Network Working Group C. Holmberg
Internet-Draft J. Axell
Intended status: Informational Ericsson
Expires: July 24, 2017 January 20, 2017

IANA Registration of New Session Initiation Protocol (SIP) Resource-Priority Namespace for Mission Critical Push To Talk service
draft-holmberg-dispatch-mcptt-rp-namespace-05

Abstract

This document creates an additional Session Initiation Protocol (SIP) Resource-Priority namespace to meet the requirements of the 3GPP defined Mission Critical Push To Talk, and places this namespace in the IANA registry.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

The Third Generation Partnership Project (3GPP) has defined a Mission Critical Push To Talk (MCPTT) over LTE service [TS.3GPP.22.179] . The MCPTT service supports an enhanced PTT service, suitable for mission critical scenarios, based upon 3GPP Evolved Packet System (EPS) services. The requirements for the MCPTT service defined within 3GPP can also form the basis for a non-mission critical Push To Talk (PTT) service.

The MCPTT service is intended to support communication between several users (a group call), where each user can gain permission to talk in an arbitrated manner. However, the MCPTT service also supports private calls between pairs of users.

MCPTT is primarily targeted to provide a professional Push To Talk service to e.g., public safety, transport companies, utilities or industrial and nuclear plants. In addition to this, a commercial PTT service for non-professional use (e.g., groups of people on holiday) may be delivered through an MCPTT system. Based on their operational model, the performance and MCPTT features in use vary per user organization, where functionality which is more mission critical specific (e.g., Imminent Peril Call) might not be available to commercial customers.

The MCPTT service provides its users with different priorities for the access to network resources in order to provide means to prioritize between calls when resources are scarce. These priorities take into account among other things the priority and role of the caller, the priority and type of the group, and the situation in which the call is made.

The SIP level call control procedures using these namespaces are specified in [TS.3GPP.24.379]. The namespaces defined here will support a wide range of queuing options. The namespaces correspond to what can be supported over the 3GPP Rx interface, defined in [TS.3GPP.29.214]. The usage of the namespaces can be tailored to the needs of the operator. The mechanism to do this is to configure which values a specific user is allowed to use. This configuration is specified in [TS.3GPP.24.384].

High priority calls when there is danger of life, for either the public safety worker or any other human, need to be set up immediately and thus require preemption. Other calls may be less sensitive in call set-up time but have a high priority once established. For these calls a queueing mechanism is more appropriate. The MCPTT data transfer service currently under development can benefit from a queueing mechanism. Another example is video only calls that are not critical in call set-up time, but where keeping the call is important.

This document creates additional Session Initiation Protocol (SIP) Resource-Priority namespaces to meet the requirements of the 3GPP defined Mission Critical Push To Talk, and places these namespaces in the IANA registry.

2. Applicability

This document defines namespaces applicable for MCPTT services defined by 3GPP that use the network services of a 3GPP defined LTE network. The use of this namespace outside such networks is undefined.

3. New SIP Resource-Priority Namespaces Created

3.1. Introduction

This document introduces the MCPTT namespaces mcpttp and mcpttq, the name coming from the 3GPP defined Mission Critical Push To Talk service.

3.2. The MCPTT namespaces

The mcpttp namespace uses the priority levels listed below from lowest to highest priority.

```
mcpttp.0 (lowest priority)
mcpttp.1
mcpttp.2
mcpttp.3
mcpttp.4
mcpttp.5
```

mcpttp.6
mcpttp.7
mcpttp.8
mcpttp.9
mcpttp.10
mcpttp.11
mcpttp.12
mcpttp.13
mcpttp.14
mcpttp.15 (highest priority)

Intended algorithm for mcpttp is preemption.

New Warning code: No.

New SIP response code: No.

The mcpttq namespace uses the priority levels listed below from lowest to highest priority.

mcpttq.0 (lowest priority)
mcpttq.1
mcpttq.2
mcpttq.3
mcpttq.4
mcpttq.5
mcpttq.6
mcpttq.7
mcpttq.8
mcpttq.9
mcpttq.10
mcpttq.11
mcpttq.12
mcpttq.13
mcpttq.14
mcpttq.15 (highest priority)

Intended algorithm for mcpttq is queuing.

New Warning code: No.

New SIP response code: No.

4. Security Considerations

This document does not have any impact on the security of the SIP MCPTT protocol. Its purpose is purely administrative in nature.

5. IANA Considerations

Abiding by the rules established within [RFC4412] and [RFC7134] , this is an Informative RFC creating two new namespaces, their associated priority-values, and intended algorithms.

6. Acknowledgments

The authors would like to thank Bob Fredericks, Baruh Hason, Mary Barnes and Keith Drage for comments and discussions.

7. Change Log

[RFC EDITOR NOTE: Please remove this section when publishing]

Changes from draft-holmberg-dispatch-mcptt-rp-namespace-04.

o - Editorial changes based on gen-art review. Renderin of authors name and address fixed.

Changes from draft-holmberg-dispatch-mcptt-rp-namespace-03.

o - Editorial changes based on sec- and opt- directorate reviews.

Changes from draft-holmberg-dispatch-mcptt-rp-namespace-01.

o - Removal of Conventions section.
o - Editorial changes.

Changes from draft-holmberg-dispatch-mcptt-rp-namespace-00.

o - The two namespaces have been spelt out explicitly.
o - The numbering of priority levels is changed from 1-16 to 0-15.
o - Address of one author has changed.

8. Normative References

[RFC4412] Schulzrinne, H. and J. Polk, "Communications Resource Priority for the Session Initiation Protocol (SIP)", RFC 4412, DOI 10.17487/RFC4412, February 2006, <http://www.rfc-editor.org/info/rfc4412>.

[RFC7134] Rosen, B., "The Management Policy of the Resource Priority Header (RPH) Registry Changed to "IETF Review"", RFC 7134, DOI 10.17487/RFC7134, March 2014, <http://www.rfc-editor.org/info/rfc7134>.

[TS.3GPP.22.179]
3GPP, "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Mission Critical Push To Talk (MCPTT) over LTE; Stage 1", 3GPP TS 22.179 13.3.0, December 2015.

[TS.3GPP.29.214]
3GPP, "3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Policy and Charging Control over Rx reference point;", 3GPP TS 29.314 13.7.0, September 2016.

[TS.3GPP.24.379]
3GPP, "3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Mission Critical Push To Talk (MCPTT) call control; Protocol specification;", 3GPP TS 24.379 13.2.0, September 2016.

[TS.3GPP.24.384]
3GPP, "3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Mission Critical Push To Talk (MCPTT) configuration management; Protocol specification", 3GPP TS 24.384 13.2.0, September 2016.

Authors’ Addresses

Christer Holmberg
Ericsson
Hirsalantie 11
Jorvas 02420
Finland

Email: christer.holmberg@ericsson.com

Joergen Axell
Ericsson
Groenlandsgatan 31
Stockholm 16480
Sweden

Email: jorgen.axell@ericsson.com

Network Working Group
Internet-Draft
Intended status: Best Current Practice
Expires: September 22, 2016

J. Peterson
Neustar
E. Rescorla
R. Barnes
Mozilla
R. Housley
Vigilsec

March 21, 2016

Best Practices for Securing RTP Media Signaled with SIP
draft-peterson-dispatch-rtpsec-00.txt

Abstract

Although the Session Initital Protocol (SIP) includes a suite of security services that has been expanded by numerous specifications over the years, there is no single place that explains how to use SIP to establish confidential media sessions. Additionally, existing mechanisms have some feature gaps that need to be identified and resolved in order for them to address the pervasive monitoring threat model. This specification describes practices for negotiating confidential media with SIP, including both comprehensive security solutions which bind the media to SIP-layer identities as well as opportunistic security solutions.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

The Session Initiation Protocol (SIP) [RFC3261] includes a suite of security services, ranging from Digest authentication for authenticating entities with a shared secret, to TLS for transport security, to S/MIME (optional) for body security. SIP is frequently used to establish media sessions, in particular audio or audiovisual sessions, which have their own security mechanisms available, such as Secure RTP [RFC3711]. However, the practices needed to bind security at the media layer to security at the SIP layer, to provide an assurance that protection is in place all the way up the stack, rely on a great many external security mechanisms and practices, and require a central point of documentation to explain their optimal use as a best practice.

Revelations about widespread pervasive monitoring of the Internet have led to a reevaluation of the threat model for Internet communications [RFC7258]. In order to maximize the use of security features, especially of media confidentiality, opportunistic measures must often serve as a stopgap when a full suite of services cannot be negotiated all the way up the stack. This document explains the limitations that may inhibit the use of comprehensive security, and provides recommendations for which external security mechanisms implementers should use to negotiate secure media with SIP. It moreover gives a gap analysis of the limitations of existing solutions, and specifies solutions to address them.

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 RFC 2119 [RFC2119] and RFC 6919 [RFC6919].

3. Security at the SIP and SDP layer

There are two approaches to providing confidentiality for media sessions set up with SIP: comprehensive security and opportunistic security.

3.1. Comprehensive Security

Comprehensive security for media sessions established by SIP requires the interaction of three protocols: SIP, the Session Description Protocol (SDP), and the Real-time Protocol, in particular its secure profile SRTP. Broadly, it is the responsibility of SIP to provide integrity for the media keying attributes conveyed by SDP, and those attributes will in turn identify the keys used by endpoints in the RTP media session that SDP negotiates. In that way, once SIP and SDP have exchanged the necessary information to initiate a session, the media endpoints will have a strong assurance that the keys they exchange have not been tampered with by third parties, and that end-to-end confidentiality is available.

Our current target mechanism for establishing the identity of the endpoints of a SIP session is the use of STIR [I-D.ietf-stir-rfc4474bis]. The STIR signature has been designed to prevent a class of impersonation attacks that are commonly used in robocalling, voicemail hacking, and related threats. STIR generates a signature over certain features of SIP requests, including header field values that contain an identity for the originator of the request, such as the From header field or P-Asserted-Identity field, and also over the media keys in SDP if they are present. As currently defined, STIR only provides a signature over the "a=fingerprint" attribute, which is a key fingerprint utilized by DTLS-SRTP [RFC5763]; consequently, STIR only offers comprehensive security for SIP sessions, in concert with SDP and SRTP, when DTLS-SRTP is the media security service. The underlying security object of STIR is extensible, however, and it would be possible to provide signatures over other SDP attributes that contain alternate keying material.

A STIR verification service can act in concept with an SRTP media endpoint to ensure that the key fingerprints, as given in SDP, match the keys exchanged to establish DTLS-SRTP. Typically, the verification service function would in this case be implemented in the SIP UAS, which would be composed with the media endpoint. If the STIR authentication service or verification service functions are implemented at an intermediary rather than an endpoint, this introduces the possibility that the intermediary could act as a man-in-the-middle, altering key fingerprints. As this attack is not in STIR’s core threat model, which focuses on impersonation rather than man-in-the-middle attacks, STIR offers no specific protections against it. However, it would be possible to build a deployment profile of STIR for media confidentiality which shifts these responsibilities to the endpoints rather than the intermediaries.

Note that STIR provides integrity protection for the SDP bodies of SIP requests, but not SIP responses. When a session is established, therefore, any SDP body carried by a 200 class response in the backwards direction will not be protected by an authentication service and cannot be verified. Thus, sending a secured SDP body in the backwards direction will require an extra RTT, typically a re-INVITE in the backwards direction. Again, this could be specified as a component of a secure media profile for STIR.

Future versions of this specification will show in detail how those gaps can be filled.

3.1.1. Anonymous Communications

In some cases, the identity of the initiator of a SIP session may be withheld due to user or provider policy. Per the recommendations of [RFC3323], this may involve using an identity such as "anonymous@anonymous.invalid" in the identity fields of a SIP request. [I-D.ietf-stir-rfc4474bis] does not currently permit authentication services to sign for requests that supply this identity. It does however permit signing for valid domains, such as "anonymous@example.com," as a way of implementation an anonymization service as specified in [RFC3323].

Even for anonymous sessions, providing media confidentiality and partial SDP integrity is still desirable. Barring the use of an anonymization service, this can only be accomplished with opportunistic security; the value of trying to provide an intermediate level between comprehensive and opportunistic security for this use case is a matter for futher discussion and study.

3.2. Opportunistic Security

Work is already underway on defining approaches to opportunistic media security for SIP in [I-D.johnston-dispatch-osrtp], which builds on the prior efforts of [I-D.kaplan-mmusic-best-effort-srtp]. The major protocol change proposed by that draft is to signal the use of opportunistic encryption by negotiating the AVP profile in SDP, rather than the SAVP profile (as specified in [RFC3711]) that would ordinarily be used when negotiating SRTP.

Opportunistic encryption approaches typically have no integrity protection for the keying material in SDP. Sending SIP over TLS hop-by-hop between user agents and any intermediaries will reduce the prospect that active attackers can alter keys for session requests on the wire.

4. Media Security

As there are several ways to negotiate media security with SDP, any of which might be used with either opportunistic or comprehensive security, further guidance to implementers is needed. In [I-D.johnston-dispatch-osrtp], opportunistic approaches considered include DTLS-SRTP, security descriptions [RFC4568], and ZRTP [RFC6189]. In order to prevent men-in-the-middle from decrypting media traffic, the "a=crypto" SDP parameter of security descriptions requires signaling confidentiality which STIR and related comprehensive security approaches cannot provide, so delivering keys by value in SDP in this fashion is NOT RECOMMENDED. Both DTLS-SRTP and ZRTP instead provide hashes which are carried in SDP, and thus require only integrity protection rather than confidentiality.

Of DTLS-SRTP and ZRTP, only DTLS-SRTP is a Standards Track Internet protocol. Future versions of this specification will give specific recommendations on support for media security protocols.

Future versions of this specification will explore the issue of multiple fingerprints appearing in the message, and offers that include both DTLS-SRTP and ZRTP security.

5. Acknowledgments

We would like to thank YOU for contributions to this problem statement and framework.

6. IANA Considerations

This memo includes no requests to the IANA.

7. Security Considerations

This document describes the security features that provide media sessions established with SIP with confidentiality, integrity, and authentication.

8. Informative References

[I-D.ietf-stir-rfc4474bis]
Peterson, J., Jennings, C., Rescorla, E., and C. Wendt, "Authenticated Identity Management in the Session Initiation Protocol (SIP)", draft-ietf-stir-rfc4474bis-07 (work in progress), February 2016.

[I-D.johnston-dispatch-osrtp]
Johnston, A., Aboba, B., Hutton, A., Liess, L., and T. Thomas, "An Opportunistic Approach for Secure Real-time Transport Protocol (OSRTP)", draft-johnston-dispatch-osrtp-02 (work in progress), February 2016.

[I-D.kaplan-mmusic-best-effort-srtp]
Audet, F. and H. Kaplan, "Session Description Protocol (SDP) Offer/Answer Negotiation For Best-Effort Secure Real-Time Transport Protocol", draft-kaplan-mmusic-best-effort-srtp-01 (work in progress), October 2006.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[RFC3261] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, DOI 10.17487/RFC3261, June 2002, <http://www.rfc-editor.org/info/rfc3261>.

[RFC3264] Rosenberg, J. and H. Schulzrinne, "An Offer/Answer Model with Session Description Protocol (SDP)", RFC 3264, DOI 10.17487/RFC3264, June 2002, <http://www.rfc-editor.org/info/rfc3264>.

[RFC3323] Peterson, J., "A Privacy Mechanism for the Session Initiation Protocol (SIP)", RFC 3323, DOI 10.17487/RFC3323, November 2002, <http://www.rfc-editor.org/info/rfc3323>.

[RFC3711] Baugher, M., McGrew, D., Naslund, M., Carrara, E., and K. Norrman, "The Secure Real-time Transport Protocol (SRTP)", RFC 3711, DOI 10.17487/RFC3711, March 2004, <http://www.rfc-editor.org/info/rfc3711>.

[RFC4568] Andreasen, F., Baugher, M., and D. Wing, "Session Description Protocol (SDP) Security Descriptions for Media Streams", RFC 4568, DOI 10.17487/RFC4568, July 2006, <http://www.rfc-editor.org/info/rfc4568>.

[RFC5124] Ott, J. and E. Carrara, "Extended Secure RTP Profile for Real-time Transport Control Protocol (RTCP)-Based Feedback (RTP/SAVPF)", RFC 5124, DOI 10.17487/RFC5124, February 2008, <http://www.rfc-editor.org/info/rfc5124>.

[RFC5763] Fischl, J., Tschofenig, H., and E. Rescorla, "Framework for Establishing a Secure Real-time Transport Protocol (SRTP) Security Context Using Datagram Transport Layer Security (DTLS)", RFC 5763, DOI 10.17487/RFC5763, May 2010, <http://www.rfc-editor.org/info/rfc5763>.

[RFC6189] Zimmermann, P., Johnston, A., Ed., and J. Callas, "ZRTP: Media Path Key Agreement for Unicast Secure RTP", RFC 6189, DOI 10.17487/RFC6189, April 2011, <http://www.rfc-editor.org/info/rfc6189>.

[RFC6919] Barnes, R., Kent, S., and E. Rescorla, "Further Key Words for Use in RFCs to Indicate Requirement Levels", RFC 6919, DOI 10.17487/RFC6919, April 2013, <http://www.rfc-editor.org/info/rfc6919>.

[RFC7258] Farrell, S. and H. Tschofenig, "Pervasive Monitoring Is an Attack", BCP 188, RFC 7258, DOI 10.17487/RFC7258, May 2014, <http://www.rfc-editor.org/info/rfc7258>.

Authors’ Addresses

Jon Peterson
Neustar, Inc.
1800 Sutter St Suite 570
Concord, CA 94520
US

Email: jon.peterson@neustar.biz

Eric Rescorla
Mozilla

Email: ekr@rtfm.com

Richard Barnes
Mozilla

Email: rbarnes@mozilla.com

Russ Housley
Vigilsec

Email: rhousley@vigilsec.com

Dispatch Working Group
Internet Draft
Intended status: Informational
Expires: August 2016

N. Weinronk
Gamma Communications

February 18, 2016

Last Diverting Line Identity
draft-weinronk-dispatch-last-diverting-line-id-00.txt

Status of this Memo

This Internet-Draft will expire on August 18, 2016.

Copyright Notice

Abstract

This document proposes an extension to the Session Initiation Protocol (SIP).

In cases where applications/services (for example verification / billing) are provided by a network that is not the originating network the Network Asserted Identity is needed to provide these services.

This extension provides the ability for a 'diversion service' to provide a Network Asserted Identity of the last diverting user to these applications/services.

This extension defines a new general header, Last Diverting Line Identity which conveys the Network Asserted Identity of the diverting party to these applications/services.

Table of Contents

1. Introduction

In cases where applications/services (for example verification / billing) are provided by a network that is not the originating network the Network Asserted Identity is needed to provide these services.

This extension provides the ability for a ’diversion service’ to provide a Network Asserted Identity of the last diverting user to these applications/services.

This extension defines a new general header, Last Diverting Line Identity which conveys the Network Asserted Identity of the diverting party to these applications/services.

In the legacy telephony network in the UK this information is provided by the Last Diverting Line Identity parameter. Note: This ISUP parameter is defined in the UK under the ’Nationally defined for National User’ parameter code range of values.

2. 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 [RFC2119].

In this document, these words will appear with that interpretation only when in ALL CAPS. Lower case uses of these words are not to be interpreted as carrying RFC-2119 significance.

3. Definitions

Diversion:

The ’diversion service’ could be defined as in [RFC7044] or as in [TS.24604].

NICC:

The UK Interoperability Standards Organisation.

4. Abbreviations

3GPP - 3rd Generation Partnership Project

ETSI - European Telecommunication Standard Institute

ISDN - Integrated Services Digital Network

ISUP - ISDN User Part

ITU - International Telecommunication Union

SIP - Session Initiation Protocol

TS - Technical Specification

UA - User Agent

UK - United Kingdom

5. Overview

In cases where applications/services (for example verification / billing) are provided by a network that is not the originating network the Network Asserted Identity is needed to provide these services.

This extension provides the ability for a ’diversion service’ to provide a Network Asserted Identity of the last diverting user to these applications/services.

This extension defines a new general header, Last Diverting Line Identity which conveys the Network Asserted Identity of the diverting party to these applications/services.

It could be added by SIP UAs, SIP Redirect Servers or SIP Proxy Servers.

In the legacy telephony network in the UK this information is provided by the Last Diverting Line Identity parameter. Note: This ISUP parameter is defined in the UK under the ’Nationally defined for National User’ parameter code range of values.

Example headers are:

```
Last-Diverting-Line-Identity: <sip:+441632123456@example.com;user=phone>

Last-Diverting-Line-Identity: <tel:+441632123456>
```

6. Formal Syntax

The following syntax specification uses the augmented Backus-Naur Form (BNF) as described in RFC-2234 [RFC2234].

Definition of new Last Diverting Line Identity header field:

The Last Diverting Line Identity header field is used among trusted SIP entities (typically intermediaries) to carry the verified identity of the diverting user.

Last-Diverting-Line-Identity = "Last-Diverting-Line-Identity" HCOLON LDLI-value

LDLI-value = name-addr

A Last-Diverting-Line-Identity header field value MUST consist of exactly one name-addr. It MUST be a sip, sips or tel URI.

6.1 The "ldli" Privacy Type

This specification adds a new priv-value to the Privacy header [RFC3323]. The presence of this privacy type in a Privacy header field indicates that the user would like the Last Diverting Line Identity to be kept private with respect to untrusted SIP entities.

priv-value = "ldli"

If the "ldli" priv-value is not present the LDLI-value presentation is allowed.

If the "ldli" priv-value is present then the LDLI-value presentation is restricted.

This document adds the following entry to Table 2 of [RFC3261]:

Header field	where	proxy	ACK	BYE	CAN	INV	OPT	REG
Last-Diverting-Line-Identity		amdr	-	-	-	o	-	-

Header field	where	proxy	SUB	NOT	REF	INF	UPD	PRA
Last-Diverting-Line-Identity		amdr	-	-	-	-	-	-

The Last-Diverting-Line-identity header carries the following information, with the mandatory parameters required when the header is included in a request:

LDLI-value a mandatory parameter for capturing the Last Diverting Line Identity.

7. Why not use existing headers

Use of the last History-Info header entry [RFC7044] was considered however this is mapped to/from the ISUP Redirecting Number and there are cases where the ISUP Redirecting Number is not the Network Asserted Identity of the last diverting user - for example the ETSI ISDN Partial Re-routing service as implemented in the UK.

Note: In the UK the mapping would be to/from the new SIP header and the UK ISUP Last Diverting Line Identity parameter which provides the same functionality in UK ISUP leaving the ISUP Redirecting Number mapping to/from History-Info header as in the existing IETF / 3GPP / ITU / NICC specifications.

8. Security Considerations

This document defines a header field for SIP. The use of the Transport Layer Security (TLS) protocol [RFC5246] as a mechanism to ensure the overall confidentiality of the Last-Diverting-Line-Identity header fields is strongly RECOMMENDED. If TLS is NOT used, the intermediary MUST ensure that the messages are only sent within an environment that is secured by other means or that the messages don’t leave the intermediary’s domain. This results in Last-Diverting-Line-Identity’s having at least the same level of security as other headers in SIP that are inserted by intermediaries. With TLS, Last-Diverting-Line-Identity header fields are no less, nor no more, secure than other SIP header fields, which generally have even more impact on the subsequent processing of SIP sessions than the Last-Diverting-Line-Identity header field.

Note that while using the SIPS scheme (as per [RFC5630]) protects Last-Diverting-Line-Identity from tampering by arbitrary parties outside the SIP message path, all the intermediaries on the path are trusted implicitly. A malicious intermediary could arbitrarily delete, rewrite, or modify Last-Diverting-Line-Identity. This specification does not attempt to prevent or detect attacks by malicious intermediaries.

In terms of ensuring the privacy of LDLI-value, the same security considerations as those described in [RFC3323] apply. The Privacy

Service that’s defined in [RFC3323] MUST also support the new Privacy header field priv-value of "ldli".

9. IANA Considerations

9.1. Registration of SIP Last-Diverting-Line-Identity Header

This document defines a new SIP header field name:

Last-Diverting-Line-Identity

The following changes should be made to the header sub-registry under:

http:///www.iana.org/assignments/sip-parameters

The following row has been added to the header field section:

Header Name	Compact Form	Reference
Last-Diverting-Line-Identity	none	[????]

9.2. Registration of "ldli" for SIP Privacy Headers

This document defines a new priv-value for the SIP Privacy header:

ldli

The following changes should be made to

http://www.iana.org/assignments/sip-priv-values

The following has been added to the registration for the SIP Privacy header:

Name	Description	Registrant	Reference
ldli	Privacy requested for Last-Diverting-Line-Identity header	[????]	[????]

10. References

10.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2234] Crocker, D. and Overell, P.(Editors), "Augmented BNF for Syntax Specifications: ABNF", RFC 2234, Internet Mail Consortium and Demon Internet Ltd., November 1997.

[RFC3261] 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.

[RFC3323] Peterson, J., "A Privacy Mechanism for the Session Initiation Protocol (SIP)", RFC 3323, November 2002.

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 2008.

[RFC5630] Audet, F., "The Use of the SIPS URI Scheme in the Session Initiation Protocol (SIP)", RFC 5630, October 2009.

[RFC7044] Barnes, M., Audet, F., Schubert, S., van Elburg, J., and C. Holmberg, "An Extension to the Session Initiation Protocol (SIP) for Request History Information", RFC 7044,February 2014.

[TS.24604] 3GPP, "Communication Diversion (CDIV) using IP Multimedia (IM) Core Network (CN) subsystem; Protocol specification"

11. Acknowledgments

NICC SIP Task Group

This document was prepared using 2-Word-v2.0.template.dot.

Authors' Address

Nigel Weinronk
Gamma Communications

Phone: +443332403421
Email: nigel.weinronk@gamma.co.uk

Contributors' Addresses

Nick Ireland
NICC

Phone: +447889861066

Email: nick.ireland@niccstandards.org.uk

Perry Wilks
BT

Phone: +442087262646
Email: perry.wilks@bt.com