Network Working Group
Internet Draft
Document: <draft-garcia-sipping-3gpp-reqs-02.txt>
Network Working Group
Date: November 2001
Expires: May 2002

M. Garcia / Ericsson
D. Mills / Vodafone
G. Bajko / Nokia
G. Mayer / Siemens
F. Derome / Alcatel
H. Shieh / AWS
A. Allen / Motorola
S. Chotai / BT
K. Drage / Lucent
J. Bharatia / Nortel
K. Hobbis / Hutchison
D. Willis / dynamicsoft

3GPP requirements on SIP

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026 [1].

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts. Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet- Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

The distribution of this memo is unlimited.

1. Abstract

The 3rd Generation Partnership Project (3GPP) has selected SIP [3] as the session establishment protocol for the 3GPP IP Multimedia Core Network Subsystem (IM CN Subsystem).

Although SIP is a protocol that fulfills most of the requirements to establish a session in an IP network, the SIP protocol suite 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 IM CN Subsystem in cellular networks.

2. Conventions used in this document

This document does not specify any protocol of any kind. Therefore, the use 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 [2], does not apply.

3. Table of Contents

4. Introduction

3GPP has selected SIP [3] as the protocol to establish and tear down multimedia sessions in the IP Multimedia Core Network Subsystem (IM CN Subsystem). A description of the IM CN Subsystem can be found in [4]. A comprehensive set of session flows can be found in [5].

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 IM CN Subsystem.

The rest of this document is structured as follows:

Section 5 offers an overview of the 3GPP IM CN Subsystem. Readers who are not familiar with it should carefully read this section.

Section 6 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.

5. Overview of the 3GPP IM CN Subsystem

This section gives the reader an overview of the 3GPP IM CN Subsystem. It is not intended to be comprehensive. But it provides enough information to understand the basis of the 3GPP IM CN Subsystem. Readers are encouraged to find a more detailed description in [4], [5] and [6].

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

An IM CN Subsystem 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.

The visited network contains a SIP outbound proxy to support the UA. The SIP outbound proxy in the visited network may translate locally dialed digits into international format, detect emergency sessions, maintain security associations between itself and the terminals, and interwork with the resource management in the packet network.

The SIP outbound proxy is assigned after the mobile 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 a SIP entry proxy. This node 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 entry proxy is configured in DNS in the form of a DNS SRV record 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) [6] as a transport network for IP datagrams. The terminals first connect to the GPRS network to get an IPv6 address. 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 obtained an IPv6 address. In the case of non-roaming terminals, the IPv6 address belongs to the home network address space. In the case of a roaming terminal, the IPv6 address belongs to the visited network address space. 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.

```
             +-------------+  +----------------+   +----------------+
             |             |  |                |   |                |
             |             |  |                |   |                |
             |             |  |                |   |      +------+  |
             |             |  |                |   |      | SIP  |  |
             |             |  |                |   |      |server|  |
       |     |             |  |                |   |      +------+  |
     +-|+    |             |  |                |   |       /        |
```

```
  |  |    |             |  |    +------+    |   | +------+       |
  |  |    |             |  |    | SIP  |    |   | | SIP  |       |
  |  | ---|-------------|--|----|server|----|---|-|server|       |
  +--+    |             |  |    +------+    |   | +------+       |
          |             |  |                |   |                |
  SIP     | GPRS access |  | Visited Network|   |  Home Network  |
  dev.    +-------------+  +----------------+   +----------------+
```

Figure 1: Overview of the 3GPP IM CN Subsystem architecture

Another possible 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, the home network has not been depicted in the figure.

```
                             +-------------+  +----------------+
                             |             |  |                |
                             |             |  |                |
                             |             |  |                |
                             |             |  |                |
                             |             |  |                |
      +-------+              |             |  |                |
      |       |       +-|+   |             |  |                |
      |       |       |  |   |             |  |    +------+    |
      +-------+       |  |   |             |  |    | SIP  |    |
     /       / --------|  | ---|-------------|-------|server|-----
-
    /-------/         +--+   |             |  |    +------+    |
                             |             |  |                |
      SIP             GPRS   | GPRS access |  | Visited Network|
     client         terminal +-------------+  +----------------+
```

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).

6. 3GPP Requirements on SIP

6.1 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.

6.1.1 Efficient use of the radio interface

The radio interface is a scarce resource. As such, the exchange of signaling messages between the UA 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 6.5.

6.1.2 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 6.5.

6.1.3 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.

6.1.4 Roaming and non roaming

The developed solutions should work efficiently in roaming and non-roaming scenarios.

6.1.5 Mobility management

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

6.1.6 IP version 6

The IP CN Subsystem is solely designed to use IP version 6 addresses.

6.2 SIP outbound proxy in the visited network

6.2.1 SIP outbound proxy in the visited network

A SIP outbound proxy, typically in the visited network, must be supported in both roaming and non-roaming case, even when the SIP serving proxy in the home network is located in the same network as the SIP outbound proxy.

6.2.2 Discovery of the SIP outbound proxy

There must be a general mechanism to configure the UA with the address of the SIP outbound proxy in the visited network.

The Internet Draft "DHCP option for SIP servers" [7] may be a good starting point to meet this requirement. However, there is no support for IPv6 in this Internet Draft.

3GPP has another mechanism provided by the GPRS access network that meets this requirement, in addition to the above one.

6.2.3 Removal of headers

Via and Record-Route headers in SIP have no fixed limit and in practice are very large (hundreds of bytes). These headers may represent a significant fraction of the total size of a typical SIP message. 3GPP proposes that the SIP outbound proxy remove and reinsert these headers on behalf of the mobile terminal, so that the size of SIP messages transmitted over the radio interface is reduced.

The SIP outbound proxy must be able to remove the network generated contents of the Via and Record-Route headers of the SIP requests to be sent to the UA. These contents are reinserted in the appropriate headers of the responses, as if they would have been included by the UA. This reduces SIP message sizes and thus transmission delay and peak bandwidth requirements over the radio interface.

6.3 Registration

Note that in SIP, registration is merely the association between SIP URLs and various Contacts. No additional information is implied by the existence of such registration data.

6.3.1 Registration required

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

1. The user must be reachable for terminating sessions and services;
2. The user is pre-authenticated early, so that authentication does not contribute to post-dial delay.
3. The user is assigned a particular serving proxy. The serving proxy downloads the service profile for that user.

The procedure should not have a penalty on the session setup time (see also requirement 6.1.2).

6.3.2 Location of the SIP Registrar

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 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 are configured in DNS with the SRV record of SIP. These are the home network entry 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 SIP [3], section 1.4.2, applied to a REGISTER message seems to be sufficient to meet this requirement.

6.3.3 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 in the visited network. This can install, if needed, soft registration states in the SIP outbound proxy.

6.3.4 Registration for roaming and non roaming cases

In order to facilitate roaming between different networks, the UA must be able to register independent of its roaming status. In the interest of simplicity, it is desirable for the registration procedure to be the same within both home and visited networks.

6.3.5 Visited domain name

The home network must be able to validate that there is 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 in the home network. As such, the visited network identity must be transported from the SIP outbound proxy to the home network.

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

6.4 De-registration

6.4.1 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.

6.4.2 Network initiated de-registration

There are a number of situations where the network needs to de-register a previously registered UA. Examples include 6.4.3, 6.4.4 and 6.4.5.

Continued function requires that the affected UA re-registers in a timely fashion. This implies a need for a notification mechanism to inform the UA of the need to re-register.

We believe this requirement is met by the SIP events [15] and a registration event package, similar to the one defined in [40].

6.4.3 Network initiated de-registration, network maintenance

The IM CN Subsystem may initiate the network initiated de-registration procedure due to forced re-registrations from subscribers, e.g. in case of data inconsistency at node failure, in case of SIM lost, etc. Canceling the current contexts of the user spread among the network nodes at registration, and imposing a new SIP registration solves this condition.

6.4.4 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. 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.

6.4.5 Network initiated de-registration, administrative

For different reasons (e.g., subscription termination, lost terminal, etc.) a home network administrative function may determine a need to clear a user’s SIP registration. This function initiates the de-registration procedure and may reside in various elements depending on the exact reason for initiating the de-registration.

There must be a procedure for an entity in the network 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 events [15] and a registration package will meet the requirement.

6.5 Compression of SIP signaling

As the radio interface is a scarce resource, the transport of SIP messages over the radio interface must be done efficiently.

Therefore, there must be a mechanism to efficiently transport SIP signaling packets over the radio interface, by compressing the SIP signaling messages between the UA and the SIP outbound proxy, and by compressing the IP and transport layer protocol headers that carry these SIP messages.

6.5.1 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.

6.5.2 SIP compression and roaming

The chosen solution(s) for SIP compression must work in roaming scenarios.

6.5.3 Minimal impact of SIP compression on the network

Application specific compression must minimize impacts on existing 3GPP network, e.g. the compression must be defined between the UA at the SIP terminal and the outbound SIP Proxy in the visited network.

6.5.4 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.

6.5.5 Default algorithm for SIP compression

If SIP signaling compression is used, a default algorithm must be supported by the UA and the network elements involved for compression.

6.5.6 Compression Negotiation

There must be a mechanism to negotiate between the UA and the first SIP outbound proxy the compression algorithm to be used. The type of negotiation mechanism that should be implemented is that the UAC includes a list of compression algorithms and the first SIP outbound proxy responds with the selected one. Subsequent SIP messages are compressed based on the agreed algorithm.

Note: 3GPP is investigating if the compression of SIP signaling is negotiated on a per call basis, on a per registration basis or something completely different. More information will be provided in future versions of this document.

6.6 QoS requirements related to SIP

6.6.1 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.

6.6.2 Coordination between SIP and QoS/Resource allocation

6.6.2.1 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 [8] and [21].

6.6.2.2 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.

We believe this requirement is met by the standard SDP negotiation described in [3] and the extensions described in [8] and [21].

6.6.2.3 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 [8] and [21].

6.7 Prevention of theft of service

The possibility for theft of service in the 3GPP IM CN Subsystem shall be no higher than that for the corresponding GPRS and circuit switched services.

We believe this requirement is met by the procedures described in [9].

6.8 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.

We believe this requirement is met by the procedures described in [9].

6.9 Prevention of denial of service

The system unavailability due to denial of service attacks in the IM CN subsystem shall be no greater than that for the corresponding GPRS and circuit switched services.

We believe this requirement is met in part by the procedures described in [9].

6.10 Identification of users

6.10.1 Private user identity

To use the 3GPP IM CN Subsystem, a subscriber must have a private user identity. The private identity is assigned by the home network operator, and used, for example, for registration, authorization, administration, and possibly accounting purposes. This identity shall take the form of a Network Access Identifier (NAI) as defined in RFC 2486 [10].

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, which may be used within the home network to uniquely identify the user from a network perspective.

The private user identity is not accessible by the user. Typically this identity is stored in a SIM card.

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

6.10.1.1 Private user ID in registrations

The 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 subscriber. The term authentication is used in this document with the same meaning as it is defined in [39].

The current working assumption is that this requirement is met by populating the From: header value of the REGISTER message with the private user ID.

6.10.2 Public user identities

To use the 3GPP IM CN Subsystem, a subscriber must have one or more public user identities. The public user identity/identities are used by any user for requesting communications to other users. For example, this 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 current working assumption in 3GPP is that this requirement is met by populating the To: header value of a REGISTER message with the public user ID. In an outbound call, the From: and/or the Remote-Party-ID header values are populated with any of the public user identities.

6.10.2.1 Format of the public user identities

The public user identity/identities must take the form of a SIP URL (as defined in SIP [3] and RFC2396 [11]) or the form of a E.164 number [12].

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.

6.10.2.2 Registration of public user IDs

It must be possible to register globally (i.e. through one single UA request) a subscriber that has more than one public identity that belongs to the same user profile, via a mechanism within the

IM CN Subsystem. In this case, the user will be registered with all the public identities associated to a user profile. This must not preclude the user from registering individually some of his/her public identities if needed.

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.

6.10.2.3 Authentication of the public user ID

Public user identities are not authenticated by the 3GPP IM CN Subsystem. However the network authorizes that the public user identity is associated to the registered private user identity. There is a list of public user IDs that are associated with each private user ID within the IM CN Subsystem. The IM CN Subsystem will reject attempts to use other public identities with this private user ID.

6.10.3 Delivery of the dialed public user ID

Typically a UA will be registered under a set of different public user IDs. As such, terminating sessions 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 initial dialed public user ID. The UA may also apply certain filtering rules or services based on the initial dialed public user ID.

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

6.11 Identifiers used for routing

Routing of SIP signaling within the IM CN Subsystem must use SIP URLs as defined in [3]. E.164 [12] format public user identities must not be used for routing within the IM CN Subsystem, and session requests based upon E.164 format public user identities will require conversion into SIP URL format for internal IM CN Subsystem usage.

We believe that this requirement is achieved by translating E.164 numbers into SIP URLs. A database, such as ENUM [14] might do the job.

6.12 Hiding requirements

We believe that the requirements in this section are met by the current SIP protocol [3].

6.12.1 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. Association of the node names of the same type of entity and their capabilities and the number of nodes may be kept private within an operator’s network. However disclosure of the internal architecture must not be prevented on a per agreement basis.

6.12.2 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).

6.12.3 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.

6.13 Cell-ID

The identity of the cell through which the 3GPP UA is accessing the IM CN Subsystem (Cell-ID) may be used by either the visited or the home network to provide localized services or information on the location of the terminal during an emergency call (see also requirement 6.16.3).

6.13.1 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 visited and home network serving the UA. Therefore, the Cell-ID should be removed prior to sending the SIP signaling beyond the network of originating serving proxy.

6.13.2 Format of the cell-ID

The cell-ID must be sent in any of the formats described in [22].

6.14 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).

6.14.1 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 one of the SIP proxies in the path is notified 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, a stateful SIP server in the signaling path could send a BYE on behalf of the mobile terminal.

6.14.2 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:
a) Accurately report the termination to the charging subsystem.
b) Release the associated network resources: bearer resources and signaling resources.
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.

6.15 Routing of SIP messages

In order to clarify the terminology, we introduce the term vector to refer to the set of proxies that the INVITE has to traverse.

6.15.1 SIP outbound proxy in the visited network

The 3GPP architecture includes an outbound proxy in the visited network. This outbound proxy provides local services such as location-specific internationalization functions. In addition, the outbound proxy may interact with the media reservation mechanism to provide authentication and authorization support for media reservation.

6.15.2 SIP serving proxy in the home network

All session setups must transit the serving proxy in the home network. This allows services to be triggered in the serving proxy on behalf of the user (example: speed dial substitution). Both the outbound proxy in the visited network (see previous paragraph) and the serving proxy in the home network must be transited for every (non-emergency) mobile-originated session. This implies a requirement for some sort of source-routing mechanism to assure these proxies are transited correctly.

6.15.3 INVITE might follow a different path than REGISTER

The path taken by the INVITE need not be restricted to the specific path taken by the REGISTER. However, the path taken by the INVITE may follow the same path taken by the REGISTER (e.g., the INVITE may traverse just the SIP outbound proxy in the visited network and the SIP serving proxy in the home network, without passing through any other proxies).

6.15.4 SIP inbound proxy in the visited network

The visited network may apply certain local policies to incoming sessions. 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 entity in the visited network.

6.15.5 Distribution of the Source Routing Vector

Section 6.15.2 and 6.15.4 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 vector (e.g., the outbound proxy or serving proxy) of what that vector should be.
The hiding requirements expressed in section 6.12 also apply to the vectors.

6.16 Emergency sessions

It must be possible to place an emergency session using the IM CN Subsystem. Emergency calls will be routed to the emergency services in accordance with national regulations for where the subscriber is located.

6.16.1 Authentication is not required for emergency calls

It must be possible to place an emergency session using SIP, independently on whether the user is authenticated by the IM CN Subsystem or not. Note, however, that in certain countries, it might be possible to reject an emergency call when the user is not authenticated by the IM CN Subsystem.

6.16.2 SIP outbound proxy support

Emergency sessions must be handled by the SIP outbound proxy in the visited network.

6.16.3 Cell Global ID in emergency sessions

It is required that location information including Cell Global ID (see also requirement 6.13) be made available in the initial INVITE and the BYE message for the purpose of locating the user and routing to the appropriate Emergency Call Center.

6.16.4 Types of emergency calls

It must be possible to initiated emergency calls to different emergency call centers, depending on the type of emergency. The following types of emergency calls are possible:

- Police
- Ambulance
- Fire brigade
- Marine guard
- Mountain rescue
- Spare, at least three different types

6.16.4 Default identifier for emergency calls

In order to support emergency calls in roaming situations, it must be allowed to establish an emergency call without the need to dial a dedicated number or SIP URL. This allows to dial an emergency center based on a menu, "red button" or a linkage to a car air bag control.

Additionally, it is desirable that the user interface for emergency calls in 3GPP terminals is similar to the one in other SIP networks.

3GPP is currently investigating the applicability of the Universal Emergency SIP URL described in [36].

6.17 Identities on session establishment

6.17.1 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 [16].

6.17.2 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 [16].

6.17.3 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 [16].

6.17.4 Anonymity

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

Note: 3GPP is still discussing whether the requirement is needed or not.

6.17.4.1 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.

6.18 Charging

It must be possible to apply charging, in a flexible manner based on any number of different charging models. Specific charging models and requirements for charging are under study. Some general requirements are listed below.

6.18.1 Collection of Call Detail 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 call, to provide to the charging subsystem.

6.18.2 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 accomplish 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.

6.19 IPv6

As the 3GPP architecture is solely based on IP version 6, all protocols must support IPv6 addresses.

We believe SIP [3] and SDP [17] meet this requirement. However, the "DHCP option for SIP servers" [7] does not support IPv6.

6.19.1 Interworking IPv6 with IPv4

3GPP IM CN subsystem is based on IPv6. As external networks may be based on IPv4 addresses, there is a need to interwork with such a external networks. Therefore, interworking between IPv6 and IPv4 at the SIP and SDP level (UAs and proxies) must be guaranteed.

6.20 General support of additional capabilities

6.20.1 Additional capabilities

3GPP is interested on applying and using additional services, like those described in [19], [37] and [38]. 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 REFER method [18] and the Replaces header [20] constitute the enablers in order to meet the above requirement.

6.20.2 DTMF signalling

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 transfer 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.

6.20.3 Early Media

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

6.21 Three-way handshake in the session description negotiation

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 where one of the parties offers his session description and the other answers to that offer.

In 3GPP IM CN Subsystem, the terminals might have restrictions with the memory, DSP capacity, etc. As such, it is required that the Session Description negotiation concludes with one out of many single 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 3GPP IM CN Subsystem, an efficient use of the network and radio resources is an important requirement. As such, the network must know in advance which codec is used for a particular media stream. The network may use this information to apply the most appropriate error correction mechanism depending on the selected codec. The network access control may use this information as well.

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

Therefore, it is required a three-way handshake model in the session description negotiation within SIP. This follows the model of offer/counter-offer/response of the session description. In this model the person who pays for the resources offers his collection of codecs, the remote party offers his selection of available codecs, and again the person who pays decides which codec to use.

6.22 Security Model

Sections 6.22, 6.23 and 6.24 have been based on the 3GPP documents [23], [4], and [24], and the work done by Dirk Kroeselberg in the Internet-Draft [31] (now expired).

The scope for security of the 3GPP IM CN Subsystem 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 first version of the IM CN Subsystem.

It is expected that security for the underlying GPRS network and the IM CN Subsystem will be provided independent of each other. Therefore, SIP signaling security must be provided independently of underlying access network security mechanisms. In particular, it must be possible to access the IM CN Subsystem services securely from other accesses than GPRS.

Each operator providing IM CN Subsystem 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 IM CN Subsystem resources is authorized. The current working assumption in the 3GPP is to perform authentication during registration and re-registrations.

Portions of the SIP signaling must be protected hop-by-hop. Looking at Figure 1 in Chapter 5, we can distinguish two distinct zones where the required security is unique:

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

- 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.

Note that authentication, as used in this context, means entity authentication that enables two entities to verify the identity of the respective peer. This is different from message origin authentication, which allows a receiver to verify the origin of a single message and is provided by the same means as integrity protection.

6.23 Access Domain First-Hop Security

6.23.1 Authentication

The client and the home network must authenticate before access is granted. Also, the client and visited proxy must establish a security association in a manner that ensures that both the client and the home network have accepted such a security association to be established.

Strong, mutual authentication method must be used.

It must be possible to support different authentication methods. Therefore authentication using an extensible authentication framework must be provided.

Authentication methods must support the secure storage of long-term authentication keys and the secure execution of authentication algorithms.

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

HTTP Basic Authentication sends the passwords as plain text, also, it is neither strong nor does it offer mutual authentication. HTTP Digest has an option for mutual authentication. It uses cryptographic means for authentication, but does not protect against man-in-the-middle attacks where attackers modify the request while preserving the authentication headers. Lower layer mechanisms allow strong and mutual authentication (but do not fulfill other requirements such as avoidance of public key cryptography and the minimization of roundtrips at session set-up). 3GPP intends to reuse UMTS AKA [24], but would prefer to a generic authentication framework at SIP level that supports UMTS AKA as well as other authentication mechanisms. 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 delegation that apply to the authentication method are given in section 6.23.2.3.

6.23.2 Scalability and Efficiency

3GPP IM CN Subsystems will be 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.

6.23.2.1 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.

Once an IPsec security association or a TLS connection are established, no additional round trips are required during call setup. However, the roundtrip requirements at registration time are particularly hard to satisfy. It seems that IKE [32] adds a number of roundtrips, particularly if run together with legacy authentication extensions developed in the IPSRA WG. TLS [25] uses fewer roundtrips, but on the other hand doesn’t support UDP.

6.23.2.2 Computation

It must be possible for IM CN Subsystem terminals to provide security without requiring public key cryptography and/or certificates. There may, however, be optional security schemes that employ these techniques.

Current HTTP authentication methods use only symmetric cryptography as required here (but do not meet other requirements). 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.

HTTP EAP [27] is another candidate method to allow both symmetric cryptography and asymmetric cryptography based authentication within SIP, though there are probably other candidates as well, such as GSS_API [28]. However, definition of UMTS AKA under EAP is already in progress [29].

6.23.2.3 Delegation of Security Tasks

Performing authentication on all SIP signaling messages would likely create bottlenecks in the authentication infrastructure. Therefore, a distributed implementation of security functions responsible for authentication is required.

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 registration. The used authentication mechanisms must be able to provide such session keys.

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-proof) 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-proof device at the client side must be able to securely delegate the session keys to the SIP user agent.

Initial authentication can be performed with existing mechanisms such as HTTP Digest [3], but there exists no method to allow subsequent protection of the SIP signaling messages. There are also no proposals to allow secure delegation of signaling protection task. Currently the use of SIP together with an authentication server isdifficult and limited in scope, though several proposals are under way to extend this [33, 34, 35]. However, the purpose of this document is not to discuss AAA requirements. They are discussed elsewhere.

6.23.3 Negotiation of mechanisms

A method must be provided to securely negotiate the security services to be used in the access domain.

This method must at least support the negotiation of different security services providing integrity protection and encryption, algorithms used within these services 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, it must not be possible for man-in-the-middle attackers to influence the negotiation result such that services with lower 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 authentication methods and 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 may 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 SA setup and parameter negotiation over several INVITEs during the registration period. However, as clients move around, it may not be possible to keep SA statebeyond the registration period.

Existing lower-layer security mechanisms provide the above functionality. We do not currently know of any mechanism that would allow this also at the SIP layer. The mechanism described in [30] might perhaps be extended to perform secure negotiation. Note that such a mechanism is required not only for negotiation of security mechanisms, but for other services as well, e.g. for compression (see section 6.5.6). Although negotiation of security mechanisms is different due to the need for secure negotiation, all negotiation mechanisms could operate in a similar fashion.

6.23.4 Message protection

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. 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 6.4.3 and 6.14).

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 at the moment 3GPP does not require this.

The security mechanism should not incur external limitations to any transport bearers carrying SIP message (for example, UDP).

All the lower layer security mechanisms offer these services for the hop-by-hop case, but currently we do not know of any mechanism that would allow also end-to-end operation.

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.

6.23.5 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.

6.24 Network Domain Security

Message authentication, key agreement, integrity and replay protection, and confidentiality must be provided for communications between SIP network entities such as proxies and servers.

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

The 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 [26].

7. Security considerations

This document does not define a protocol, but still presents some security requirements to protocols. The main security requirements are in sections 6.22 "Security Model", 6.23 "Access Domain Security" and 6.24 "Network Domain Security". Additional security-related issues are discussed under 6.7 "Prevention of theft of service", 6.8 "Radio resource authorization", 6.9 "Prevention of denial of service", 6.12 "Hiding requirements" and 6.10 "Identification of users".

8. Author's Addresses

Miguel A. Garcia
Ericsson
FIN-02420, Jorvas, Finland
Tel: +358 9299 3553
e-mail: miguel.a.garcia@ericsson.com

Duncan Mills
Vodafone UK Ltd.
The Courtyard, Newbury, Berkshire, RG14 1JX, UK
Tel: +44 1635 676074

Fax: +44 1635 234445
e-mail: duncan.mills@vf.vodafone.co.uk

Gabor Bajko
Nokia
H-1096 Budapest, Koztelek 6, Hungary
Tel: +36 20 9849259
e-mail: gabor.bajko@nokia.com

Georg Mayer
Siemens
Hofmannstr. 51, 81359 Munich, Germany
Tel: +49-172-5371233
e-mail: georg.mayer@icn.siemens.de

Francois-Xavier Derome
Alcatel
10 rue latecoere, F-78141
tel: +33 130 773 834
e-mail: francois-xavier.derome@alcatel.fr

Hugh Shieh
AT&T Wireless
PO Box 97061, Redmond, WA 98073
Tel: +1 425 580 6898
e-mail: hugh.shieh@attws.com

Andrew Allen
Motorola,
1501 W Shure Dr,
Arlington Hts, IL 60004
Phone: 847-435-0016
e-mail: CAA019@motorola.com

Sunil Chotai
BT
Adastral Park, Ipswich, UK.
Tel: +44 1473 605603
e-mail: sunil.chotai@o2.com

Keith Drage
Lucent Technologies
Tel: +44 1793 776249
e-mail: drage@lucent.com

Jayshree Bharatia

Nortel Networks
2201 Lakeside Blvd.
Richardson, Texas 75082
Tel: +1 972 684 5767
e-mail: jayshree@nortelnetworks.com

Kevan Hobbis
Hutchison 3G UK Ltd
Star House
20 Grenfell Road
Maidenhead
Berkshire, UK
Tel: +44 1628 765252
e-mail: kevan.hobbis@hutchison3g.com

Dean Willis
dynamicsoft Inc.
5100 Tennyson Parkway
Plano,TX 75024
email: dwillis@dynamicsoft.com

9. Acknowledgments

The authors will like to thank Rohan Mahy and the members of the 3GPP CN1 and SA3 mailing lists for their collaborative effort.

10. References

1. S. Bradner, "The Internet Standards Process -- Revision 3", BCP 9, RFC 2026, October 1996.

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

3. J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, E. Schooler: "SIP, Session Initiation Protocol", draft-ietf-sip-rfc2543bis-05.txt, October 2001, work in progress.

4. 3GPP TS 23.228 "IP Multimedia (IM) Subsystem (Stage 2) - Release 5". Version 5.1.0 is available at ftp://ftp.3gpp.org/Specs/2001-06/Rel-5/23_series/23228-510.zip

5. 3GPP TS 24.228: "Signaling flows for the IP Multimedia call control based on SIP and SDP". Version 1.7.0 is available at ftp://ftp.3gpp.org/Specs/Latest_drafts/24228-170.zip

6. 3GPP TS 23.060: "General Packet Radio Service (GRPS); Service Description; Stage 2". Version 4.1.0 is available at ftp://ftp.3gpp.org/Specs/2001-06/Rel-4/23_series/23060-410.zip

7. H. Schulzrinne, G. Nair. "DHCP Option for SIP Servers", draft-ietf-sip-dhcp-04.txt, March 2001, work in progress.

8. W. Marshall et al. "Integration of Resource Management and SIP", draft-ietf-sip-manyfolks-resource-02.txt, August 2001, work in progress.

9. W. Marshall et al. "SIP Extensions for Media Authorization", draft-ietf-sip-call-auth-02.txt, August 2001, work in progress.

10. B. Aboba, M. Beadles, "The Network Access Identifier", RFC 2486, January 1999.

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

12. ITU-T Recommendation E.164 (05/97): "The international public telecommunication numbering plan".

13. A. Vaha-Sipila, "URLs for Telephone calls", RFC 2806, April 2000.

14. P. Faltstrom, "E.164 number and DNS", RFC 2916, September 2000.

15. A. Roach, "SIP-Specific Event Notification", draft-ietf-sip-events-01.txt, November 2001, work in progress.

16. W. Marshall et al, "SIP Extensions for Caller Identity and Privacy", draft-ietf-sip-privacy-02.txt, May 2001, work in progress.

17. M. Handley, V. Jacobson, C. Perkins: "SDP: Session Description Protocol", draft-ietf-mmusic-sdp-new-03.txt, July 2001, work in progress.

18. R. Sparks: "The REFER method", draft-ietf-sip-refer-02.txt, October 2001, work in progress.

19. R. Sparks: "SIP Call Control - Transfer", draft-ietf-sip-cc-transfer-05.txt, July 2001, work in progress.

20. B. Biggs and R. Dean, "The SIP Replaces Header", draft-sip-replaces-01.txt, July 2001, work in progress.

21. J. Rosenberg, H. Schulzrinne: "Reliability of Provisional Responses in SIP", draft-ietf-sip-100rel-04.txt, September 2001, work in progress.

22. 3GPP TS 23.003, "Numbering, addressing and identification (Release 5)". Version 5.0.0 is available is available at ftp://ftp.3gpp.org/Specs/2001-06/Rel-5/23_series/23003-500.zip

23. 3GPP TS 33.203 "Access Security for IP-Based Services", Version 0.5.0 is available at ftp://ftp.3gpp.org/tsg_sa/WG3_Security/TSGS3_ADHOC_MAP_IMS_Sophia/Docs/PDF/S3z010089.pdf

24. 3GPP TR 33.210 "Network Domain Security", Version 0.6.0.

25. T. Dierks, C. Allen. "The TLS Protocol Version 1.0", RFC 2246, January 1999.

26. S. Kent, R. Atkinson. "Security Architecture for the Internet Protocol", RFC 2401, November 1998.

27. V. Torvinen, J. Arkko, A. Niemi. "HTTP Authentication with EAP", draft-torvinen-http-eap-00.txt, June 2001, work in progress.

28. J. Linn. "Generic Security Service Application Program Interface Version 2, Update 1". RFC 2743, IETF. January 2000.

29. J. Arkko, H. Haverinen. "EAP AKA Authentication", draft-arkko-pppext-eap-aka-00.txt, May 2001, work in progress, May 2001.

30. S. Parameswar, B. Stucker. "The SIP NEGOTIATE Method", draft-spbs-sip-negotiate-00.txt, September 2001, work in progress,.

31. D. Kroeselberg. "SIP security requirements from 3G wireless networks", draft-kroeselberg-sip-3g-security-req-00.txt, January 2001, work in progress.

32. D. Harkins, D. Carrel: "The Internet Key Exchange (IKE)", RFC 2409, November 1998.

33. Srinivas, Chan, Sengodan, Costa-Requena: "Mapping of Basic and Digest Authentication to DIAMETER AAA Messages", draft-srinivas-aaa-basic-digest-00.txt, July 2001, work in progress.

34. B. Sterman: "Digest Authentication in SIP using RADIUS", draft-sterman-sip-radius-00.txt, February 2001, work in progress.

35. P.R. Calhoun, W. Bulley, A.C. Rubens, J. Haag, G. Zorn: "Diameter NASREQ Application", draft-ietf-aaa-diameter-nasreq-07.txt, July 2001, work in progress.

36. H. Schulzrinne: "Universal Emergency Address for SIP-based Internet Telephony", draft-schulzrinne-sipping-sos-00.txt, July 2001, work in progress.

37. A. Johnston, S. Donovan, R. Sparks, C. Cunningham, D. Willis, J. Rosenberg, K. Summers, H. Schulzrinne: "SIP Call Flow Examples", draft-ietf-sip-call-flows-05.txt, June 2001, work in progress.

38. A. Johnston, R. Sparks, C. Cunningham, S. Donovan, K. Summers: "SIP Service Examples", draft-ietf-sip-service-examples-02.txt, June 2001, work in progress.

39. R. Shirey: "Internet Security Glossary", RFC 2828, May 2000.

40. H. Sugano, S. Fujimoto, G. Klyne, A. Bateman: "CPIM Presence Information Data Format", draft-ietf-impp-cpim-pidf-01.txt, October 2001, work in progress.

11. Changes from previous versions

11.1 Changes from version -00

- Reference section is updated.
- Added new section 6.21.2 on DTMF signaling.
- Added new section 6.23.5 on Network initiated re-authentication.
- Section 6.13.1 clarifies that the Cell-ID is not sent beyond the network of the originating serving proxy.
- Section 6.4.2 is rewritten to clarify the need for the requirement.

- Section 6.9 says that the requirement is only partly covered by [9], as this document only covers the media aspects of a denial of service, but not the signaling aspects.
- Sections 6.10.2.2 and 6.10.2.3 are clarified.
- Sections 6.14 are 6.15 are rewritten in the sake of clarity.

11.2 Changes from version -01

This version is an effort to clarify many of the requirements.

- Among others, section 6.2.3, 6.3, 6.3.1, 6.3.2, 6.3.3, 6.3.4, 6.14.1, 6.15.4, 6.16.1, 6.21, 6.22, 6.23.2.1, 6.23.2.2 and 6.23.6 have been modified or re-written.
- Old section 6.4.5, network initiated de-registration (application layer determined) has been removed.
- Added a couple of new charging related requirements under sections 6.18.1 and 6.18.2.
- Added a requirement for Early Media in section 6.20.3.

Full Copyright Statement