hiding proxy may be included in the SIP signaling path. Such additional proxy may be used to shield the internal structure of a network from other networks.

4.13 Cell-ID

The identity of the cell through which the 3GPP UA is accessing the IMS (Cell-ID) may be used by the home network to provide localized services or information on the location of the terminal during an emergency call (when emergency calls are handled in IMS, see also the requirement stated in Section 4.16).

4.13.1 Cell-ID in signaling from the UA to the visited and home networks

Assuming that the Cell-ID is obtained by the UA by other mechanisms outside the scope or beyond SIP, the Cell-ID must be transported at least in the following procedures:

- Registration
- Session Establishment (Mobile Originated)
- Session Establishment (Mobile Terminated)
- Session Release

The Cell-ID is private information and only of interest in the UA home network. Therefore, the Cell-ID should be removed prior to sending the SIP signaling beyond the originating home network.

4.13.2 Format of the cell-ID

The cell-ID must be sent in any of the formats described in the 3GPP

Technical Specification 23.003 [29].

4.14 Release of sessions

In addition to the normal mechanisms to release a SIP session (e.g., BYE), two cases are considered in this section. The ungraceful release of the session (e.g., the terminal moves to an out-of-coverage zone) and the graceful session release ordered by the network (e.g., pre-paid caller runs out of credit).

We believe this requirement is met by a SIP entity acting as a so-called transparent back-to-back User Agent.

4.14.1 Ungraceful session release

If an ungraceful session termination occurs (e.g., flat battery or mobile leaves coverage), when a call stateful SIP proxy server (such as the SIP serving proxy at home) is involved in a session, memory leaks and eventually server failure can occur due to hanging state machines. To ensure stable server operation and carrier grade service, a mechanism to handle the ungraceful session termination issue must be provided. We assume that there is a mechanism by which the SIP outbound proxy is notified, by a mechanism external to SIP, of the ungraceful session termination. This allows transforming the ungraceful session release into a graceful session release ordered by the network (see next section). For example, the SIP outbound proxy, upon reception of the notification of loss of mobile radio coverage, could send a BYE request on behalf of the terminal, although this BYE cannot be authenticated.

4.14.2 Graceful session release

There must be a mechanism so that an entity in the network may order the release of resources to other entities. This may be used, e.g., in pre-paid calls when the user runs out of credit.

This release must not involve any request to the UA to send out a release request (BYE), as the UA might not follow this request. The receiving entity needs the guarantee that resources are released when requested by the ordering entity.

The following objectives must be met:

- o Accurately report the termination to the charging subsystem.
- o Release the associated network resources: bearer resources and signaling resources.
- o Notify other parties to the session, if any, of the session termination.

Where feasible, this mechanism should be at the SIP protocol level in order to guarantee access independence for the system.

4.15 Routing of SIP messages

4.15.1 SIP outbound proxy

The 3GPP architecture includes a SIP outbound proxy which is typically located in the visited network (although it may be located in the home network). This outbound proxy provides local services such as compression of SIP messages or security functions. In addition, the outbound proxy may interact with the media reservation mechanism to provide authentication and authorization support for media reservation.

All mobile terminal originated session setup attempts must transit the outbound proxy, so that the services provided by the outbound proxy can be delivered to the mobile terminal.

4.15.2 SIP serving proxy in the home network

The serving proxy in the home network allows triggering of user customized services that are typically executed in an application server.

All mobile terminal originated session setup attempts must transit the serving proxy in the home network, so that the proxy can properly trigger the SIP services allocated to the user(e.g., speed dial substitution). This implies a requirement for some sort of source-routing mechanism to assure these proxies are transited correctly.

4.15.3 INVITE might follow a different path than REGISTER

The path taken by an INVITE request need not be restricted to the specific path taken by a mobile terminal originated REGISTER request, e.g., the INVITE may traverse just the SIP outbound proxy and the SIP serving proxy, without passing through any other proxies. However, the path taken by the INVITE may follow the same path taken by the REGISTER .

4.15.4 SIP inbound proxy

The visited network may apply certain services and policies to incoming sessions (such as establishment of security services or interaction with the media reservation mechanism). Therefore, the visited network may contain a SIP inbound proxy for terminating sessions. In general, the SIP inbound proxy and the SIP outbound proxy are the same SIP proxy.

4.15.5 Distribution of the Source Routing set of proxies

Section 4.15.2 and Section 4.15.4 assume that a source routing mechanism is used to effect traversal of the required SIP proxies

during session setup.

There must be some means of dynamically informing the node which adds the source routing set of proxies that the INVITE has to traverse (e.g., the outbound proxy or serving proxy) of what that set of proxies should be.

The hiding requirements expressed in Section 4.12 also apply to the said set of proxies.

4.16 Emergency sessions

3GPP networks already contain alternative procedures to deliver emergency sessions. The Release 5 of the 3GPP specifications does not add any requirement with respect SIP emergency sessions.

4.17 Identities used for session establishment

4.17.1 Remote Party Identification presentation

It must be possible to present to the caller the identity of the party to which he/she may dial back to return a call.

We believe this requirement is met by the procedures described in draft-ietf-sip-asserted-identity [19].

4.17.2 Remote Party Identification privacy

In addition to the previous requirement, the called party must be able to request that his/her identity not be revealed to the caller.

We believe this requirement is met by the procedures described in draft-ietf-sip-privacy-general [20].

4.17.3 Remote Party Identification blocking

Regulatory agencies, as well as subscribers, may require the ability of a caller to block the display of their caller identification. This function may be performed by the destination subscriber's SIP serving proxy. In this way, the destination subscriber is still able to do a session-return, session-trace, transfer, or any other supplementary service.

Therefore, it must be possible that the caller requests to block the display of his/her identity at the callee's display.

We believe this requirement is met by the procedures described in draft-ietf-sip-privacy-general [20].

4.17.4 Anonymity

Procedures are required for an anonymous session establishment. However, sessions are not intended to be anonymous to the originating or terminating network operators.

We believe this requirement is met by the procedures described in draft-ietf-sip-privacy-general [20] and draft-ietf-sip-asserted-identity [19].

4.17.5 Anonymous session establishment

If the caller requests the session to be anonymous, the UAC must not reveal any identity information to the UAS.

If the caller requests the session to be anonymous, the terminating network must not reveal any identity or signaling routing information to the destination endpoint. The terminating network should distinguish at least two cases, first if the caller intended the session to be anonymous, and second if the caller's identity was deleted by a transit network.

We believe this requirement is met by the procedures described in draft-ietf-sip-privacy-general [20] and draft-ietf-sip-asserted-identity [19].

4.18 Charging

The 3GPP charging implications are described in the 3GPP Technical Specification 32.225 [34].

4.18.1 Support of both prepaid and postpaid models

Operators may choose to offer prepaid and/or postpaid services. The prepaid model is accomplished with the support of the on-line charging model. The postpaid model is accomplished by the support of the off-line charging model.

On-line charging is the process where charging information can affect, in real-time, the service rendered to the user, such as request for a graceful release of an existing session. On-line charging interacts with the SIP signaling.

Off-line charging is the process where charging information does not affect, in real-time, the service rendered to the user.

4.18.2 Charging correlation levels

The following levels of correlation for IMS charging are considered:

- Correlation within a session. A session may comprise a number of media components. It must be possible to correlate the charging data of the different media components belonging to a session.

- Correlation at media component level. For a session comprising several media types (such as audio and video), charging data is generated for each media type and needs to be correlated between network elements. For this, a media identifier shall be unique and shall clearly identify to which media type of a session this charging information belongs to. This component identifier is not exchanged between network elements and is based on the ordering of media flows in the SDP. This ordering is the same as the one used in the binding information passed to the GPRS network.

4.18.3 Charging correlation principles

To support the correlation of charging information, the following principles apply to both offline and online charging:

- The correlation of charging information for an IMS session is based on the use of IMS Charging Identifiers (ICID).

- The first IMS network entity within the SIP signaling path is responsible for assigning an ICID. This ICID shall then be passed along the whole session path in an end-to-end manner. However, this shall not preclude further elements (other SIP proxies) along the session path generating additional identifiers to be passed along.

- The ICID is passed to all IMS network entities in the session signaling path. This is performed using SIP signaling.

- The addresses of the charging functions are passed by the serving SIP proxy to all IMS network entities in the session signaling path. This is to provide a common destination for all the charging records generated by each IMS network entity with the same ICID.

- For the charging correlation between the GPRS network and the IMS, one or more GPRS Charging IDs, which identify the PDP contexts of the session, are passed from the GPRS network to the IMS.

- The GPRS Charging IDs are passed by the outbound SIP proxy to the

serving SIP proxy and the Application Servers using SIP signaling. They are not transferred from one home IMS (e.g., caller's home) to another home IMS (e.g., callee's home).

- o Inter Operator Identifiers (IOI) are shared betweenthe caller's home IMS and the callee's home IMS to provide identifiers of the home originating and home terminating networks.

4.18.4 Collection of Session Detailed Information

The SIP serving proxy or another SIP server in the home network must be able to log details of all sessions, such as the duration, source, and destination of a session, to provide to the charging subsystem.

4.19 General support of additional capabilities

4.19.1 Additional capabilities

3GPP is interested on applying and using additional services, like those described in SIP Call Control - Transfer [23], SIP Basic Call Flow Examples [24], SIP PSTN Call Flows [25] and SIP service examples [26]. Although 3GPP is not going to standardize additional services, 3GPP may make sure that the capabilities that enable those services are granted in the network.

As such we believe that the SIP REFER method [27] and the Replaces header [28] constitute a complement to be used as an enabler in order to meet the above requirement.

4.19.2 DTMF signaling

Support for voice calls must provide a similar level of service to the existing circuit based voice service. This includes the ability to utilize DTMF signaling e.g., for control of interactive voice response systems such as ticket sales lines, timetable information etc.

The transport of DTMF tones from the mobile terminal to target systems that may be in the PSTN, or to SIP based solutions (i.e., no PSTN connection) must be supported.

The transport of DTMF signals may be required for the whole call, just for the first part, or from some later point in the call, i.e., the start time and duration of such signaling is unpredictable.

We believe that the mechanisms specified in RFC 2833 [9] meet the

requirement without impacting SIP.

4.19.3 Early Media

As mobile terminals will frequently interoperate with the PSTN, support for early media is required.

4.20 Exchange of session description

Typically a session description protocol like SDP is used in SIP to describe the media streams and codecs needed to establish the session. SIP uses an offer/answer model of the session description, as described in RFC 3264 [12] where one of the parties offers his session description and the other answers to that offer.

In the 3GPP IMS, the mobile terminals might have restrictions with the memory, DSP capacity, etc. As such, it is required a mechanism by which the Session Description negotiation may conclude with one out of many codecs per media stream. Both UAC and UAS must know, prior to any media is sent or received, which codec is used for each media stream.

In the 3GPP IMS, an efficient use of the network and radio resources is an important requirement. As such, the network should know in advance which codecs is used for a particular media stream. The network access control may use this information to grant access to the network and control the resource utilization.

Additionally, it is required that the party who pays for the resource utilization has the opportunity to decide the codecs to use, once both end parties are aware of the capabilities supported at the remote UA.

Therefore, it is required a mechanism by which both UAC and UAS have the ability to negotiate and trim down the number of codecs used per media stream, so that at the end of the negotiation there can be a reduced set of agreed codecs per media stream.

We believe that the mechanism specified in RFC 3264 [12] meet the requirement.

4.21 Prohibition of certain SDP parameters

4.21.1 Prohibition of codecs

The SIP outbound proxy may contain local policy rules with respect the codecs allowed in the network. For instance, certain networks may disallow high bandwidth consuming audio codecs. There has to be a mechanism whereby the SIP outbound proxy can reject a session establishment attempt when a codec is prohibited in the network due

to local policy.

4.21.2 Prohibition of media types

Certain user's subscription may include restrictions to use certain media types. For instance, a user may not be allowed to establish a video session. The SIP serving proxy in the home network downloads the user profile, which contains the rules of this kind of restrictions.

As the establishment of sessions traverse the SIP serving proxy in the home network, this proxy can prohibit an attempt to establish a session that includes a non-allowed media type for the user. Therefore, there has to be a mechanism whereby the SIP serving proxy can reject a session establishment attempt when the session includes a forbidden media type.

4.22 Network initiated re-authentication

Network operators need to authenticate users to ensure that they are charged appropriately for the services they use. The re-authentication done when the user initiates a message will not suffice for this purpose, as described below.

If the duration of the authentication period is set to a relatively low value to ensure that the user cannot incur a high amount of charges between two authentications, it may create a lot of unnecessary authentications of users which have remained largely inactive, and therefore utilize unnecessary air interface resources.

If the duration of the authentication period is set to a relatively high value to avoid these unnecessary authentications the risk is then that some users may incur high charges between authentications.

A user's authentication is automatically invalidated when a certain threshold for charges (or number, or duration of sessions) is reached without giving the user a chance to re-authenticate, even if a valid registration exists. This would not provide an adequate level of service.

Consequently it must be possible for the network to initiate a re-authentication process at any time. The triggers must be set within the network and may include charging thresholds, number of events, session duration etc.

4.23 Security model

Section 4.23, Section 4.24 and Section 4.25 have been based on the

3GPP Technical Specifications 33.203 [35], 23.228 [31] and 33.210 [36].

The scope for security of the 3GPP IMS is securing the SIP signaling between the various SIP entities. Protecting the end-to-end media streams may be a future extension but is not considered in the Release 5 version of the IMS specifications.

Each operator providing IMS services acts as its own domain of trust, and shares a long-term security association with its subscribers (e.g., pre-shared keys). Operators may enter into roaming agreements with other operators, in which case a certain level of trust exists between their respective domains.

SIP user agents must authenticate to their home network before the use of IMS resources is authorized. In the Release 5 of the 3GPP IMS specifications, authentication is performed during registration and re-registrations.

Portions of the SIP signaling must be protected hop-by-hop. Looking at Figure 1 in Section 3, we can distinguish two distinct zones where the required security is unique:

- Access Domain: Between the SIP user device and the visited network.

- o Network Domain: Between the visited and the home networks, or inside the home network.

Characteristics needed in the Access Domain are quite different from those of the Network Domain because the terminal's requirements on mobility, computation restriction, battery limit, bandwidth conservation and radio interface. SIP entities in the access domain should be able to maintain security contexts with a large group of users in parallel. Furthermore, Access Domain provides user specific security associations while Network Domain provides security associations between network nodes. Therefore the weight of protocols and algorithms and the compliance of them with compression mechanisms are very important to Access Domain Security. It is therefore required that the security solutions must allow different mechanisms in these two domains.

4.24 Access Domain Security

4.24.1 General requirements

4.24.1.1 Scalability and Efficiency

3GPP IMS is characterized by a large subscriber base of up to a billion users, all of which must be treated in a secure manner.

The security solutions must allow global roaming among a large number of administrative domains.

4.24.1.2 Bandwidth and Roundtrips

The wireless interface in 3GPP terminals is an expensive resource both in terms of power consumption and maximum utilization of scarce spectrum. Furthermore, cellular networks have typically long round-trip time delays, which must be taken in account in the design of the security solutions.

Any security mechanism that involves 3GPP terminals should not unnecessarily increase the bandwidth needs.

All security mechanisms that involve 3GPP terminals should minimize the number of necessary extra roundtrips. In particular, during normal call signaling there should not be any additional security related messages.

For example, once an IPsec security association or a TLS connection is established, no additional round trips are required during session setup. However, the requirement of minimizing the number of round trips is hard to satisfy with IKE or TLS. It seems that IKE [6] adds a number of roundtrips, particularly if run together with legacy authentication extensions developed in the IPSRA WG. TLS [3] uses fewer roundtrips, but on the other hand doesn't support UDP.

4.24.1.3 Computation

It must be possible for mobile device terminals to provide security without requiring public key cryptography and/or certificates. 3GPP IMS may, however, include optional security schemes that employ these techniques.

Current HTTP authentication methods use only symmetric cryptography as required here. Lower-layer mechanisms (ex: IKE, TLS) require implementation of public-key cryptography and/or Diffie-Helman. If these lower-layer mechanisms were used, the mobile terminal would authenticate and negotiate session keys with the visited network using only symmetric methods.

4.24.1.4 Independence of the transport protocol

The selected security mechanism should work with any transport protocol allowed by SIP (e.g., TCP, UDP).

4.24.2 Authentication

Authentication, as used in this context, means entity authentication that enables two entities to verify the identity of the respective peer.

4.24.2.1 Authentication method

A strong, mutual authentication must be provided.

The authentication method must be able to work when there are zero or more SIP proxies in the SIP path between the authenticator and the authenticated user.

It must be possible to support extensible authentication methods. Therefore authentication using an extensible authentication framework is strongly recommended.

Authentication methods based on the secure storage of long-term keys used for authentication and the secure execution of authentication algorithms must be supported.

The SIP client's credentials must not be transferred as plain text.

3GPP intends to reuse UMTS AKA [15]. UMTS AKA applies a symmetric cryptographic scheme, provides mutual authentication, and is typically implemented on a so-called SIM card that provides secure storage on the user's side.

Additional requirements related to message protection that apply to the authentication method are stated in Section 4.24.3.

4.24.3 Message Protection

4.24.3.1 Message Protection Mechanisms

SIP entities (typically a SIP client and a SIP proxy) must be able to communicate using integrity and replay protection. By integrity, we mean the ability for receiver of a message to verify that the message has not been modified in transit. SIP entities should be able to communicate confidentially. In 3GPP IMS, these protection modes must be based on initial authentication. Integrity protection and confidentiality must be possible using symmetric cryptographic keys.

It must be possible to handle also error conditions in a satisfactory manner as to allow recovery (see also Section 4.3.6.3 and Section 4.14).

It must be possible to provide this protection between two adjacent

SIP entities. In future network scenarios it may also be necessary to provide this protection through proxies, though the 3GPP Release 5 IMS does not require this.

The security mechanism must be able to protect a complete SIP message.

If header compression/removal or SIP compression is applied to SIP messages, it must be compatible with message protection.

4.24.3.2 Delegation

3GPP IMS implements distributed security functions responsible for authentication and message protection.

It must be possible to perform an initial authentication based on long-term authentication credentials, followed by subsequent protected signaling that uses short-term authentication credentials, such as session keys created during initial authentication. The used authentication mechanism is able to provide such session keys. It must be possible to apply subsequent message protection as soon as possible, even during the initial authentication period.

Initial authentication is performed between the SIP UA and the authenticating SIP serving proxy in the home network. However, the authentication mechanism must not require access to the long-term authentication credentials in these nodes. In the home network, the authenticating SIP serving proxy must support interaction with a dedicated authentication server in order to accomplish the authentication task. At the client side a secured (tamper-resistant) device storing the long-term credentials of the user must perform the authentication.

Additionally, the SIP serving proxy that performed the initial authentication must be able to securely delegate subsequent SIP signaling protection (e.g., session keys for integrity or encryption) to an authorized SIP proxy further downstream. The tamper-resistant device at the client side must be able to securely delegate the session keys to the SIP user agent.

4.24.4 Negotiation of mechanisms

A method must be provided to securely negotiate the security

mechanisms to be used in the access domain.

This method must at least support the negotiation of different security mechanisms providing integrity protection and encryption, algorithms used within these mechanisms and additional parameters they require to be exchanged.

The negotiation mechanism must protect against attackers who do not have access to authentication credentials. In particular, the negotiation mechanism must be able to detect a possible man-in-the-middle attacker who could influence the negotiation result such that services with weaker or no security are negotiated.

A negotiation mechanism is generally required in all secure protocols to decide which security services to use and when they should be started. This security mechanism serves algorithm and protocol development as well as interoperability. Often, the negotiation is handled within a security service. For example, the HTTP authentication scheme includes a selection mechanism for choosing among appropriate algorithms. Note that when referring to negotiation we mean just the negotiation, not all functions in protocols like IKE. For instance, we expect the session key generation is to be a part of the initial authentication.

SIP entities must be able to use the same security mode parameters to protect several SIP sessions without re-negotiation. For example, security mode parameters may be assumed to be valid within the lifetime of a registration. Note that it is necessary to amortize the cost of security association setup and parameter negotiation over several INVITEs.

4.24.5 Verification of messages

4.24.5.1 Verification at the SIP outbound proxy

The SIP outbound proxy must be able to guarantee the message origin and verify that the message has not been changed (e.g., it is integrity protected).

4.24.5.2 Verification at the SIP serving proxy

The serving SIP proxy needs to receive an indication if the outbound proxy was able to verify the message origin and, in the case of a REGISTER request, whether it was integrity protected or not.

4.25 Network Domain Security

Message authentication, key agreement, integrity and replay

protection, and confidentiality must be provided for communications between SIP network entities such as proxy servers.

Network domain security mechanisms must be scalable up to a large number of network elements.

3GPP intends to make it mandatory to have the protection discussed above at least between two operators, and optional within an operator's own network. Security gateways exist between operator's networks.

We believe the above requirements to be fulfilled by applying security mechanisms as specified in the current IP Security standards specified in RFC 2401 [5].

5. Security considerations

This document does not define a protocol, but still presents some security requirements to protocols. The main security requirements are stated in Section 4.23, Section 4.24 and Section 4.25. Additional security-related issues are discussed under Section 4.6, Section 4.7, Section 4.8, Section 4.9, Section 4.12 and Section 4.10.

6. IANA considerations

This document introduces no new IANA considerations.

7. Contributors

The following people contributed to this document:

Duncan Mills (Vodafone), Gabor Bajko (Nokia), Georg Mayer (Siemens), Francois-Xerome Derome (Alcatel), Hugh Shieh (AWS), Andrew Allen (dynamicsoft), Sunil Chotai (mmO2), Keith Drage (Lucent), Jayshree Bharatia (Nortel), Kevan Hobbis (Huthison 3G UK), Dean Willis (dynamicsoft), Krisztian Kiss (Nokia), Vesa Torvinen (Ericsson), Jari Arkko (Ericsson), Sonia Garapaty (Nortel).

Normative References

[1] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[2] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M. and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, June 2002.

Informational References

[3] Dierks, T., Allen, C., Treese, W., Karlton, P., Freier, A. and P. Kocher, "The TLS Protocol Version 1.0", RFC 2246, January 1999.

[4] Berners-Lee, T., Fielding, R. and L. Masinter, "Uniform Resource Identifiers (URI): Generic Syntax", RFC 2396, August 1998.

[5] Kent, S. and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November 1998.

[6] Harkins, D. and D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409, November 1998.

[7] Aboba, B. and M. Beadles, "The Network Access Identifier", RFC 2486, January 1999.

[8] Shirey, R., "Internet Security Glossary", RFC 2828, May 2000.

[9] Schulzrinne, H. and S. Petrack, "RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals", RFC 2833, May 2000.

[10] Faltstrom, P., "E.164 number and DNS", RFC 2916, September 2000.

[11] Rosenberg, J. and H. Schulzrinne, "Session Initiation Protocol (SIP): Locating SIP Servers", RFC 3263, June 2002.

[12] Rosenberg, J. and H. Schulzrinne, "An Offer/Answer Model with Session Description Protocol (SDP)", RFC 3264, June 2002.

[13] Roach, A., "Session Initiation Protocol (SIP)-Specific Event Notification", RFC 3265, June 2002.

[14] Olson, S., Camarillo, G. and A. Roach, "Support for IPv6 in

Session Description Protocol (SDP)", RFC 3266, June 2002.

[15] Niemi, A., Arkko, J. and V. Torvinen, "Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)", RFC 3310, September 2002.

[16] Rosenberg, J., "A Session Initiation Protocol (SIP) Event Package for Registrations", draft-rosenberg-sip-reg-00 (work in progress), May 2002.

[17] Rosenberg, J., Camarillo, G. and F. Andreasen, "Integration of Resource Management and SIP", draft-ietf-sip-manyfolks-resource-07 (work in progress), April 2002.

[18] Evans, D., Marshall, W. and F. Andreasen, "SIP Extensions for Media Authorization", draft-ietf-sip-call-auth-06 (work in progress), May 2002.

[19] Watson, M., Peterson, J. and C. Jennings, "Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks", draft-ietf-sip-asserted-identity-02 (work in progress), August 2002.

[20] Peterson, J., "A Privacy Mechanism for the Session Initiation Protocol (SIP)", draft-ietf-sip-privacy-general-01 (work in progress), June 2002.

[21] Droms, R., Perkins, C., Bound, J., Volz, B., Carney, M. and T. Lemon, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", draft-ietf-dhc-dhcpv6-26 (work in progress), June 2002.

[22] Volz, B. and H. Schulzrinne, "DHCPv6 Options for SIP Servers", draft-ietf-sip-dhcpv6-00 (work in progress), April 2002.

[23] Sparks, R., "SIP Call Control - Transfer", draft-ietf-sip-cc-transfer-05 (work in progress), May 2002.

[24] Johnston, A., "Session Initiation Protocol Basic Call Flow Examples", draft-ietf-sipping-basic-call-flows-01 (work in progress), October 2002.

[25] Johnston, A., "Session Initiation Protocol PSTN Call Flows",

draft-ietf-sipping-pstn-call-flows-00 (work in progress), August 2002.

[26] Johnston, A., "SIP Service Examples", draft-ietf-sipping-service-examples-02 (work in progress), July 2002.

[27] Sparks, R., "The SIP Refer Method", draft-ietf-sip-refer-06 (work in progress), July 2002.

[28] Dean, R., Biggs, B. and R. Mahy, "The Session Inititation Protocol (SIP) 'Replaces' Header", draft-ietf-sip-replaces-02 (work in progress), May 2002.

[29] 3GPP, "TS 23.003 Numbering, addressing and identification (Release 5)", September 2002, <ftp://ftp.3gpp.org/Specs/archive/23_series/23.003/>.

[30] 3GPP, "TS 23.060:General Packet Radio Service (GRPS); Service Description; Stage 2", September 2002, <ftp://ftp.3gpp.org/Specs/archive/23_series/23.060/>.

[31] 3GPP, "TS 23.228: IP Multimedia Subsystem (IMS) (Stage 2) - Release 5", September 2002, <ftp://ftp.3gpp.org/Specs/archive/23_series/23.228/>.

[32] 3GPP, "TS 24.228: Signaling flows for the IP Multimedia call control based on SIP and SDP", September 2002, <ftp://ftp.3gpp.org/Specs/archive/24_series/24.228/>.

[33] 3GPP, "TS 24.229: IP Multimedia Subsystem (IMS) (Stage 3) - Release 5", September 2002, <ftp://ftp.3gpp.org/Specs/archive/24_series/24.229/>.

[34] 3GPP, "TS 32.225: Telecommunication Management; Charging Management; Charging Data Description for IP Multimedia Subsystem; (Release 5)", September 2002, <ftp://ftp.3gpp.org/Specs/archive/32_series/32.225/>.

[35] 3GPP, "TS 32.203: 3G Security; Access security for IP based services; (Release 5)", September 2002, <ftp://ftp.3gpp.org/Specs/archive/33_series/33.203/>.

[37] ITU-T, "Recommendation E.164 (05/97): The international public telecommunication numbering plan", May 1997, <http://www.itu.int/rec/recommendation.asp?type=folders&lang=e&parent=T-REC-E.164>.

Author's Address

Miguel A. Garcia Martin
Ericsson
Hirsalantie 11
Jorvas FIN-02420
Finland

EMail: miguel.a.garcia@ericsson.com

Full Copyright Statement

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.