sipcore
Internet-Draft
Updates: 4119, 5606, 5774, 6442, 7378, 8262 (if approved)
Intended status: Standards Track
Expires: 17 September 2026

B. Rosen
Unaffiliated
J. Martin
Comtech TCS

16 March 2026

Comprehensive Errata for the 'retransmission-allowed' XML Element

draft-ietf-sipcore-retransmission-allowed-fixes-04

Abstract

This document fixes use of the 'retransmission-allowed' element of PIDF-LO in six published RFCs. All text and examples should show 'true' or 'false' to match the XML schema definitions, but some RFCs incorrectly use 'yes' or 'no'. This document updates RFC4119, RFC5606, RFC5774, RFC6442, RFC7378, RFC8262.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on 17 September 2026.

Copyright Notice

Table of Contents

1. Introduction

The PIDF Location Object (PIDF-LO) format defined by [RFC4119] includes the <retransmission-allowed> element. Section 2.2.5 "Schema Definitions" defines this element as a boolean data type as described in W3C's "XML Schema Part 2: Datatypes (Second Edition)" [XMLSCHEMA]. As a boolean data type, <retransmission-allowed> can have the following values: 'true', 'false', '0', or '1'.

Unfortunately the examples in the text of RFC 4119 used values 'yes' and 'no', which are not allowed per section 2.2.5 "Schema Definitions". This problem was reported in errata id 1535 (https://www.rfc-editor.org/errata/eid1535) in 2008, and verified in 2010.

Since RFC 4119, there are another 13 RFCs with <retransmission-allowed> example text. Despite the errata for RFC 4119, 5 of these 13 RFCs repeated the incorrect use of 'yes' and 'no' in their examples of <retransmission-allowed>: [RFC5606], [RFC5774], [RFC6442], [RFC7378], and [RFC8262]. The other 8 RFCs correctly use 'true' and 'false' in their examples: [RFC5580], [RFC5985], [RFC6397], [RFC6753], [RFC6772], [RFC7199], [RFC7852], and [RFC8876].

Rather than submitting individual errata against those 5 RFCs' incorrect examples of <retransmission-allowed>, this document updates them all to replace all use of 'yes' with 'true', and all use of 'no' with 'false'. The original RFC 4119 is also updated here for completeness, to further confirm the existing errata id 1535 for RFC 4119.

This also incorporates fixes to namespace issues in the <retransmission-allowed> examples in RFC4119 & RFC5774, as initially reported in errata id 1771 (https://www.rfc-editor.org/errata/eid1771).

Finally, this incorporates all the fixes in errata ids 1535 & 1771 to RFC4119. In addition to the <retransmission-allowed> fixes discussed above, these two errata also have minor fixes for the discussion of elements <retention-expiry> & <ruleset-reference>, and namespace issues for the examples of <retention-expiry>.

1.1. Requirements Notation

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

1.2. Additional Copyright Notice

2. Changes to Documents

2.1. RFC 4119 - A Presence-based GEOPRIV Location Object Format (PIDF-LO)

[RFC4119] section 2.2.2 page 8, replace:

> 'retransmission-allowed': When the value of this element is 'no', the Recipient of this Location Object is not permitted to share the enclosed Location Information, or the object as a whole, with other parties. When the value of this element is 'yes', distributing this Location is permitted (barring an existing out-of-band agreement or obligation to the contrary). By default, the value MUST be assumed to be 'no'. Implementations MUST include this field, with a value of 'no', if the Rule Maker specifies no preference.

With:

> 'retransmission-allowed': When the value of this element is *'false'*, the Recipient of this Location Object is not permitted to share the enclosed Location Information, or the object as a whole, with other parties. When the value of this element is *'true'*, distributing this Location is permitted (barring an existing out-of-band agreement or obligation to the contrary). By default, the value MUST be assumed to be *'false'*. Implementations MUST include this field, with a value of *'false'*, if the Rule Maker specifies no preference.

And replace:

> 'retention-expires': This field [...] in the 'retention-expires' element [...]
>
> 'ruleset-reference': This field [...] HTTPS-based ruleset-references into [...]

With:

> *'retention-expiry'*: This field [...] in the *'retention-expiry'* element [...]
>
> *'external-ruleset'*: This field [...] HTTPS-based *external-ruleset* into [...]

Section 2.3 "Example Location Objects", replace both occurrences of:

> xmlns:gp="urn:ietf:params:xml:ns:pidf:geopriv10"

With:

```
xmlns:gp="urn:ietf:params:xml:ns:pidf:geopriv10"
xmlns:gpb="urn:ietf:params:xml:ns:pidf:geopriv10:basicPolicy"
```

And replace:

```
<gp:retransmission-allowed>no</gp:retransmission-allowed>
<gp:retention-expiry>2003-06-23T04:57:29Z</gp:retention-expiry>
```

With:

```
<gpb:retransmission-allowed>false</gpb:retransmission-allowed>
<gpb:retention-expiry>2003-06-23T04:57:29Z</gpb:retention-expiry>
```

And replace:

```
<gp:retransmission-allowed>yes</gp:retransmission-allowed>
<gp:retention-expiry>2003-06-23T04:57:29Z</gp:retention-expiry>
```

With: > <gpb:retransmission-allowed>yes</gpb:retransmission-allowed>
> <gpb:retention-expiry>2003-06-23T04:57:29Z</gpb:retention-expiry>

2.2. RFC 5606 - Implications of ’retransmission-allowed’ for SIP Location Conveyance

[RFC5606] Section 2, replace:

> These questions and concerns are particularly problematic when <retransmission-allowed> is set to "no" (the default case). This core concern might be put as "to whom does <retransmission-allowed> apply in location-based routing?" More specifically:
>
> Is any entity that reads LI bound by <retransmission-allowed>? If so, does that mean a proxy that performs location-based routing is unable to forward a request and complete a SIP call if <retransmission-allowed> is "no"? Alternatively, must they strip the location body from the message in order to complete the call?
>
> If the proxy does not understand RFC 4119, it may forward a SIP message containing a policy statement <retransmission-allowed> set to "no". Is any proxy that does understand RFC 4119 required to parse the LI for this statement, even if it would not do so in order to route the message?

With:

> These questions and concerns are particularly problematic when <retransmission-allowed> is set to *"false"* (the default case). This core concern might be put as "to whom does <retransmission-allowed> apply in location-based routing?" More specifically:
>
> Is any entity that reads LI bound by <retransmission-allowed>? If so, does that mean a proxy that performs location-based routing is unable to forward a request and complete a SIP call if <retransmission-allowed> is *"false"*? Alternatively, must they strip the location body from the message in order to complete the call?
>
> If the proxy does not understand RFC 4119, it may forward a SIP message containing a policy statement <retransmission-allowed> set to *"false"*. Is any proxy that does understand RFC 4119 required to parse the LI for this statement, even if it would not do so in order to route the message?

Section 3.1, replace:

> After extensive discussion in both GEOPRIV and SIP contexts, there seems to be consensus that a solution for this problem must enable location-based routing to work even when the <retransmission-allowed> flag is set to "no".

With:

> After extensive discussion in both GEOPRIV and SIP contexts, there seems to be consensus that a solution for this problem must enable location-based routing to work even when the <retransmission-allowed> flag is set to *"false"*.

Section 3.2, replace:

> Because of this presumption, one SIP element may pass the LI to another even if the LO it contains has <retransmission-allowed> set to "no"; this sees the passing of the SIP message as part of the delivery to authorized recipients, rather than as retransmission. SIP entities are still enjoined from passing these messages outside the normal routing to external entities if <retransmission-allowed> is set to "no", as it is the passing to third parties that <retransmission-allowed> is meant to control.

With:

> Because of this presumption, one SIP element may pass the LI to another even if the LO it contains has <retransmission-allowed> set to *"false"*; this sees the passing of the SIP message as part

of the delivery to authorized recipients, rather than as retransmission. SIP entities are still enjoined from passing these messages outside the normal routing to external entities if <retransmission-allowed> is set to *"false"*, as it is the passing to third parties that <retransmission-allowed> is meant to control.

Section 3.5, replace:

"Location-Routing-Allowed" being set to "No" has no protocol-level mechanism for enforcement of this behavior; like the PIDF-LO <retransmission-allowed> being set to "no", it is a way for the Rule Maker to express a preference to the SIP elements, which are LI recipients.

With:

"Location-Routing-Allowed" being set to "No" has no protocol-level mechanism for enforcement of this behavior; like the PIDF-LO <retransmission-allowed> being set to *"false"*, it is a way for the Rule Maker to express a preference to the SIP elements, which are LI recipients.

Section 3.6, replace:

Where the B2BUA in fact does act as an endpoint (terminating the session and originating a different session), <retransmission-allowed> applies to it, and it must not copy location if <retransmission-allowed> is "no".

With:

Where the B2BUA in fact does act as an endpoint (terminating the session and originating a different session), <retransmission-allowed> applies to it, and it must not copy location if <retransmission-allowed> is *"false"*.

2.3. RFC 5774 - Considerations for Civic Addresses in PIDF-LO: Guidelines and IANA Registry Definition

[RFC5774] Section A.5 "Example", replace:

```
xmlns:gp="urn:ietf:params:xml:ns:pidf:geopriv10"
```

With:

```
xmlns:gp="urn:ietf:params:xml:ns:pidf:geopriv10"
xmlns:gpb="urn:ietf:params:xml:ns:pidf:geopriv10:basicPolicy"
```

And replace:

```
<gp:retransmission-allowed>yes</gp:retransmission-allowed>
<gp:retention-expiry>2009-11-10T12:00:00Z</gp:retention-expiry>
```

With:

```
<gpb:retransmission-allowed>true</gpb:retransmission-allowed>
<gpb:retention-expiry>2009-11-10T12:00:00Z</gpb:retention-expiry>
```

2.4. RFC 6442 - Location Conveyance for SIP

[RFC6442] section 4.4 page 18, replace:

> This location error is specific to having the PIDF-LO [RFC4119] <retransmission-allowed> element set to "no". This location error is stating it requires permission (i.e., PIDF-LO <retransmission-allowed> element set to "yes") to process this SIP request further. If the LS sending the location information does not want to give this permission, it will not change this permission in a new request. If the LS wants this message processed with the <retransmission-allowed> element set to "yes", it MUST choose another logical path (if one exists) for this SIP request.

With:

> This location error is specific to having the PIDF-LO [RFC4119] <retransmission-allowed> element set to *"false"*. This location error is stating it requires permission (i.e., PIDF-LO <retransmission-allowed> element set to *"true"*) to process this SIP request further. If the LS sending the location information does not want to give this permission, it will not change this permission in a new request. If the LS wants this message processed with the <retransmission-allowed> element set to *"false"*, it MUST choose another logical path (if one exists) for this SIP request.

Errata id 4236 (https://www.rfc-editor.org/errata/eid4236) incorrectly includes the following text

> Section 5.1, 5.2 says:
>
> ```
> <gbp:retransmission-allowed>false
> </gbp:retransmission-allowed>
> ```
>
> It should say:

```
<gbp:retransmission-allowed>no
</gbp:retransmission-allowed>
```

Sections 5.1 and 5.2 of RFC6442 are correct without any need for this errata id 4236. This errata should be ignored.

2.5. RFC 7378 - Trustworthy Location

[RFC7378] section 6 page 25, replace:

> as noted in RFC5606, Section 3.2:
>
> ... Because of this presumption, one SIP element may pass the LI to another even if the LO it contains has <retransmission-allowed> set to "no"; this sees the passing of the SIP message as part of the delivery to authorized recipients, rather than as retransmission. SIP entities are still enjoined from passing these messages outside the normal routing to external entities if <retransmission-allowed> is set to "no", as it is the passing to third parties that <retransmission-allowed> is meant to control.

With:

> as noted in RFC5606, Section 3.2:
>
> ... Because of this presumption, one SIP element may pass the LI to another even if the LO it contains has <retransmission-allowed> set to *"false"*; this sees the passing of the SIP message as part of the delivery to authorized recipients, rather than as retransmission. SIP entities are still enjoined from passing these messages outside the normal routing to external entities if <retransmission-allowed> is set to *"false"*, as it is the passing to third parties that <retransmission-allowed> is meant to control.

2.6. RFC 8262 - Content-ID Header Field in SIP

[RFC8262] section 1.4.1 "Example 1", replace:

```
<gbp:retransmission-allowed>no
</gbp:retransmission-allowed>
```

With:

```
<gbp:retransmission-allowed>false
</gbp:retransmission-allowed>
```

3. General guidance to implementers

Implementations that create <retransmission-allowed> MUST use only values 'true', 'false', '0', or '1' as required by the schema in section 2.2.5 of [RFC4119]. Implementations that create SHOULD use only values 'true' and 'false'.

Implementations that accept <retransmission-allowed> MUST handle values 'true', 'false', '0', and '1'. Implementations that accept SHOULD treat values 'yes' & 'no' as synonyms for 'true' & 'false'.

4. Security Considerations

The changes in this document do not require additional security considerations beyond those already noted in the individual RFCs affected by this RFC.

5. IANA Considerations

None

6. References

6.1. Normative References

[RFC4119] Peterson, J., "A Presence-based GEOPRIV Location Object Format", RFC 4119, DOI 10.17487/RFC4119, December 2005, <https://www.rfc-editor.org/rfc/rfc4119>.

[RFC5606] Peterson, J., Hardie, T., and J. Morris, "Implications of 'retransmission-allowed' for SIP Location Conveyance", RFC 5606, DOI 10.17487/RFC5606, August 2009, <https://www.rfc-editor.org/rfc/rfc5606>.

[RFC5774] Wolf, K. and A. Mayrhofer, "Considerations for Civic Addresses in the Presence Information Data Format Location Object (PIDF-LO): Guidelines and IANA Registry Definition", BCP 154, RFC 5774, DOI 10.17487/RFC5774, March 2010, <https://www.rfc-editor.org/rfc/rfc5774>.

[RFC6442] Polk, J., Rosen, B., and J. Peterson, "Location Conveyance for the Session Initiation Protocol", RFC 6442, DOI 10.17487/RFC6442, December 2011, <https://www.rfc-editor.org/rfc/rfc6442>.

[RFC7378] Tschofenig, H., Schulzrinne, H., and B. Aboba, Ed., "Trustworthy Location", RFC 7378, DOI 10.17487/RFC7378, December 2014, <https://www.rfc-editor.org/rfc/rfc7378>.

[RFC8262] Holmberg, C. and I. Sedlacek, "Content-ID Header Field in the Session Initiation Protocol (SIP)", RFC 8262, DOI 10.17487/RFC8262, October 2017, <https://www.rfc-editor.org/rfc/rfc8262>.

[XMLSCHEMA] "XML Schema Part 2: Datatypes Second Edition", 28 October 2004, <https://www.w3.org/TR/xmlschema-2/>. See section 3.2.2 boolean

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

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

6.2. Informative References

[RFC5580] Tschofenig, H., Ed., Adrangi, F., Jones, M., Lior, A., and B. Aboba, "Carrying Location Objects in RADIUS and Diameter", RFC 5580, DOI 10.17487/RFC5580, August 2009, <https://www.rfc-editor.org/rfc/rfc5580>.

[RFC5985] Barnes, M., Ed., "HTTP-Enabled Location Delivery (HELD)", RFC 5985, DOI 10.17487/RFC5985, September 2010, <https://www.rfc-editor.org/rfc/rfc5985>.

[RFC6397] Manderson, T., "Multi-Threaded Routing Toolkit (MRT) Border Gateway Protocol (BGP) Routing Information Export Format with Geo-Location Extensions", RFC 6397, DOI 10.17487/RFC6397, October 2011, <https://www.rfc-editor.org/rfc/rfc6397>.

[RFC6753] Winterbottom, J., Tschofenig, H., Schulzrinne, H., and M. Thomson, "A Location Dereference Protocol Using HTTP-Enabled Location Delivery (HELD)", RFC 6753, DOI 10.17487/RFC6753, October 2012, <https://www.rfc-editor.org/rfc/rfc6753>.

[RFC6772] Schulzrinne, H., Ed., Tschofenig, H., Ed., Cuellar, J., Polk, J., Morris, J., and M. Thomson, "Geolocation Policy: A Document Format for Expressing Privacy Preferences for Location Information", RFC 6772, DOI 10.17487/RFC6772, January 2013, <https://www.rfc-editor.org/rfc/rfc6772>.

[RFC7199] Barnes, R., Thomson, M., Winterbottom, J., and H. Tschofenig, "Location Configuration Extensions for Policy Management", RFC 7199, DOI 10.17487/RFC7199, April 2014, <https://www.rfc-editor.org/rfc/rfc7199>.

[RFC7852] Gellens, R., Rosen, B., Tschofenig, H., Marshall, R., and J. Winterbottom, "Additional Data Related to an Emergency Call", RFC 7852, DOI 10.17487/RFC7852, July 2016, <https://www.rfc-editor.org/rfc/rfc7852>.

[RFC8876] Rosen, B., Schulzrinne, H., Tschofenig, H., and R. Gellens, "Non-interactive Emergency Calls", RFC 8876, DOI 10.17487/RFC8876, September 2020, <https://www.rfc-editor.org/rfc/rfc8876>.

Contributors

Gordon Hines
Comtech TCS
2401 Elliott Avenue
Seattle, WA 98121
United States of America
Email: skip.hines@comtech.com

Roger Marshall
Comtech TCS
2401 Elliott Avenue
Seattle, WA 98121
United States of America
Email: roger.marshall@comtech.com

Victor Burton
Comtech TCS
2401 Elliott Avenue
Seattle, WA 98121
United States of America
Email: victor.burton@comtech.com

Authors' Addresses

Brian Rosen
Unaffiliated
Mars, PA
United States of America
Email: br@brianrosen.net

Jeff Martin
Comtech TCS
2401 Elliott Avenue
Seattle, WA 98121
United States of America
Email: jeff.martin@comtech.com