Message Annotations for Response Routing Version 1.0

Committee Specification 01

16 February 2021

This stage:
https://docs.oasis-open.org/amqp/respann/v1.0/cs01/respann-v1.0-cs01.docx (Authoritative)
https://docs.oasis-open.org/amqp/respann/v1.0/cs01/respann-v1.0-cs01.html
https://docs.oasis-open.org/amqp/respann/v1.0/cs01/respann-v1.0-cs01.pdf

Previous stage:
https://docs.oasis-open.org/amqp/respann/v1.0/csprd01/respann-v1.0-csprd01.docx (Authoritative)
https://docs.oasis-open.org/amqp/respann/v1.0/csprd01/respann-v1.0-csprd01.html
https://docs.oasis-open.org/amqp/respann/v1.0/csprd01/respann-v1.0-csprd01.pdf

Latest stage:
https://docs.oasis-open.org/amqp/respann/v1.0/respann-v1.0.docx (Authoritative)
https://docs.oasis-open.org/amqp/respann/v1.0/respann-v1.0.html
https://docs.oasis-open.org/amqp/respann/v1.0/respann-v1.0.pdf

Technical Committee:
OASIS Advanced Message Queuing Protocol (AMQP) TC

Chairs:
Rob Godfrey (rgodfrey@redhat.com), Red Hat
Clemens Vasters (clemensv@microsoft.com), Microsoft

Editor:
Rob Godfrey (rgodfrey@redhat.com), Red Hat

Related work:
This specification is related to:

- *OASIS Advanced Message Queuing Protocol (AMQP) Version 1.0 Part 0: Overview*. Edited by Robert Godfrey, David Ingham, and Rafael Schloming. 29 October 2012. OASIS Standard. http://docs.oasis-open.org/amqp/core/v1.0/os/amqp-core-overview-v1.0-os.html.

Abstract:
Large scale messaging networks may consist of multiple distinct sub-networks where addresses visible at one point in the network are not visible at other points. Where messages are transferred across network boundaries, addresses contained within the message (such as those in the reply-to field) may no longer be valid. This document defines mechanisms to allow messages which transit such boundaries to be annotated with sufficient information to allow responses to be directed back to the intended recipient.

Status:
This document was last revised or approved by the OASIS Advanced Message Queuing Protocol (AMQP) TC on the above date. The level of approval is also listed above. Check the "Latest stage" location noted above for possible later revisions of this document. Any other numbered Versions and other technical work produced by the Technical Committee (TC) are listed at https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=amqp#technical.

TC members should send comments on this document to the TC's email list. Others should send comments to the TC's public comment list, after subscribing to it by following the instructions at the "Send A Comment" button on the TC's web page at https://www.oasis-open.org/committees/amqp/.

This specification is provided under the RF on RAND Terms Mode of the OASIS IPR Policy, the mode chosen when the Technical Committee was established. For information on whether any patents have been disclosed that may be essential to implementing this specification, and any offers of patent licensing terms, please refer to the Intellectual Property Rights section of the TC's web page (https://www.oasis-open.org/committees/amqp/ipr.php).

Note that any machine-readable content (Computer Language Definitions) declared Normative for this Work Product is provided in separate plain text files. In the event of a discrepancy between any such plain text file and display content in the Work Product's prose narrative document(s), the content in the separate plain text file prevails.

Citation format:
When referencing this specification, the following citation format should be used:

[Message-Annotations-v1.0]

Message Annotations for Response Routing Version 1.0. Edited by Rob Godfrey. 16 February 2021. OASIS Committee Specification 01. https://docs.oasis-open.org/amqp/respann/v1.0/cs01/respann-v1.0-cs01.html. Latest stage: https://docs.oasis-open.org/amqp/respann/v1.0/respann-v1.0.html.

Notices

All capitalized terms in the following text have the meanings assigned to them in the OASIS Intellectual Property Rights Policy (the "OASIS IPR Policy"). The full Policy may be found at the OASIS website.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published, and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this section are included on all such copies and derivative works. However, this document itself may not be modified in any way, including by removing the copyright notice or references to OASIS, except as needed for the purpose of developing any document or deliverable produced by an OASIS Technical Committee (in which case the rules applicable to copyrights, as set forth in the OASIS IPR Policy, must be followed) or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by OASIS or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and OASIS DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY OWNERSHIP RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

As stated in the OASIS IPR Policy, the following three paragraphs in brackets apply to OASIS Standards Final Deliverable documents (Committee Specifications, OASIS Standards, or Approved Errata).

[OASIS requests that any OASIS Party or any other party that believes it has patent claims that would necessarily be infringed by implementations of this OASIS Standards Final Deliverable, to notify OASIS TC Administrator and provide an indication of its willingness to grant patent licenses to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this deliverable.]

[OASIS invites any party to contact the OASIS TC Administrator if it is aware of a claim of ownership of any patent claims that would necessarily be infringed by implementations of this OASIS Standards Final Deliverable by a patent holder that is not willing to provide a license to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this OASIS Standards Final Deliverable. OASIS may include such claims on its website, but disclaims any obligation to do so.]

[OASIS takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this OASIS Standards Final Deliverable or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on OASIS' procedures with respect to rights in any document or deliverable produced by an OASIS Technical Committee can be found on the OASIS website. Copies of claims of rights made available for publication 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 OASIS Standards Final Deliverable, can be obtained from the OASIS TC Administrator. OASIS makes no representation that any information or list of intellectual property rights will at any time be complete, or that any claims in such list are, in fact, Essential Claims.]

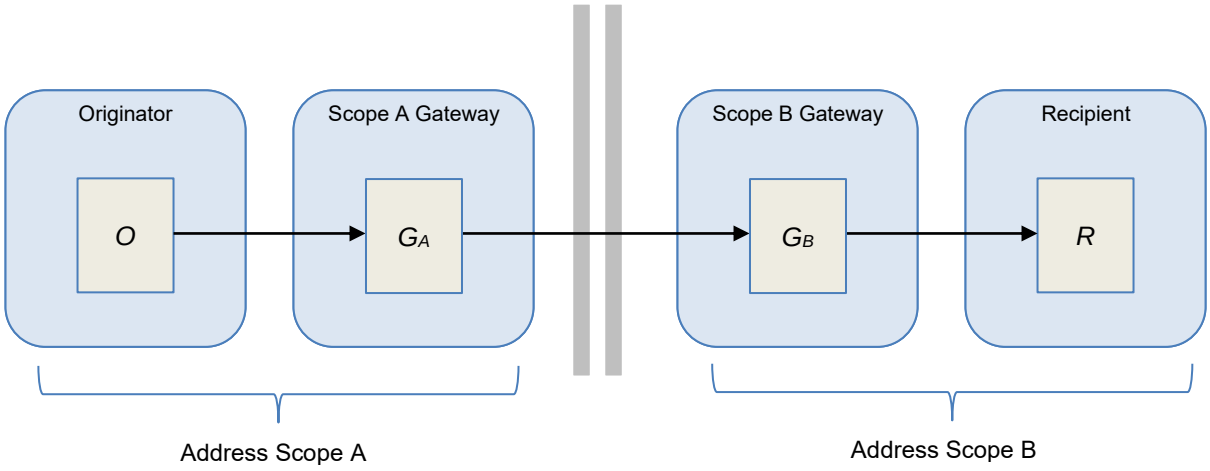
The name "OASIS" is a trademark of OASIS, the owner and developer of this specification, and should be used only to refer to the organization and its official outputs. OASIS welcomes reference to, and implementation and use of, specifications, while reserving the right to enforce its marks against misleading uses. Please see https://www.oasis-open.org/policies-guidelines/trademark for above guidance.

Table of Contents

1 Introduction

Large scale messaging networks may be composed of multiple sub-networks connected via defined gateways or bridges. Each sub-network may purposefully restrict the exposure of their internal address topology and/or prevent unsolicited attachment to its nodes. An address defined in one sub-network may not be directly reachable from another sub-network. Unless a coordinated addressing policy is enacted across the network, an address is scoped only to the scope in which the message originated.

An AMQP message may carry explicit or implicit address information to be used by the ultimate recipient (for example in the reply-to property). These addresses are set by the originator of the message, and thus would be expected to be scoped to the address scope of the originator. If the message traverses a boundary between address scopes, this means that addresses may no longer be meaningful to the recipient (they may not be routable, or may be routed to the wrong destination in the case of naming collision between namespaces). For any address in the bare message the value MUST NOT be modified, as this would contravene the requirements of Section 3.2 in [**AMQP**]. This document defines a mechanism by which messages can be annotated in such a way that response messages may be correctly routed.



1.1 Terminology

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] and [RFC8174] when, and only when, they appear in all capitals, as shown here.

1.2 Normative References

[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.

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

[AMQP] Godfrey, Robert; Ingham, David; Schloming, Rafael, “Advanced Message Queuing Protocol (AMQP) Version 1.0”, October 2012. OASIS Standard. http://docs.oasis-open.org/amqp/core/v1.0/os/amqp-core-overview-v1.0-os.html.

[AMQPANON] Godfrey, Robert, “Using the AMQP Anonymous Terminus for Message Routing Version 1.0". Latest version: http://docs.oasis-open.org/amqp/anonterm/v1.0/anonterm-v1.0.html.

[AMQPLINKPAIR] *AMQP Request-Response Messaging with Link Pairing Version 1.0*. Edited by Rob Godfrey. Latest version: https://docs.oasis-open.org/amqp/linkpair/v1.0/linkpair-v1.0.html.

2 Response Annotations

In order that responses are correctly routed, messages traversing an address scope boundary MUST be annotated to provide additional context information. This additional information is used by the recipient of the message to route and annotate response messages such that they carry sufficient information to be correctly routed to the response address in the origin scope.

Let us consider an example:

> A sender *S* has a connection to container *O*. *S* sends a message *M* to address *D*, with the reply-to property set to *Q*. The address *Q* denotes a queue in the container *O*. *O* determines that address *D* represents a service on a separate AMQP network with a different address scope (i.e. the address *Q* is not directly routable from any container within that network). O forwards the message to a container G_A which acts as a gateway. G_A is has established a receiving link from target address *T* in the remote network. G_A adds two delivery annotations to the message:
>
> - response-link-target-address with the value T
> - response-address-cookie with value being a binary value *B* containing information G_A wishes to receive on response messages.
>
> The annotated message is then sent into the remote network, which will route the message to the destination D.
>
> Upon arrival at destination D, a response message *N* is created. The to property of *N* is set to *Q* (the reply-to property of the incoming message). However, the service at D recognizes the two delivery annotations, indicating that the response message cannot be routed directly to *Q*. Instead an outgoing link to *T* is created, and response message *N* is also annotated with address-cookie having value *B*. The response message *N* is thus routed back via the gateway G_A which verifies the cookie, and routes the message to the final destination *Q*.

2.1 Connection Capabilities

On connection establishment, a peer MUST indicate whether it supports the use of response annotations. This is done through the exchange of connection capabilities (see Section 2.7.1 [**AMQP**]).

Capability Name	Definition
RESPONSE_ANNOTATIONS_V1_0	If present in the offered-capabilities field of the open performative, the sender of the open is capable of supporting response annotations for at least some incoming links. If present in the desired-capabilities field of the open performative, the sender of the open MAY attempt to use response annotations on some outgoing links if the receiver of the open supports this capability.

If a container does not support response annotations, then a message transiting between address scopes MUST be re-written (see 2.5 Message Rewriting).

2.2 Target Capabilities

When establishing a link which will carry messages which have traversed address scopes, the ability of the receiving endpoint to correctly interpret the response annotations MUST be established. This is achieved using a capability on the target of the link.

Capability Name	Definition
response-address-supported	If this capability is present in the target sent by the receiving link endpoint, responses to messages sent along the link MUST use the response annotations (if any) carried by the incoming messages as defined in this section.

If a target does not support response annotations, then a message which carries the response response-address-cookie or response-link-target-address annotations (see below) MUST be re-written (see 2.5 Message Rewriting).

2.3 Delivery Annotations (Request Message)

Where a sender is transiting messages between address scopes, and the target of the link supports response annotations, then the following delivery annotations are used.

Annotation Name	Definition
response-address-cookie	If this delivery annotation is present on a message transferred to a target with capability response-address-supported, then the value associated with this annotation MUST be placed as a delivery-annotation with name address-cookie in every response message. The value associated with this annotation MUST be of type binary. If this delivery annotation is present on a message transferred to a target which does not have capability response-address-supported, then the link on which the message was transferred MUST be detached with a not-implemented error as defined in section 3.2.10 of [**AMQP**].

Annotation Name	Definition
response-link-target-address	If this delivery annotation is present on a message transferred to a target with capability response-address-supported, then responses to this message MUST be sent over a link with the target set to the value of this delivery annotation, unless the request message was transferred on a paired link [AMQPLINKPAIR] and the response address is $me. If the message was transferred on a paired link and the response address is $me, then the paired link should be used for the response. If this delivery annotation is not present, and the message was not transferred over a paired link or the response address is not $me, then the response(s) should be sent on a link to the address in the "to" field of the response message, or, if supported, the link to the anonymous terminus [AMQPANON]. The value associated with this annotation MUST be of type string.
response-address-cookie-expiry	If present, this delivery annotation indicates the last possible moment in time where the response address cookie will still be valid. After this point in time messages sent with the address-cookie annotation set to the value of the response-address-cookie should be expected to be rejected. The value associated with this annotation MUST be of type timestamp. Note that expiry is purely informational and is not to be echoed back. A peer which is aware their token is close to expiry might use this information to solicit a new token through some application specific mechanism which generates a new request message.

2.4 Delivery Annotations (Response Messages)

For a target which has the capability response-address-supported, responses to messages carrying a response address cookie MUST echo the cookie back in the response message's delivery-annotations section so that the response can be correctly routed.

Annotation Name	Definition
address-cookie	Contains the value of the cookie that was provided in the response-address-cookie annotation of a request message. The value associated with this annotation MUST be of type binary.

2.5 Message Rewriting

Where a message is transiting between address scopes and response annotations are not supported, or when a message annotated with response annotations needs to be sent over a link where the target does not support them, then an alternative mechanism is required. One alternative mechanism is for the intermediary to rewrite the request message. That is, a new message (with a distinct message-id) needs to be created where the bare message is identical to the original except for any reference to response addresses (e.g. in the reply-to field). Such addresses need to be changed to an address that is

a) routable in the destination address scope and
b) capable of applying an inverse of the rewriting (that is converting addresses in the destination scope back to an address in the source scope).

Further the node at the rewritten address will need to convert any references to the message-id of the response message to a reference to the message-id of the original message (e.g. in the correlation-id property).

3 Conformance

When considering this specification, we can consider two distinct roles an AMQP container may play: Firstly, that of a Transiting Container – a container which transits messages between addressing scopes; Secondly a Responding Container – a container which receives messages (potentially originating from a different addressing scope) and responds to them.

A Transiting Container is conformant with this specification if:

1. When transiting messages to a target in a different address scope, the existence of the `response-address-supported` capability of the receiving link is respected.
2. Messages which are being transited to a different address scope and to be sent along a link which does provide the `response-address-supported` capability are enhanced with delivery annotations as per section 2.3.
3. Messages which are being transited to a different address scope and to be sent along a link which does not does provide the `response-address-supported` capability are to be rewritten as per section 2.5.
4. Messages which are received with an `address-cookie` annotation (as per section 2.4) must be forwarded to the target inferred from the `address-cookie` by the Transiting Container.

A Responding Container is conformant with this specification if:

1. The attach sent by a receiving link from a target which supports response annotations contains the `response-address-supported` capability.
2. Upon receiving a message sent over a link where the `response-address-supported` capability was set, and the request message contains delivery annotations as per section 2.3, response messages are sent with annotations as defined in section 2.4.

Appendix A. Acknowledgments

The following individuals have participated in the creation of this specification and are gratefully acknowledged:

Participants:
Alan Conway, Red Hat
Robbie Gemmell, Red Hat
Rob Godfrey, Red Hat
David Ingham, Red Hat
Ted Ross, Red Hat
Clemens Vasters, Microsoft
Keith Wall, Red Hat

Appendix B. Revision History

Revision	Date	Editor	Changes Made
WD01	5-May- 2017	Robert Godfrey	Initial working draft
WD02	15-May-2019	Robert Godfrey	Removed MUST wording from rewriting section. Changed address “domain” to “scope”.
WD03	14-June-2019	Robert Godfrey	Added conformance details
WD04	14-June-2019	Robert Godfrey	Fixed column title in tables