SIPPING Working Group
Internet-Draft
Intended status: Standards Track
Expires: June 8, 2007

M. Garcia-Martin
Nokia
G. Camarillo
Ericsson
December 5, 2006

Extensible Markup Language (XML) Format Extension for Representing Copy Control Attributes in Resource Lists

draft-ietf-sipping-capacity-attribute-03.txt

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

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.

This Internet-Draft will expire on June 8, 2007.

Copyright Notice

Copyright (C) The IETF Trust (2006).

Abstract

In certain types of multimedia communications, a Session Initiation Protocol (SIP) request is distributed to a group of SIP User Agents (UAs). The sender sends a single SIP request to a server which further distributes the request to the group. This SIP request contains a list of Uniform Resource Identifiers (URIs), which identify the recipients of the SIP request. This URI-list is

expressed as a resource list XML document. This specification defines an XML extension to the XML resource list format that allows the sender of the request to qualify a recipient with a copy control level similar to the copy control level of existing e-mail systems.

Table of Contents

1. Introduction 3
2. Terminology 3
3. Overview of operation 4
4. Extension to the resource lists data format 6
5. XML Schema 8
6. Examples 8
7. Carrying URI-lists in SIP 10
8. Security Considerations 11
9. IANA Considerations 12
9.1. Disposition Type Registration 12
9.2. XML Namespace Registration 12
9.3. XML Schema Registration 13
10. Acknowledgements 13
11. References 14
11.1. Normative References 14
11.2. Informational References 14
Authors' Addresses 15
Intellectual Property and Copyright Statements 16

1. Introduction

The Framework and Security Considerations for Session Initiation Protocol (SIP) URI-List Services [9] describes a generic framework for carrying Uniform Resource Identifier (URI)-lists in SIP [5] messages. Specifically, the document provides a common framework for specific implementations of URI-list services, such as conferences initiated with INVITE requests [10] or Multiple-recipient MESSAGE requests [11].

Common to all URI-list services is the presence of a SIP request that contains a collection of resources, typically expressed as an XML resource list [7]. SIP requests carrying resource lists can appear either in requests received by the URI-list server, indicating the list of intended recipients, or in each of the requests that the URI-list server sends to recipients, indicating the list of recipients of the same SIP request.

Although the XML resource list [7] provides a powerful mechanism for describing a list of resources, there is a need for a copy control attribute to determine whether a resource is receiving a SIP request as a primary recipient, a carbon copy, or a blind carbon copy. This is similar to common e-mail systems, where the sender can categorize each recipient as To, Cc, or Bcc recipient.

This document addresses this problem by providing an extension to the XML resource list [7] that enables the sender to supply a copy control attribute that labels each recipient as a "to", "cc", or "bcc" recipient. This attribute indicates whether the recipient is receiving a primary copy of the SIP request, a carbon copy, or a blind carbon copy. Additionally, we provide the sender with the capability of indicating in the URI-list that one or more resources should be anonymized, so that some recipients' URIs are not disclosed to the other recipients. Instead, these URIs are replaced with anonymous URIs.

The remainder of this document is organized as follows: Section 2 introduces the terminology used throughout this specification. Section 3 gives an overview of operation. Section 4 formally defines an extension to URI-lists. The XML schema definition is provided in Section 5. Section 6 shows examples of the URI-lists with the extensions defined in this document. Section 7 discusses the implications of carrying URI-lists in SIP messages.

2. Terminology

In this document, the key words "MUST", "MUST NOT", "REQUIRED",

"SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" are to be interpreted as described in BCP 14, RFC 2119 [1] and indicate requirement levels for compliant implementations.

URI-list service: SIP application service that receives a SIP request containing a URI-list and sends a similar SIP request to each URI in the list.

Intended recipient: The intended final recipient of the request to be generated by URI-list service.

Copy control: An attribute assigned by the sender to a URI in a XML resource list. Its purpose is to indicate to the recipient whether he is getting a primary, carbon, or blind carbon copy of the SIP request.

Recipient list or recipient XML resource list: An XML resource list containing the list of intended recipients. The sender sets this list in the SIP request he sends to the URI-list server.

Recipient-history list or recipient-history XML resource list: An XML resource list containing the visible list of recipients (i.e., those non-anonymous non-bcc). The URI-list server creates this list, based on the recipient list, and includes it in each of the SIP requests it sends to each recipient.

3. Overview of operation

Figure 1 depicts a general overview of the operation of a URI-list server. A SIP User Agent Client (UAC) issuer sends a SIP request (F1) to a URI-list server containing a recipient list. The URI-list server generates a SIP request to each recipient, according to the specific SIP method. Each of these SIP requests contains a recipient-history list that indicates the visible list of recipients of the SIP request.

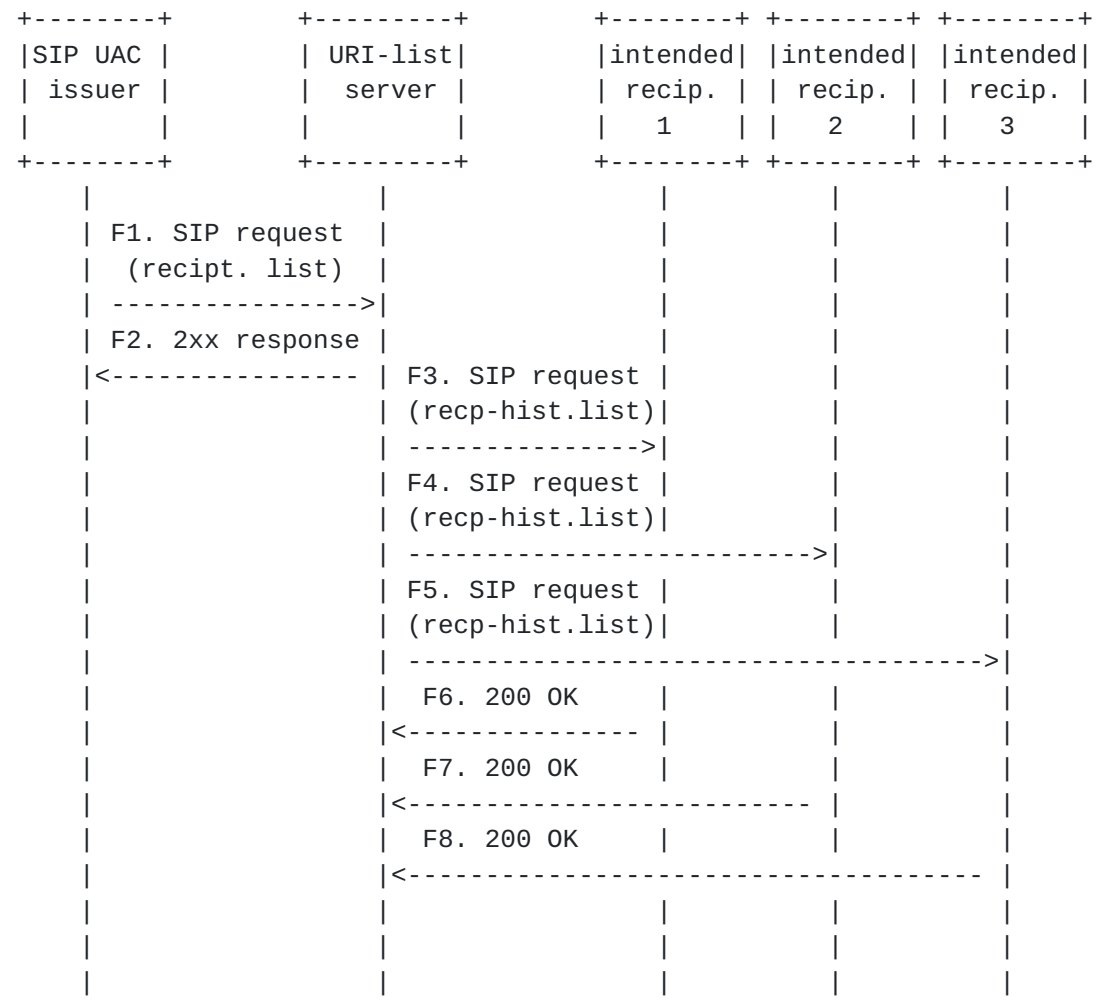


Figure 1: Example of operation

The URI-list mechanism allows a sender to specify multiple targets for a SIP request by including a recipient XML resource list [7] in the body of the SIP request. This recipient list includes the target URIs of the SIP request (the actual procedures are method specific and outside the scope of this document). Each target URI may also be marked with a copy control attribute to indicate the copy level in which the recipient is receiving the SIP request. This is achieved by the sender qualifying each URI in the URI-list with a 'copyControl' attribute. The available values of the 'copyControl' attribute include "to", "cc", and "bcc" (analogous to e-mail). This is discussed in greater detailed in Section 4. When the URI-list server expands the request to each recipient, the URI-list server includes a recipient-history XML resource list built upon the recipient list received from the sender. The recipient-history XML resource list replaces the recipient list in the SIP requests generated by the URI-list server towards each recipient. The URI-list server copies from the recipient list those targets which are

marked with the "to" and "cc" copy control level, and pastes them in the recipient-history list. The URI-list server explicitly excludes from the copy those URIs marked with a "bcc" copy control. When a recipient receives the SIP request containing the recipient-history XML resource list, he is able to determine which other visible recipients are getting the same SIP requests, and whether they are marked with the "to" or "cc" copy control level. Later, if needed, the recipient can generate a reply to those visible recipients.

In addition to the 'copyControl' attribute for a URI in an XML resource list, we define a second boolean attribute called 'anonymize'. The sender of a SIP request can mark a URI in a recipient XML resource list with the 'anonymize' attribute to indicate the URI-list server that the URI marked with that attribute is to be replaced with an anonymous URI in the recipient-history XML resource list. This provides a knowledge to recipients of a SIP request of a number of additional recipients whose URIs have not been disclosed.

There are cases when the sender marks several URIs with the 'anonymize' attribute. The URI-list server can group the anonymized URIs in a single anonymized URI within its copy control level, and provide a count of the number of anonymized URIs. To support this scenario, we define a new 'count' attribute to a URI in the recipient-history XML resource list. It is expected that the 'count' attribute is only used with anonymous URIs, although syntactically it is possible to add a 'count' attribute to any URI in any XML resource list.

Initially, it may be thought that the 'anonymize' attribute overlaps with the "bcc" value of the 'copyControl' attribute. However, there are differences between them. If the sender qualifies a URI with a 'copyControl' attribute of "bcc" in the recipient XML resource list, the URI-list server will completely remove that URI from the recipient-history XML resource list. Recipients of the SIP request will not notice that one or more extra URIs also received the request. However, if the sender qualifies a URI with the 'anonymize' attribute in the recipient XML resource list, the URI-list server will replace the URI with an anonymous one in the recipient-history list. Recipients of the SIP request will notice that there have been one or more additional recipients of the same request, but their URIs have not been disclosed.

4. Extension to the resource lists data format

This document defines an extension to the XML resource list data format [7] that allows the sender to indicate a copy control

attribute that qualifies a recipient with a copy control level. We define a new 'copyControl' attribute to the <entry> element of the resource list document format [7]. The 'copyControl' attribute has similar semantics to the type of destination address in e-mail systems. It can take the values "to", "cc", and "bcc". A "to" value of the 'copyControl' attribute indicates that the resource is considered a primary recipient of the SIP request. A "cc" value indicates that the resource receives a carbon copy of the SIP request. A "bcc" value indicates that the resource receives a blind carbon copy of the SIP request (i.e., this URI is not disclosed in the recipient-history list). The default 'copyControl' value is "bcc". That is, the absence of a 'copyControl' attribute MUST be treated as if the 'copyControl' was set to "bcc". URI-list servers use URIs marked with the "bcc" 'copyControl' attribute to route SIP requests, but MUST NOT include them in recipient-history lists.

A new 'anonymize' attribute can be included in a <entry> element of the resource list document format [7]. If set to a "true" value, it provides an indication to the URI-list server for not disclosing the URI itself in a URI-list sent to the recipient, but instead, to anonymize the URI (i.e., making it bogus in the recipient-history XML resource list). URI-list servers can use URIs tagged with the 'anonymize' attribute for routing SIP requests, but MUST convert them to an anonymized URI (such as sip:anonymous@anonymous.invalid) in recipient-history lists. The default value of the 'anonymize' attribute is "false".

Processing of URIs tagged with a 'copyControl' attribute set to a "bcc" value has higher precedence over the 'anonymize' attribute. Thus, if the 'copyControl' of a URI is set to "bcc", the URI-list server MUST remove that URI from the recipient-history list, and the 'anonymize' attribute will be ignored. Therefore, the 'anonymize' attribute is only useful for those URIs tagged with a 'copyControl' of "to" or "cc".

A new 'count' attribute can be also included in a <entry> element of the resource list document format [7]. It provides the number of equal URIs. Typically, recipient lists created by UACs will not have equal (or duplicate) URI entries, thus, it is not expected to contain URIs tagged with 'count' attributes. However, recipient-history lists can contain duplicated anonymized URIs, therefore, it is expected that recipient-history lists will contain 'count' attributes. The default value of the 'count' attribute is "1".

The 'copyControl', 'anonymize', and 'count' attributes SHOULD be included as modifiers of any of the child elements included in the <list> element of a resource list (e.g., attribute of the <entry> or <external> elements).

Section 5 describes the format of the 'copyControl', 'anonymize', and 'count' attributes. Implementations according to this specification MUST support this XML Schema.

5. XML Schema

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema targetNamespace="urn:ietf:params:xml:ns:copycontrol"
    xmlns="urn:ietf:params:xml:ns:copycontrol"
    xmlns:rls="urn:ietf:params:xml:ns:resource-lists"
    xmlns:xs="http://www.w3.org/2001/XMLSchema"
    elementFormDefault="qualified"
    attributeFormDefault="unqualified">

    <xs:annotation>
      <xs:documentation xml:lang="en">
         Adds the copyControl, anonymize, and count attributes
         to URIs included in a resource list.
      </xs:documentation>
    </xs:annotation>

   <xs:import namespace="urn:ietf:params:xml:ns:resource-lists"
          schemaLocation="urn:ietf:params:xml:schema:resource-lists"/>

    <xs:attribute name="copyControl">
       <xs:simpleType>
          <xs:restriction base="xs:string">
             <xs:enumeration value="to"/>
             <xs:enumeration value="cc"/>
             <xs:enumeration value="bcc"/>
          </xs:restriction>
       </xs:simpleType>
    </xs:attribute>

   <xs:attribute name="anonymize" type="xs:boolean" default="false"/>
   <xs:attribute name="count" type="xs:nonNegativeInteger"
                              default="1"/>

</xs:schema>
```

Figure 2: XML Schema of the extension to the resource list format

6. Examples

This section shows two examples of URI-lists that can be included in SIP requests. The first example in Figure 3 shows a recipient list

that the UAC sends to the URI-list server. This corresponds to a list that will be included in the flow F2 in Figure 1. The recipient list contains a flat list according to the resource list data format [7]. Each resource indicates the copy control of a resource with a 'copyControl' attribute. Some of the resources are also marked with the 'anonymize' attribute. This provides an indication to the URI-list service for not disclosing their URIs in a recipient-history list. The last two <entry> elements are marked with a 'copyControl' attribute of "bcc". This provides an indication to the URI-list server for removing these URIs in the recipient-history list.

```
<?xml version="1.0" encoding="UTF-8"?>
<resource-lists xmlns="urn:ietf:params:xml:ns:resource-lists"
          xmlns:cp="urn:ietf:params:xml:ns:copycontrol">
  <list>
    <entry uri="sip:bill@example.com" cp:copyControl="to" />
    <entry uri="sip:randy@example.net" cp:copyControl="to"
                                        cp:anonymize="true"/>
    <entry uri="sip:eddy@example.com" cp:copyControl="to"
                                       cp:anonymize="true"/>
    <entry uri="sip:joe@example.org" cp:copyControl="cc" />
    <entry uri="sip:carol@example.net" cp:copyControl="cc"
                                        cp:anonymize="true"/>
    <entry uri="sip:ted@example.net" cp:copyControl="bcc" />
    <entry uri="sip:andy@example.com" cp:copyControl="bcc" />
  </list>
</resource-lists>
```

Figure 3: Recipient list sent from the UAC to the URI-list server

Upon receipt of the SIP request containing the recipient list of Figure 3 the URI-list server creates a SIP request to each of the URIs listed in the recipient list (so, in our example, it creates 7 SIP requests). The URI-list server processes the recipient list and creates a recipient-history list that is included in each of the outgoing SIP requests. The process is as follows: the URI-list server creates a new recipient-history list, based on the recipient list, but with changes. First it copies all the URIs (<entry> elements) marked with the "to" or "cc" 'copyControl' attributes, which do not contain an 'anonymize' attribute (or when the 'anonymize' attribute is set to "false"). Then all the URIs marked with a 'copyControl' attribute set to "to" and 'anonymize' attribute set to "true" are replaced with an anonymous URI, such as "sip:anonymous@anonymous.invalid". In this entry the URI-list server also adds the original value of the 'copyControl' attribute ("to" in our example), and it adds a 'count' attribute containing the number of anonymous entries in this group ("2" in our example). Then the URI-list server does the same operation to the URIs tagged with the

'copyControl' attribute set to "cc" and 'anonymize' attribute set to "true", adding also the 'count' attribute containing the number of anonymous attributes in this group ("1" in the example). Last, the URI-list server completely removes URIs marked with the "bcc" 'copyControl' attribute. The resulting recipient-history list is shown in Figure 4.

```
<?xml version="1.0" encoding="UTF-8"?>
<resource-lists xmlns="urn:ietf:params:xml:ns:resource-lists"
          xmlns:cp="urn:ietf:params:xml:ns:copycontrol">
  <list>
    <entry uri="sip:bill@example.com" cp:copyControl="to" />
    <entry uri="sip:anonymous@anonymous.invalid" cp:copyControl="to"
                                                 cp:count="2"/>
    <entry uri="sip:joe@example.org" cp:copyControl="cc" />
    <entry uri="sip:anonymous@anonymous.invalid" cp:copyControl="cc"
                                                 cp:count="1"/>
  </list>
</resource-lists>
```

Figure 4: Recipient-history list sent from the URI-list server to each recipient

7. Carrying URI-lists in SIP

A SIP UAC (User Agent Client) that composes a SIP request can include a URI-list with the extensions specified in this document to indicate the list of intended recipients. On doing so, as specified in the Framework and Security Considerations for SIP URI-List Services [9], the UAC adds a Content-Disposition [2] header field set to the value 'recipient-list'. Typically UACs send these 'recipient-list' bodies to URI-list services (this corresponds to flow F1 in Figure 1). A body whose Content-Disposition type is 'recipient-list' contains a URI-list that includes the intended recipients of the SIP request, something known throughout this document as a recipient list. The <entry> element in the URI-list MAY also include a 'copyControl' and 'anonymize' attributes, as specified in Section 4.

To be able to inform intended recipients of who else is receiving a copy of the SIP request, we define a new mail disposition type to be included in a Content-Disposition [2] header field of a SIP request. The value of this new disposition type is 'recipient-list-history' and its purpose is to indicate a list of recipients that a SIP request was sent to, something known throughout this document as a recipient-history list. A body whose Content-Disposition type is 'recipient-list-history' contains a URI-list with the visible (including anonymized) recipients of the SIP request. The <entry>

element in the URI-list MAY also include a 'copyControl' and 'count' attributes, as specified in Section 4.

On sending a SIP request that contains a recipient-history list, if the intended recipient does not support this specification, the SIP request should not fail. In order to ensure successful receipt of the SIP requests that include 'recipient-list-history' bodies, User Agents (such as URI-list servers) that build SIP requests with the Content-Disposition header field set to 'recipient-list-history' SHOULD add a 'handling' parameter [4] set to "optional". Otherwise, the SIP request could fail and never be received by the intended recipient.

8. Security Considerations

The Framework and Security Considerations for SIP URI-List Services [9] discusses issues related to SIP URI-list services. Implementations of this specification MUST follow the security-related rules in the Framework and Security Considerations for SIP URI-List Services [9]. These rules include mandatory authentication and authorization of clients, and opt-in lists.

User Agent Clients SHOULD NOT hand SIP requests containing URI-list services to unauthenticated and untrusted parties. This is to avoid man-in-the-middle attacks or acquiring URI-lists for performing SPAM attacks.

URI-lists may contain private information, such as SIP URIs. It is therefore not desirable that these URI-lists are known by third parties. Eavesdroppers are able to watch URI-lists contained in SIP requests unless the SIP message is sent over a secured channel, by using any of the available SIP mechanisms, such as Transport Layer Security (TLS) [3], or unless the URI-list body itself is encrypted with, e.g., S/MIME [8]. Therefore, it is RECOMMENDED that URI-list bodies are encrypted with S/MIME [8] or that the SIP request is encrypted with TLS [3] or any other suitable encryption mechanism.

Note that this URI-list does not indicate the actual participants in the session. It indicates only the URIs invited and that might accept the request. It does not assert that these parties actually exist, that they are reachable at the given URI, or that they have accepted the invitation. No inferences about billing should be made from this information. It is subject to spoofing by loading the list with falsified content.

9. IANA Considerations

The following sections instruct the IANA to register: a new disposition type, a new XML namespace, and a new XML schema.

9.1. Disposition Type Registration

Section 7 defines a new 'recipient-list-history' value of the Mail Content Disposition Values registry. This value should be registered in the IANA registry of Mail Content Disposition Values with the following registration data:

Name	Description	Reference
recipient-list-history	the body contains a list of URIs that indicates the recipients of the SIP request	[RFCXXXX]

Table 1: Registration of the 'recipient-list-history' Mail Content Disposition Value

Note to IANA and the RFC editor: replace RFCXXXX above with the RFC number of this specification.

9.2. XML Namespace Registration

This section registers a new XML namespace in the IANA XML registry, as per the guidelines in RFC 3688 [6].

URI: The URI for this namespace is urn:ietf:params:xml:ns:copycontrol

Registrant Contact: IETF, SIPPING working group, (sipping@ietf.org), Miguel Garcia-Martin (miguel.an.garcia@nokia.com).

XML:

```
BEGIN
<?xml version="1.0"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML Basic 1.0//EN"
  "http://www.w3.org/TR/xhtml-basic/xhtml-basic10.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
  <meta http-equiv="content-type"
     content="text/html;charset=iso-8859-1"/>
  <title>Copy Control Namespace</title>
</head>
<body>
  <h1>Namespace for the Copy Control Attribute Extension
  in Resource Lists</h1>
  <h2>urn:ietf:params:xml:ns:copycontrol</h2>
  <p>See <a href="[URL of published RFC]">RFCXXXX
  [NOTE TO IANA/RFC-EDITOR: Please replace XXXX with
  the RFC number of this specification.]</a>.</p>
</body>
</html>
END
```

9.3. XML Schema Registration

This section registers a new XML schema in the IANA XML registry per the procedures in RFC 3688 [6].

URI: urn:ietf:params:xml:schema:copycontrol

Registrant Contact: IETF, SIPPING working group, (sipping@ietf.org), Miguel Garcia-Martin (miguel.an.garcia@nokia.com).

The XML for this schema can be found as the sole content of Section 5.

10. Acknowledgements

Thanks to Dean Willis, Jari Urpalainen, Pekka Kuure, Atsushi Sato, Brian Rosen, Mary Barnes, and James Polk for reviewing this document and providing helpful comments.

11. References

11.1. Normative References

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

[2] Troost, R., Dorner, S., and K. Moore, "Communicating Presentation Information in Internet Messages: The Content-Disposition Header Field", RFC 2183, August 1997.

[3] Dierks, T. and C. Allen, "The TLS Protocol Version 1.0", RFC 2246, January 1999.

[4] Zimmerer, E., Peterson, J., Vemuri, A., Ong, L., Audet, F., Watson, M., and M. Zonoun, "MIME media types for ISUP and QSIG Objects", RFC 3204, December 2001.

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

[6] Mealling, M., "The IETF XML Registry", BCP 81, RFC 3688, January 2004.

[7] Rosenberg, J., "Extensible Markup Language (XML) Formats for Representing Resource Lists", draft-ietf-simple-xcap-list-usage-05 (work in progress), February 2005.

[8] Ramsdell, B., "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification", RFC 3851, July 2004.

[9] Camarillo, G. and A. Roach, "Framework and Security Considerations for Session Initiation Protocol (SIP) Uniform Resource Identifier (URI)-List Services", draft-ietf-sipping-uri-services-06 (work in progress), September 2006.

11.2. Informational References

[10] Camarillo, G. and A. Johnston, "Conference Establishment Using Request-Contained Lists in the Session Initiation Protocol (SIP)", draft-ietf-sip-uri-list-conferencing-00 (work in progress), September 2006.

[11] Garcia-Martin, M. and G. Camarillo, "Multiple-Recipient MESSAGE Requests in the Session Initiation Protocol (SIP)", draft-ietf-sip-uri-list-message-00 (work in progress),

September 2006.

Authors' Addresses

Miguel A. Garcia-Martin
Nokia
P.O.Box 407
NOKIA GROUP, FIN 00045
Finland

Email: miguel.an.garcia@nokia.com

Gonzalo Camarillo
Ericsson
Hirsalantie 11
Jorvas 02420
Finland

Email: Gonzalo.Camarillo@ericsson.com

Full Copyright Statement

Copyright (C) The IETF Trust (2006).

This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).