
-----Original Message-----
From: Jari Arkko [mailto:Jari.Arkko@LMF.ERICSSON.SE]
Sent: 10 September 2001 16:43
To: 3GPP_TSG_SA_WG3@LIST.ETSI.FR
Subject: IMS requirements on SIP for IETF

Dear SA3,

Please find attached a preliminary version of an Internet Draft Ericsson has posted to the CN1 mailing lists today (see the e-mail below), together with some other participating companies. This is a requirements draft, targeted towards IETF from 3GPP, and includes requirements for the SIP protocol.

The matter is relevant for SA3 because the draft contains also security requirements, and because we need to get our security solutions agreed with the IETF. The draft contains a security requirements section which we have written based on SA3's documents as well as an earlier Internet Draft by Dirk Kroeselberg from Siemens.

The security sections are an Ericsson's initial attempt at the requirements; they have not come from CN1 nor agreed there. We solicit input from SA3 to help ensure we send the right requirements to IETF.

We would like to discuss further the requirements under agenda point 5.2 in the IMS Ad Hoc meeting in Sophia. By Friday we should also have presentation materials that show better the requirements and their relationship to existing SA3 documents.

Jari Arkko
Ericsson

-----Original Message-----
From: Miguel A. Garcia [mailto:Miguel.A.Garcia@ericsson.com]
Sent: 10 September 2001 14:21
To: 3GPP_TSG_CN_WG1
Subject: 3GPP requirements to IETF SIPPING

Hello All,

Please find enclosed a start to an internet draft trying to capture the 3GPP requirements on SIP. This has tried to take into account the relevant comments provided during the email discussions provoked by N1-011242.

Ericsson feels that this internet draft should focus on the requirements which 3GPP is placing on the application of SIP. According to some comments that I have got, we should point to possible solutions when there is common agreement that such solution exists, however, we should keep focus on the requirements level. I feel that this should reflect the common view of 3GPP.

Feedback welcome and appreciated - and please indicate whether you would like to have your name included as a co-author, in case you are not.

My suggestion on how to progress this work from now on: - Start a one week e-mail discussion, preferably focusing on general aspects, rather than minor wording.
- Perhaps, if needed, we can setup a conference call next week to inspect all the details.
- Circulate the document to other relevant 3GPP WG (e.g., SA3, perhaps SA2).

Best Regards,

Miguel Garcia
--
Miguel-Angel Garcia
mailto:Miguel.A.Garcia@ericsson.com
mailto:Miguel.A.Garcia@piuha.net

Oy LM Ericsson AB
Jorvas, Finland
Phone: +358 9 299 3553
Mobile: +358 40 5140002

:PPING Working Group
ıternet Draft
ocument: <draft-garcia-sipping-3gpp-reqs-00.txt>

M. Garcia / Ericsson
D. Mills / Vodafone
G. Bajko / Nokia
G. Mayer / Siemens
F. Derome / Alcatel
H. Shieh / AWS
A. Allen / Motorola

September, 2001

3GPP requirements on SIP

atus of this Memo

Abstract

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

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 specific requirements to operate in a cellular network.

In this document we express the requirements identified by 3GPP to support SIP for IMS in cellular networks.

Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC-2119 [2].

Table of Contents

Introduction

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

While SIP offers an attractive set of mechanisms to initiate multimedia sessions, it has not taken into account the interaction with other protocols, nor does it consider the requirements derived from the operation of SIP in cellular network.

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.

The rest of this document is structured as follows:

Section 5 offers an overview of the 3GPP IP Multimedia 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. After each requirement, there is 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.

Overview of the 3GPP IP Multimedia Subsystem

This section gives the reader an overview of the 3GPP IP Multimedia Subsystem. 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 [4], [5] and [6].

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 serving SIP 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 proxy server to support the terminal. The SIP proxy server 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.

3GPP cellular IP Multimedia terminals use the existing General Packet Radio Service (GPRS) [6] as a transport network for IP datagrams. The terminals first attach to the GPRS network to get an IPv6 address. This procedure is required to be completed before any IP Multimedia session can be established.

As a result of the GPRS attach, the terminal has got an IPv6 address. The address belongs to the GPRS access address space and it does not change as the mobile terminal moves while still attached to the same GPRS address space.

If the terminal moves from a GPRS access to another GPRS access, the GPRS attach procedure needs to start from the beginning to allocate an IPv6 address to the terminal.

Figure 1 shows an overview of the 3GPP architecture for IMS.

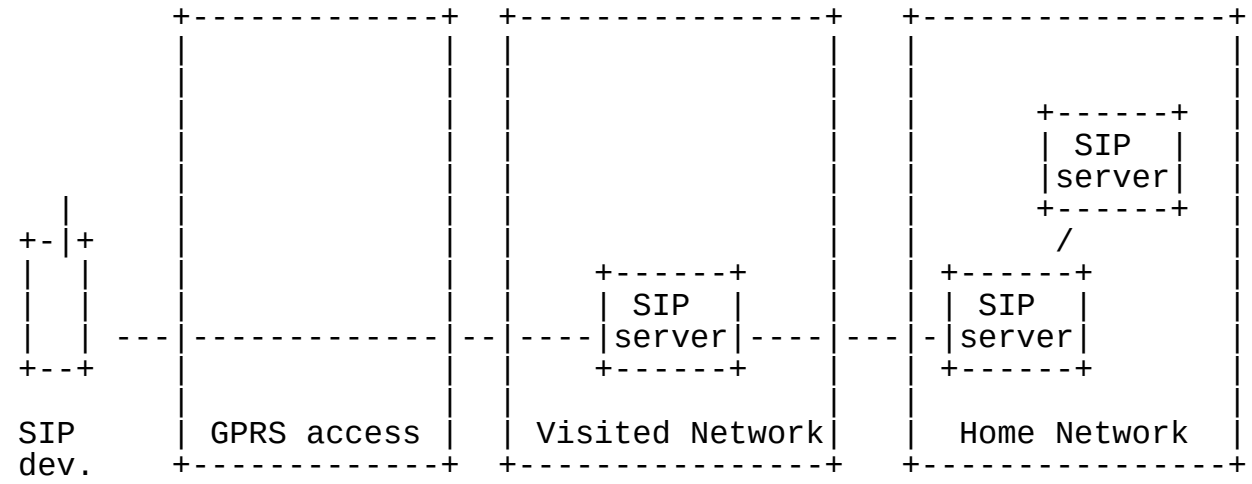

Figure 1: Overview of the 3GPP SIP architecture

3GPP Requirements on SIP

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 air interface

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

6.1.2 Minimum session setup time

All the procedures and mechanisms developed by the IETF MUST have a minimum impact on the session setup time. Therefore, procedures that can be used before the session establishment MUST be used before session establishment.

6.1.3 Minimum support required in the terminal

As terminals could be rather small devices, memory requirements, power consumption, processing power, etc. MUST be kept to a minimum. Particularly, support for protocols other than SIP, SDP, and RTP must be carefully considered before mandating them.

2 Outbound SIP proxy server in the visited network

6.2.1 Outbound SIP proxy server in the visited network

An outbound SIP proxy server in the visited network MUST be supported in both roaming and non-roaming case, even when the home SIP proxy is located in the same network.

6.2.2 Discovery of the outbound SIP proxy server

GPRS provides 3GPP SIP terminals with mechanisms to discover the address of the outbound proxy server located in the visited network.

One such mechanism is that the address of the outbound SIP proxy server in the visited network is transported in the GPRS attach procedure signaling.

However, there MUST be a general mechanism developed by the IETF to configure the terminal with the address of the outbound SIP proxy server 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 not support for IPv6 in this Internet Draft.

6.2.3 Reassigning the outbound SIP proxy server

Reassigning the outbound SIP proxy server assigned during the discovery procedures is NOT REQUIRED. Procedures to allow registration time outbound SIP proxy server reassignment MAY be considered in the future.

6.2.4 Removal of headers

The outbout SIP proxy server 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. This increases security and reduces SIP message sizes and thus transmission delay over the air interface.

3 Registration

6.3.1 Registration to the access network

Registration to the access network (e.g. GPRS) MUST be done independently and before the SIP application registration procedure is executed.

6.3.2 Registration required

A user MUST register to the IMS before he/she can initiate or terminate any session. The rational behind is that the user must be authenticated and billed for the resources that he/she will use. 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 SIP registrar is located in the Home network. The SIP registrar authenticates and registers the user.

Once the terminal is switched on, it read its configuration data. This data may be stored in a SIM card or any other memory device. The configuration data contains the domain name of the home network. The device MUST find the SIP registrar address from the home network domain name.

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 servers are typically stateless SIP proxy servers. Their mission is to serve as a first point of contact in the home network, hide network configuration (if needed) 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 air interface resource, a single registration MUST be used to register both in the visited and in the home network.

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

6.3.4 Registration for roaming and non roaming cases

It is desirable that the UA will use the same registration procedure(s) within its 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. Therefore, there MUST be a mechanism so that the visited domain name is known at registration time in the home network.

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 or possibly when he movess.

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

6.4.2 Types of network initiated de-registrations

Two types of network initiated de-registrations are REQUIRED:

- To deal with registrations expirations
- To allow the network to force de-registrations following any of possible causes for this to occur.

6.4.3 Network initiated de-registration, network maintenance

The IMS 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. Cancelling 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 duplicate registrations or inconsistent information storage. This case will occur when a subscriber roams to a different network without de-registering the previous one. This case may occur at the change of the roaming agreement parameters between two operators, imposing new service conditions to roamers.

6.4.5 Netork initiated de-registration, application layer determined

The service capability offered by the system to the application aayers may have parameters specifying whether all SIP registrations are to be removed, or only those from one or a group of terminals from the user, etc.

6.4.6 Network initiated de-registration, subscription management

The operator MUST be able to restrict user access to the system upon detection of contract expiration, removal of subscription, fraud detection, etc.

6.4. 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 terminal.

We believe that a procedure based on SIP events [15] and a registration package will meet the requirement.

5 Compression of SIP signaling

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

Therefore, there MUST be a mechanism to efficiently transport of SIP signaling packets over the radio interface, typically by compressing the SIP signaling messages 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 shall 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. This is to facilitate devices like a laptop to be able to the IMS when the needed compression algorithms may not be available to the UA in the laptop.

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 outbound SIP 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 outbound SIP Proxy responds with the selected one. Subsequent SIP messages are compressed based on the agreed algorithm.

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 (radio) bearer establishment be successfully allocated before the destination user is alerted. Note, however, that it MUST be also possible for an 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 (radio) 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].

7 Prevention of theft of service

The possibility for theft of service in the 3GPP IP Multimedia 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].

8 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 by the procedures described in [9].

9 Identification of users

6.9.1 Private user identity

Every 3GPP IMS subscriber MUST have a private user identity. The private identity is assigned by the home network operator, and used, for example, for Registration, Authorisation, Administration, and may be 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 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.

6.9.1.1 Private user ID in registrations

The private user identity MUST be contained in all REGISTER messages passed from the UA to the registrar in the home network.

6.9.1.2 Authentication of the private user ID

The private user identity is authenticated only during registration of the subscriber, (including re-registration and de-registration).

6.9.2 Public user identities

Every 3GPP IMS 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.

6.9.2.1 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 fulfil the requirement.

6.9.2.2 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 via a mechanism within the IP multimedia subsystem. This MUST NOT preclude the user from registering individually some of his/her public identities if needed.

6.9.2.3 Authentication of the public user ID

Public user identities are not authenticated by the network during registration.

10 Identifiers used for routing

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

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

11 Hiding requirements

6.11.1 Hiding of the network structure

A network operator MUST 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 SIP proxies, name of the SIP proxies, capabilities of the SIP proxies or capacity of the netowrk. Association of the node names of the same type of entity and their capabilities and the number of nodes will be kept within an operator’s network. However disclosure of the internal architecture MUST NOT be prevented on a per agreement basis.

6.11.2 Hiding of IP addresses

A network MUST NOT be required to expose the explicit IP addresses of the nodes within the network (excluding firewalls and border gateways).

6.11.3 Hiding proxy

In order to support the hiding requirements, a 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.

12 Cell-ID

The 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 6.12).

6.12.1 Cell-ID in signaling from the UA to the home

Assuming that the cell-ID is received by the SIP application by other mechanisms beyond SIP control, the cell-ID MUST be transported in all the messages that the application sends to the serving SIP proxy in the home network.

6.12.2 Format of the cell-ID

The cell-ID MUST be sent in the format of a Cell Global ID, as described in [22].

13 Release of sessions

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).

6.13.1 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 serving SIP proxy at home) is involved in a session, memory leaks and eventually server failure can occur due to hanging state machines. To ensure stable proxy operation and carrier grade service, a mechanism to handle the ungraceful session termination issue is REQUIRED. This mechanism should be at the SIP protocol level in order to guarantee access independence for the system.

6.13.2 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 UE 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.

14 Routing of SIP messages

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

6.14.1 Outbound proxy in the visited network

As the outbound proxy in the visited network is supporting the terminal in terms of dialed digits translation (e.g., local to international), emergency calls, etc, all sessions initiated in the mobile terminal when using IMS, MUST be first routed to the outbound SIP proxy server in the visited network, independently of the destination of the session.

6.14.2 Serving SIP proxy server in the home network

As services are triggered in the home network, all sessions initiated in the mobile terminal MUST be routed to the allocated serving SIP proxy server in the home network, independently of the destination of the session.

6.14.3 INVITE might follow a different path than REGISTER

The path taken by the INVITE MUST NOT be restricted to specific congruence with the path taken by the REGISTER. However, the path taken by the INVITE MAY follow the same path taken by the REGISTER.

6.14.4 Information of the vector

There MUST be some means of dynamically informing the node which adds the vector of what that vector should be, in the specific case where the vector is used to find a home proxy in the home network.

6.14.5 Hiding

It MUST be possible for operators to hide their network configuration (names, number of nodes) between the different proxies that conform the vector. This is connected with hiding requirements expressed in section 6.11.

In order to fulfil this requirements, 3GPP networks may deploy a hiding SIP proxy server to hide configurations between different networks.

6.14.6 Roaming and non roaming

The developed solution SHOULD work efficiently in roaming and non-roaming scenarios.

6.14.7 Inbound proxy in the visited network

The visited network may apply certain local policies to incoming sessions. Therefore, there is a need to have an inbound proxy in the visited network for terminating sessions. In general, the inbound

proxy and the outbound proxy are the same entity in the visited network.

15 Emergency sessions

It MUST be possible to place an emergency session using the SIP based multimedia system.

6.15.1 Registration is not required

It MUST be possible to place an emergency session using SIP, independently on whether the user is registered to the IMS or not.

6.15.2 Outbound proxy support

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

6.15.2 Cell Global ID in emergency sessions

It is REQUIRED that location information including Cell Global ID (see also requirement 6.12) 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.

16 Remote Party Identification and anonimity

6.16.1 Remote Party Identification presentation

It MUST be possible to present to the caller the identity of the party to which he/she is connected.

We believe this requirement is met by the procedures described in [16].

6.16.2 Remote Party Identification privacy

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

We believe this requirement is met by the procedures described in [16].

6.16.3 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 subcriber’s home 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].

6.16.4 Anonimity

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

6.16.4.1 Anonymous session establishment

If the caller 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 callee MUST not reveal any identity or signalling routing information to the destination endpoint. The terminating network should distinguish at least two cases, first where the caller intended the session to be anonymous, and second where the caller’s identity was deleted by a transit network.

17 Charging

6.17.1 Types of charging

Depending on regulatory requirements, there are two different models to charge the user of the IP Multimedia service. It MUST be possible to apply charging according to any of the following models:

1. The caller pays for the access IP-connectivity service of both originating and destination side,

2. The callee pays for the access IP-connectivity service of both originating and terminating side.

6.17.2 Synchronization with session control

The session control and bearer control mechanisms MUST allow the session control to decide when user plane traffic between end-points of a SIP session may start/shall stop. This allows this traffic to start/stop in synchronisation with the start/stop of charging for a session.

18 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.

19 Session transfer

Procedures are REQUIRED for performing session transfers. A basic primitive is needed that can be used by endpoints to cause a multi-media session to be transferred.

We believe that the REFER method [18], the Call Transfer procedures [19] and the Replaces header [20] meet this requirement.

6.19.1 Blind transfer

A blind transfer starts with an existing session, established between the initiator and the recipient. In a typical case, this session was actually initiated by the recipient. The initiator refers to the transfer target. In the end it is desired that the recipient has a session with the target.

Blind transfer MUST be supported.

6.19.2 Assured transfer

An assured transfer is identical to the above, except that the initiator waits until the REFER successfully completes before issuing the BYE message to terminate its connection with the recipient. If the new session from the recipient to the target were to fail, the recipient would still have a session with the initiator.

Assured transfer MUST be supported.

6.19.3 Consultative tranfer

A consultative transfer starts with an existing session, established from the Initiator to the Recipient. The initiator first consults with the garget, then decides to transfer the original session to the target.

Consultative transfer MUST be supported.

6.19.4 Three-way session

A three-way session starts with an existing session, between the initiator and a second party. The initiator places this session on hold, and establishes a second session with a third party. The initiator then decides to create an ad-hoc conference of all three parties.

Three-way session MUST be supported.

20 Security Model

Sections 6.20, 6.21 and 6.22 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 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 first version of the IMS.

It is expected that security for the underlying GPRS network and the IMS will 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 IMS services securely from other accesses than GPRS and UMTS.

Each operator providing IMS services acts as its own domain of trust, and shares a long-term security association with its subscribers. 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. The current working assumption in the 3GPP is to perform authentication during registration.

A hop-by-hop model MUST be used to protect actual SIP signaling. Looking at Figure 1 in Chapter 5, we can distinguish two main areas where security is needed:

- 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. For instance, bandwidth conservation and the ability to use low-cost equipment are of high importance in the Access Domain. It is therefore required that the security solutions MUST allow different mechanisms in these two domains.

21 Access Domain Security

6.21.1 Authentication

Strong, mutual authentication method MUST be used.

Authentication using legacy authentication methods MUST be provided.

Authentication methods MUST support the secure storage of long-term authentication keys.

Current HTTP authentication methods do not provide either strong or mutual authentication. Lower layer mechanisms allow strong and mutual authentication (but may not fulfill other requirements). 3GPP intends to reuse UMTS AKA [24], but would prefer to have other legacy mechanisms to be possible as well. UMTS AKA applies a symmetric cryptographic scheme, provides mutual authentication, and is typically implemented on a so-called SIM card that provides secure storage.

6.21.2 Scalability and Efficiency

3GPP IP Multimedia Networks 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.

6.21.2.1 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 MUST minimize the number of necessary extra roundtrips. In particular, during normal call signaling there SHOULD NOT be any additional security related messages.

The roundtrip requirements are particularly hard to satisfy. It appears that security solutions running at a lower layer such as TLS [25] or IPSec/IKE [26] make a substantial increase to the number of necessary roundtrips during the initial stages the cellular devices contact the IMS.

6.21.2.2 Computation

It MUST be possible for IMS terminals to provide security without 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 might not meet other requirements). Lower-layer security mechanisms all appear to use public key cryptography, or at least Diffie-Hellman as a mandatory part in their operation. HTTP EAP [27] is one 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, EAP already supports UMTS AKA [29].

6.21.2.3 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, followed by subsequent protected signaling that uses only session keys. The used authentication mechanisms MUST be able to provide also session keys. Initial authentication is performed between SIP client and the authenticating SIP proxy or server. However, the authentication mechanism MUST NOT require the storage of authentication credentials such as passwords in these nodes, and there MUST be a way to access these credentials remotely from dedicated authentication servers.

Additionally, the SIP entity that performed the initial authentication MUST be able to delegate subsequent SIP signaling protection to an authorized SIP proxy further downstream.

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 currently also no proposals to allow delegation of signaling protection tasks.

6.21.3 Secure negotiation of mechanisms

The so-called security mode set-up procedure 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 security mode set-up is handled within a security service. For example, HTTP authentication scheme includes negotiation mechanism for choosing among appropriate authentication methods and algorithms.

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 one registration.

It MUST be possible to choose among several security services, and select parameters they might need. For example, it should be possible for a user agent and a proxy to decide that they use a particular integrity protection mechanism, and a particular algorithm within that mechanism.

It MUST be possible to protect the service and parameter negotiation against attackers. In particular, it MUST NOT be possible for man-in-the-middle attackers to change the proposed services to ones with lower or no security.

Existing lower-layer security mechanisms provide the above functionality as a part of them. We do not currently know of any mechanism that would allow this also at the SIP layer, [30] might perhaps be extended to perform secure negotiation.

6.21.4 Message protection

SIP entities (typically a SIP client and a SIP proxy) MUST be able to communicate using integrity and replay protection. This protection MUST be based on initial authentication. Integrity protection MUST be possible using symmetric cryptographic keys.

It MUST be possible to handle also error conditions, SIP entity crashes, and other special situations in a satisfactory manner as to allow recovery.

It MUST be possible to provide this protection between two adjacent SIP entities. It SHOULD be possible to provide this protection also through proxies.

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.

22 Network Domain Security

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

Establishing security pair-wise between all SIP proxies is likely to be unscalable. The security associations MUST be independent of the number of network elements.

The 3GPP intends to make it mandatory to have 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 current IP Security standards [26].

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
Email: CAA019@motorola.com

References

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

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

3. Handley M, Schulzrinne H, Schooler E, Rosenberg J., "SIP, Session Initiation Protocol", draft-ietf-sip-rfc2543bis-04.txt, 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 1.2.0 is available at ftp://ftp.3gpp.org/Specs/Latest_drafts/24228-120.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, Work in progress.

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

9. W. Marshall et al. "SIP Extensions for Media Authorization", draft-ietf-sip-call-auth-02.txt, 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 telcommunication 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-00.txt, Work in progress.

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

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

18. R. Sparks: "The REFER method", draft-ietf-sip-refer-01.txt, Work in progress.

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

20. Biggs, B. and R. Dean, "The SIP Replaces Header", draft-sip-replaces-00.txt, Work in progress.

21. J.Rosenberg, H.Schulzrinne: "Reliability of Provisional Responses in SIP", draft-ietf-sip-100rel-03.txt, 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://www.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, Work In Progress, June 2001.

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, Work In Progress, May 2001.

30. S. Parameswar, B. Stucker. "The SIP NEGOTIATE Method", draft-spbs-sip-negotiate-00.txt, Work In Progress, IETF, September 2001.

31. D. Kroeselberg. "SIP security requirements from 3G wireless networks", draft-kroeselberg-sip-3g-security-req-00.txt. Work In Progress, IETF, January 2001.

ll Copyright Statement