Implementation Guide for Direct Edge Protocols

Version 1.1, June 25, 2014

Contents

Change Control

Date	Version	Description of changes
10-30-2013	0.1	Initial Draft
01-10-2014	1.0	Initial Published Version
06-25-2014	1.1	Based on feedback from the community, clarified the combinations of edge protocols in scope and interoperability constraints, and further documented edge protocol delivery status notification in support of message tracking.

Status of this Guide

This document is PUBLISHED.

Introduction

Overview

Direct Project's Applicability Statement for Secure Health Transport establishes the standard protocols, along with message formats and processing requirements, for communication between Security/Trust Agents (STAs), which are commonly referred to by the name of the entities that operate STAs on behalf of others: Health Information Service Providers (HISPs). For the sake of uniformity, the term HISP will be used throughout this document. The communication protocol between HISPs is known as the Direct backbone protocol and is based on SMTP. While the Direct project has standardized the backbone protocol for communication between HISPs, currently there is minimal implementation guidance on how HISPs' clients' Edge systems should communicate with their respective HISP. In this document, the protocols used between HISP clients and the HISP are called "Direct Edge protocols," and the HISP clients are referred to as Edge systems.

Establishing standards between Edge systems and HISPs will enable CEHRT (Certified EHR Technology) to more easily interoperate with a variety of different HISP partners. In addition organizations such as HISP vendors, HIOs and RHIOs can support the standardized edge protocols as part of their HISP solution and expect Edge systems to integrate using the standardized edge protocols. The absence of these standardized edge protocols lead to custom solutions between HISPs and the Edge systems and negatively affect interoperability between systems.

This document provides guidance for standardizing Direct edge protocols and improving interoperability between HISPs and Edge systems. This implementation guidance is complementary to currently existing Direct project specifications.

Scope

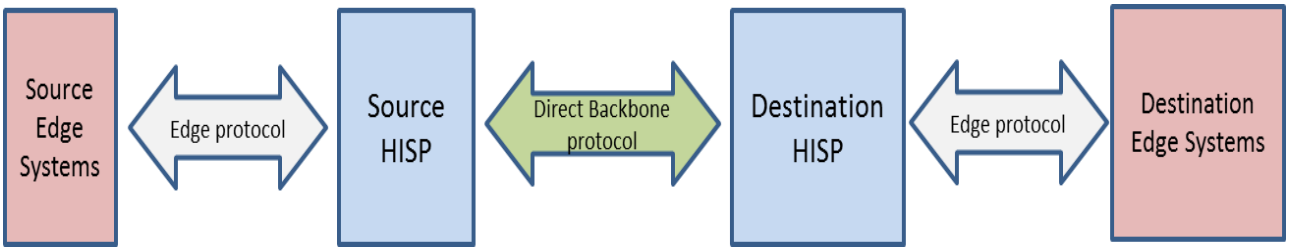
This guide details options for Direct edge protocols and specifies requirements for Edge systems and HISPs. The document also specifies preferred mechanisms that can be used for tracking and counting transactions, such as for ensuring the timely and reliable delivery of laboratory results reports or for ensuring the delivery of transitions of care in support of establishing numerator counts for Meaningful Use measures.

Definitions and Context

This section describes the top-level actors and definitions required to outline the specific requirements.

Directed Exchange Context

The following figure shows the context and actors involved in directed exchange. (Note: In real-world deployment the various actors can be played by one or more systems.)



As shown in the above diagram edge protocols are used to communicate between the Source Edge systems and the Source HISP and similarly between the Destination HISP and the Destination Edge systems. In Directed exchange, messages are pushed from Source Edge systems to Destination Edge systems using the edge and backbone protocols as shown above.

Assumptions

The decision to implement a particular edge protocol will vary based on each organization's technology preferences and policies. Similarly HISP vendors may support some or all of the different edge protocols specified in this implementation guide based on their technology preferences and policies. In more integrated pairings of HISPs and Edge systems, it's possible that edge protocols could be used that are outside the scope of this document.

Requirements

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.

An implementation is not compliant if it fails to satisfy one or more of the MUST, SHALL, or REQUIRED level requirements for the protocols it implements. An implementation that satisfies all the MUST, SHALL, or REQUIRED level and all the SHOULD level requirements for its protocols is said to be "unconditionally compliant"; one that satisfies all the MUST, SHALL, or REQUIRED level requirements but not all the SHOULD level requirements for its protocols is said to be "conditionally compliant."

In addition, annotations called "*Implementation Note*:" are used to provide additional clarification to implementers. These are non-normative and provided for clarification and informational purposes only.

1.0 Edge protocol options

The existing Direct project specifications use SMTP as the back bone protocol between HISP's and additionally define specifications to transform from IHE XDR and IHE XDM profiles to Internet Format Messages used by SMTP and vice versa. In addition to the above specifications vendors' systems are using a variety of edge protocols for communication between the Edge System and the HISP. While these Edge protocols vary, the following are commonly used edge protocols covered by this guide:

- IHE XDR profile for Limited Metadata Document Sources
- SMTP
- IMAP4
- POP3

From an implementation standpoint,

- HISPs SHOULD support all of the following edge protocols for sending information to and receiving information from Edge systems:
    - IHE XDR profile for Limited Metadata Document Sources
    - SMTP
- HISPs additionally MAY support one or more of the following edge protocols for sending information to Edge systems:
    - IMAP4
    - POP3
- Edge systems SHOULD support one or more of the following edge protocols for sending information to and receiving information from HISPs:
    - IHE XDR profile for Limited Metadata Document Sources
    - SMTP
    - Combination of SMTP and IMAP4 (i.e., SMTP+IMAP): SMTP for sending information to HISPs and IMAP4 for receiving information from HISPs

- Combination of SMTP and POP3 (i.e., SMTP+POP3): SMTP for sending information to HISPs and POP3 for receiving information from HISPs

1.1 IHE XDR Edge Protocol

A HISP or an Edge system should support IHE XDR as an edge protocol. In such a situation, following the guidance outlined in the next few sub-sections will lead to an interoperable solution between the Edge systems and the various HISPs.

1.1.1 HISP specific requirements

- A Direct HISP MUST conform to the *XDR and XDM for Direct Messaging v1.0* specification to translate between SMTP and XDR systems.
- A Direct HISP MUST conform to IHE XDR profile for Limited Metadata Document Sources to interoperate between SMTP backbone and XDR Edge systems.

1.1.2 Edge system specific requirements

- Edge systems implementing IHE XDR edge protocol MUST conform to IHE XDR profile for Limited Metadata Document Sources to interoperate with Direct HISPs.

1.1.3 Transport/Authentication Security requirements between HISP and Edge

- In order to minimize the security risks when transactions are not conducted over a secure network, both the Direct HISP and the Edge system MUST conform to the Connection Authentication requirements as specified by IHE ATNA profile Authenticate Node Transaction (ITI-19) described in section IHE ITI-2: 3.19.

1.2 SMTP Edge Protocol

A HISP or an Edge system should support SMTP as an edge protocol. In such a situation following the guidance outlined in the next few sub-sections will lead to an interoperable solution between the Edge systems and the various HISPs.

1.2.1 HISP specific requirements

- A Direct HISP MUST conform to RFC 2821 to interoperate with SMTP based Edge systems.

1.2.2 Edge system specific requirements

- Edge systems implementing SMTP edge protocol MUST conform to RFC 2821 to interoperate with Direct HISPs.

1.2.3 Transport Security requirements between HISP and Edge

- In order to minimize the security risks, both the Direct HISP and the Edge system MUST establish an encrypted TLS connection using the SMTP STARTTLS extension as defined in RFC 2487 if transactions are not otherwise conducted over a secure network.

1.2.4 Authentication requirements between HISP and Edge

SMTP can be used by a Direct HISP to send information to an Edge system and by an Edge system to send information to a Direct HISP. As a result, the Direct HISP or Edge system could be acting as an SMTP server or as an SMTP client depending on circumstances.

- For transactions not otherwise conducted over an authenticated channel, an SMTP client MUST support all of the following authentication mechanisms and an SMTP server MUST support one or more of the following authentication mechanisms:
    - The PLAIN SASL mechanism as defined in RFC 4616
    - The DIGEST-MD5 SASL mechanism as defined in RFC 2831
- An SMTP server and an SMTP client MAY use as appropriate alternative authentication mechanisms to those named specifically above.

1.3 IMAP4 Edge Protocol

A HISP or an Edge system may consider supporting IMAP4 as an edge protocol enabling an Edge system to receive information from a HISP. In such a situation, following the guidance outlined in the next few sub-sections will lead to an interoperable solution between the Edge systems and the various HISPs.

1.3.1 HISP specific requirements

- A Direct HISP MUST conform to RFC 3501 to interoperate with IMAP4 based Edge systems.

1.3.2 Edge system specific requirements

- Edge systems implementing IMAP4 edge protocol MUST conform to RFC 3501 to interoperate with Direct HISPs.

1.3.3 Transport Security requirements between HISP and Edge

- In order to minimize the security risks, both the Direct HISP and the Edge system MUST establish an encrypted TLS connection using the STARTTLS capabilities as defined in RFC 3501 if transactions are not otherwise conducted over a secure network.

1.3.4 Authentication requirements between HISP and Edge

- For transactions not otherwise conducted over an authenticated channel, an Edge system MUST support all of the following authentication mechanisms and a Direct HISP MUST support one or more of the following authentication mechanisms:
    - The PLAIN SASL mechanism as defined in RFC 4616
    - The DIGEST-MD5 SASL mechanism as defined in RFC 2831
- A Direct HISP and an Edge system MAY use as appropriate alternative authentication mechanisms to those named specifically above.

1.4 POP3 Edge Protocol

A HISP or an Edge system may consider supporting POP3 as an edge protocol enabling an Edge system to receive information from a HISP. In such a situation, following the guidance outlined in the next few sub-sections will lead to an interoperable solution between the Edge systems and the various HISPs.

1.4.1 HISP specific requirements

- A Direct HISP MUST conform to RFC 1939 to interoperate with POP3 based Edge systems.

1.4.2 Edge system specific requirements

- Edge systems implementing POP3 edge protocol MUST conform to RFC 1939 to interoperate with Direct HISPs.

1.4.3 Transport Security requirements between HISP and Edge

- In order to minimize the security risks, both the Direct HISP and the Edge system MUST establish an encrypted TLS connection using the POP3 STARTTLS capabilities as defined in Section 4 of RFC 2595 if transactions are not otherwise conducted over a secure network.

1.4.4 Authentication requirements between HISP and Edge

- For transactions not otherwise conducted over an authenticated channel, an Edge system MUST support all of the following authentication mechanisms and a Direct HISP MUST support one or more of the following authentication mechanisms:
    - The PLAIN SASL mechanism as defined in RFC 4616
    - The DIGEST-MD5 SASL mechanism as defined in RFC 2831
- A Direct HISP and an Edge system MAY use as appropriate alternative authentication mechanisms to those named specifically above.

1.5 Delivery Notification Tracking for Meaningful Use

Within healthcare, there are a number of use cases in which the sender needs to ensure that messages were successfully delivered from the source to the destination and retain the necessary proof to indicate that these transactions were successful. In order to implement these requirements there is a need to track the messages from the source to destination or destination HISP.

The Direct Project provides two mechanisms for tracking message delivery between HISPs:

- Using Message Disposition Notifications (MDN's) from Section 3 of the *Applicability Statement for Secure Health Transport v1.1* – Destination HISPs send MDN messages to the Source HISP on successful receipt and trust verification of a message. According to the *Applicability Statement*:
    - " By sending an MDN, the receiving STA is asserting:
        - That bilateral message trust has been verified
        - That the receiving user agent has received the message and is taking responsibility to deliver the message to the intended recipient "
- Using *Implementation Guide for Delivery Notification in Direct v1.0* - To provide a higher level of assurance that a message has arrived at its destination, the Direct Project created the *Implementation Guide for Delivery Notification in Direct v1.0*. This implementation guide outlines the various exception flows that result in compromised message delivery along with the mitigation actions that should be taken by HISPs to provide success and failure notifications to the sending system.

In both of these cases, the *Applicability Statement* and the *Implementation Guide for Delivery Notification in Direct v1.0* outline the functional requirements of the Source HISP and Destination HISP. However, these documents do not prescribe the mechanisms for tracking messages between a Sending Edge system and the Sending Edge system's HISP as these depend on the

edge protocols used between the Edge system and its respective HISP. Tracking messages between the Sending Edge system and the Sending Edge system's HISP involves the following three aspects:

- Edge systems "requesting" HISPs to provide status notifications for each message.
- HISPs "monitoring" received Direct notifications to determine status of each message per recipient.
- HISPs "reporting" to the Edge system the status of each message per recipient.

The requirements for the tracking of Direct messages depends on the edge protocols and the tracking mechanisms used between the Sending Edge system and its respective HISP. These requirements are identified in Sections 1.5.1 and 1.5.2, and Appendix A provides additional information on the use of these tracking mechanisms.

1.5.1 Tracking Messages for IMAP4/POP3/SMTP Edge protocols

1.5.1.1 HISP specific requirements

A Direct HISP that supports tracking of messages for IMAP4/POP3/SMTP Edge protocols MUST do so using the *Implementation Guide for Delivery Notification in Direct v1.0* and using processed MDNs implemented based on the *Applicability Statement*.

- A Direct HISP MUST fulfill requests from Edge systems for positive and negative delivery notifications by conforming to the *Implementation Guide for Delivery Notification in Direct v1.0* and implementing the tracking mechanisms required therein.
- For messages from Edge systems that do not request positive and negative delivery notifications per the *Implementation Guide for Delivery Notification in Direct v1.0*, a Direct HISP MUST notify or indicate back to the Edge system failed delivery to a destination if no processed MDN is received from the destination's HISP within a reasonable timeframe or if a failure notification is received from the destination or destination's HISP.
    - *Implementation Note:* when determining a "reasonable timeframe," a HISP should select a value that is appropriate for the health information exchange use case(s) it supports and consider the timeouts associated with Direct's SMTP-based transport (as outlined in RFC 2821).

1.5.1.2 Edge specific requirements

For IMAP4/POP3/SMTP Edge protocols, an Edge system that needs to track a particular message SHOULD do so by either:

- Conforming to the *Implementation Guide for Delivery Notification in Direct v1.0* and requesting positive and negative delivery notifications for that message by adding the

required headers per Section 1.3 of the *Implementation Guide for Delivery Notification in Direct v1.0* to the message to be tracked, or

  - *Implementation Note:* An Edge may choose to delegate control of when positive and negative delivery notifications are requested from destination HISPs to its own HISP rather than itself adding the required headers requesting such notifications. The mechanisms for doing this are outside the scope of this document.

- Monitoring for notifications associated with the message indicating failed delivery to any of the message's recipients.

In either case, the Edge system MUST include a `message-id` header in the message to be tracked as specified in RFC 5322 to permit automatic correlation with its associated Direct delivery notifications.

- *Implementation Note:* if an Edge system does not ensure the uniqueness of the `message-id`, the HISP might fail the message or provide an unreliable delivery notification.

1.5.2 Tracking Messages for IHE XDR Edge protocol

1.5.2.1 HISP specific requirements

A Direct HISP that supports tracking of messages for the IHE XDR Edge protocol MUST do so using the *Implementation Guide for Delivery Notification in Direct v1.0* and using `processed` MDNs implemented based on the *Applicability Statement*.

- A Direct HISP MUST fulfill requests from Edge systems for positive and negative delivery notifications by conforming to the *Implementation Guide for Delivery Notification in Direct v1.0* and implementing the tracking mechanisms required therein. To detect such requests, a Direct HISP MUST support a SOAP header named `X-DIRECT-FINAL-DESTINATION-DELIVERY` as part of the direct `addressBlock` header that is defined in Section 4.1 of *XDR and XDM for Direct Messaging v1.0*; when the value of this header is "true", an Edge system is requesting use of the *Implementation Guide for Delivery Notification in Direct*.

- For messages from Edge systems that do not request positive and negative delivery notifications per the *Implementation Guide for Delivery Notification in Direct v1.0*, a Direct HISP MUST notify or indicate back to the Edge system failed delivery to a destination if no `processed` MDN is received from the destination's HISP within a reasonable timeframe or if a failure notification is received from the destination or destination's HISP.

  - *Implementation Note:* when determining a "reasonable timeframe," a HISP should select a value that is appropriate for the health information exchange use case(s) it supports and consider the timeouts associated with Direct's SMTP-based transport (as outlined in RFC 2821).

To enable delivery of the notifications noted in the requirements above, a Direct HISP MUST support the requirements for delivery status notification using XDR detailed in Section 1.5.2.1.1 below. A Direct HISP MAY also support the requirements for status notification using WS-ReliableMessaging in Section 1.5.2.1.2.

Implementation Note: to enable message tracking, Edge systems send a unique MessageID in the WS-Addressing Header to the source HISP. As such, HISPs should map the MessageID used by the Edge system, as well as an identifier of the Edge system, to the `message-id` that the source HISP uses as it communicates with the destination HISP. This enables the source HISP to ensure that it returns delivery notifications to the appropriate Edge system.

1.5.2.1.1 Delivery Status Notification Using XDR

A Direct HISP MUST support delivery status notification using XDR. The requirements for doing so are listed below.

- For each notification of successful or failed delivery, a Direct HISP MUST create an XDR based message to be sent to the Edge system supplying delivery status. This message MUST have the following characteristics:
    - The intendedRecipient and/or <direct:to> MUST be the recipient of the notification
    - A <direct:notification> header MUST be included as part of the direct `addressBlock` defined in Section 4.1 of *XDR and XDM for Direct Messaging v1.0*. This header MUST have an attribute named "relatesTo" with a value matching the MessageID of the original message sent by the Edge system. The presence of this header indicates to the Edge system that the message pertains to a Direct delivery notification.
    - Other metadata MUST be consistent with the *XDR and XDM for Direct Messaging v1.0* specification, for minimal metadata.
    - The message MUST contain an XML based document payload of the following form, where "recipient" is an individual recipient of the original message. This document MUST be the only document contained in the message.

```
<direct:messageDisposition>
<direct:recipient>mailto:entity1@direct.example.org </direct:recipient>
<direct:disposition>success<direct:disposition>
</direct:messageDisposition>

OR
```

```
<direct:messageDisposition>
<direct:recipient>mailto:entity1@direct.example.org </direct:recipient>
<direct:disposition>failure<direct:disposition>
[<direct:reasonForFailure>reason</direct:reasonForFailure>] optional
</direct:messageDisposition>
```

1.5.2.1.2 Delivery Status Notification Using WS-ReliableMessaging

A Direct HISP MAY support status notification using WS-ReliableMessaging; the requirements for doing so are listed below. For an overview of WS-ReliableMessaging, please refer to Appendix B.

- A Direct HISP MUST implement the Reliable Messaging Destination requirements of the WS-ReliableMessaging 1.2 Protocol.
- A Direct HISP MUST notify or indicate back to the Edge system via WS-ReliableMessaging successful or failed delivery to a destination.

1.5.2.2 Edge specific requirements

For the IHE XDR Edge protocol, an Edge system that needs to track a particular message SHOULD do so by either:

- Requesting positive and negative delivery notifications as discussed in the *Implementation Guide for Delivery Notification in Direct v1.0*, or
- Monitoring for notifications associated with the message indicating failed delivery to any of the message's recipients.

To do this, an Edge System MUST support the requirements for delivery status notification using XDR detailed in Section 1.5.2.2.1 below. An Edge System MAY also support the requirements for status notification using WS-ReliableMessaging in Section 1.5.2.2.2.

1.5.2.2.1 Delivery Status Notification Using XDR

An Edge System MUST support delivery status notification using XDR. The requirements for doing so are outlined below.

- To enable tracking using the *Implementation Guide for Delivery Notification in Direct*, an Edge system MUST request positive and negative delivery notifications via a SOAP header named `X-DIRECT-FINAL-DESTINATION-DELIVERY` with a value of "true" as part of the direct `addressBlock` header that is defined in Section 4.1 of *XDR and XDM for Direct Messaging v1.0*.
    - *Implementation Note:* An Edge may choose to delegate control of when positive and negative delivery notifications are requested from destination HISPs to its own

HISP rather than itself adding the required headers requesting such notifications. The mechanisms for doing this are outside the scope of this document. However, unless such control has been explicitly delegated to its own HISP, the absence of the `X-DIRECT-FINAL-DESTINATION-DELIVERY` header will indicate that the Edge system will monitor for failed delivery notifications only.

- The Edge system MUST include the MessageID WS-Addressing header in the message to be tracked to permit automatic correlation with its associated Direct delivery notifications.
    - *Implementation Note:* if an Edge system does not ensure the uniqueness of the MessageID, the HISP might fail the message or provide an unreliable delivery notification.
- Upon receipt of an XDR message, an Edge system MUST look for a <direct:notification> header with an attribute named "relatesTo" contained as part of the direct `addressBlock` (the direct `addressBlock` is defined in Section 4.1 of *XDR and XDM for Direct Messaging v1.0*). The Edge system MUST treat the presence of this header as indicating the incoming message is a Direct delivery notification; the value of the "relatesTo" attribute will be the MessageID of the original message associated with the notification.
- For messages identified as Direct delivery notifications, an Edge system MUST use the included XML-based document payload specified in Section 1.5.2.1.1 to obtain delivery statuses.

1.5.2.2.2 Delivery Status Notification Using WS-ReliableMessaging

An Edge system MAY support status notification using WS-ReliableMessaging; for an overview of WS-ReliableMessaging, please refer to Appendix B. The requirements for using WS-ReliableMessaging when supporting the *Implementation Guide for Delivery Notification in Direct* versus monitoring for failed delivery notifications are outlined below.

- An Edge system MUST implement the Reliable Messaging Source requirements of WS-ReliableMessaging 1.2 Protocol.
- An Edge system MUST indicate to the HISP that WS-ReliableMessaging 1.2 Protocol be applied to the messages being exchanged.
- To enable tracking using the *Implementation Guide for Delivery Notification in Direct*, an Edge system MUST request positive and negative delivery notifications via a SOAP header named `X-DIRECT-FINAL-DESTINATION-DELIVERY` with a value of "true" as part of the direct `addressBlock` header that is defined in Section 4.1 of *XDR and XDM for Direct Messaging v1.0*.
    - *Implementation Note:* An Edge may choose to delegate control of when positive and negative delivery notifications are requested from destination HISPs to its own

HISP rather than itself adding the required headers requesting such notifications. The mechanisms for doing this are outside the scope of this document. However, unless such control has been explicitly delegated to its own HISP, the absence of the `X-DIRECT-FINAL-DESTINATION-DELIVERY` header will indicate that the Edge system will monitor for failed delivery notifications only.

- The Edge system MUST include the MessageID WS-Addressing header in the message to be tracked to permit automatic correlation with its associated Direct delivery notifications.
    - *Implementation Note:* if an Edge system does not ensure the uniqueness of the MessageID, the HISP might fail the message or provide an unreliable delivery notification.

Implementation Note: The mechanism used by WS-ReliableMessaging to provide delivery status details "success" and "failure" of a given message as a whole. As a result, while delivery status for a message with a single recipient should be clear to an Edge system, in cases where a message has multiple recipients, if sending to one or more recipients fails, it may not be as clear from the WS-ReliableMessaging delivery status which recipients failed.

2.0 References

1. Applicability Statement for Secure Health Transport v1.1
2. XDR and XDM for Direct Messaging v1.0
3. Implementation Guide for Delivery Notification in Direct v1.0
4. RFC 1939 - Post Office Protocol - Version 3
5. RFC 2119 - Keywords to use in RFC's for Requirement Levels
6. RFC 2487 - SMTP Service Extension for Secure SMTP over TLS
7. RFC 2595 - Using TLS with IMAP, POP3 and ACAP
8. RFC 2821 - Simple Mail Transfer Protocol
9. RFC 2831 - Using Digest Authentication as a SASL Mechanism
10. RFC 3501 - Internet Message Access Protocol - Version 4rev1
11. RFC 4616 - The PLAIN Simple Authentication and Security Layer (SASL) Mechanism
12. RFC 5322 - Internet Message Format
13. WS-Reliable Messaging
    a. http://en.wikipedia.org/wiki/WS-ReliableMessaging
    b. http://docs.oasis-open.org/ws-rx/wsrm/v1.2/wsrm.pdf
    c. http://docs.oasis-open.org/ws-rx/wsrm/200702/wsrm-1.2-spec-os.html

Appendix A: Message Delivery Tracking Options

As previously noted, the Direct Project provides two mechanisms for tracking message delivery between HISPs:

- `Processed` MDNs in *Applicability Statement for Secure Health Transport v1.1* – on successful receipt and trust verification of a message, Destination HISPs send `processed` Message Disposition Notification (MDN) messages to the Source HISP. By sending a `processed` MDN, the Destination HISP is asserting that 1) bilateral message trust has been verified and 2) that the Destination HISP is taking responsibility to deliver the message to the intended recipient.

- *Implementation Guide for Delivery Notification in Direct v1.0* – provides guidance enabling HISPs to provide a high level of assurance that a message has arrived at its destination and outlines the various exception flows that result in compromised message delivery and the mitigation actions that should be taken by HISPs to provide success and failure notifications to the sending system.

Assuming an Edge system and its HISP conform to the tracking requirements within this implementation guide, the Edge system may utilize either or both of these methods – positive and negative delivery notifications as specified by the *Implementation Guide for Delivery Notification*, or failed delivery notifications provided by its HISP when `processed` MDNs associated with sent messages are not received in a reasonable timeframe. However, implementers and end-users may be unclear as to which method is preferable for a particular use case or transaction type. This appendix provides a brief discussion of this issue.

To start, it's important to understand the difference between the type of delivery notification provided by a `processed` MDN versus that of the *Implementation Guide for Delivery Notification in Direct*.

An analogy may be helpful to clarify this. If Direct were a package delivery service, `processed` MDNs would be roughly equivalent to knowing that a package is 'out for delivery' on the local truck. While the probability of a successful delivery to the destination may be high, one wouldn't know with certainty that the package ultimately reached its destination nor the time at which that delivery occurred. In contrast, following the *Implementation Guide for Delivery Notification in Direct* closes that gap by providing mechanisms to ensure the timely and reliable delivery of the package to its destination. However, it is important to note that neither of these mechanisms ensure that the recipient opened the package and/or acted upon it.

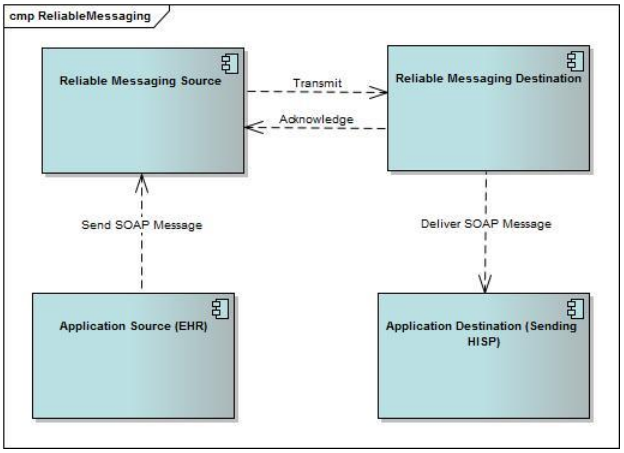
With this understanding, one may compare and contrast the attributes of both options with the functionality required for a particular use case. For example, government regulations or local policy may require the timely and reliable delivery of certain healthcare information, such as laboratory results. In such a case, an Edge system should request tracking based on the *Implementation Guide for Delivery Notification in Direct*. In contrast, to count transactions for Meaningful Use Stage 2 Transitions of Care (ToC) Measure #2 within a provider's numerator one

must only have a reasonable assurance that the message successfully reached its destination. Thus, tracking based on `processed` MDNs would be sufficient in this case.

Appendix B: WS-ReliableMessaging Overview

WS-ReliableMessaging (WS-RM) describes a protocol that allows SOAP messages to be reliably delivered between distributed applications in the presence of software component, system, or network failures. The protocol is standardized on version 1.2 at this time. The mechanism involves a series of standardized asynchronous messages and headers that are triggered by the sending of a SOAP business message. The standard works behind the scenes in order to communicate the success or failure of the delivery of the SOAP business message to the originator, without any change to the business web service operations themselves. On standard web service platforms, WS-Reliable Messaging can be turned on for any business transaction simply by making a configuration decision.

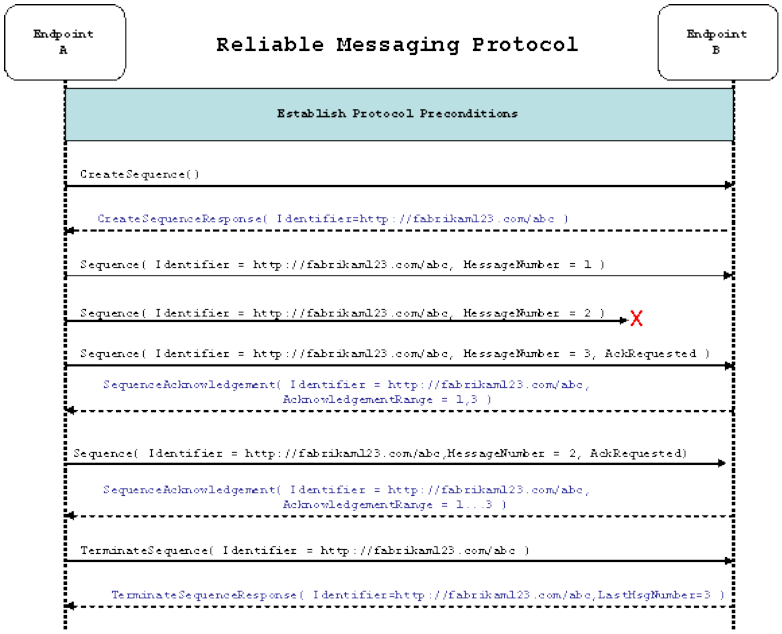
The Reliable Messaging Model



An Application Source (AS) wishes to reliably send messages to an Application Destination (AD) over an unreliable infrastructure. **In the case of this document the AS is an EHR and the AD is a HISP that is being used by the EHR.** To accomplish this they make use of a Reliable Messaging Source (RMS) and a Reliable Messaging Destination (RMD), which are added to the messaging stack through web service configuration. **The RMS part of the stack is associated with the Application Source (AS) and the RMD is associated with the HISP.** The AS sends a message to the AD as usual, but behind the scenes the message passes through the RMS and RMD. The RMS uses the WS-RM protocol to transmit the message to the RMD. The RMD delivers the message to the AD. If the RMS cannot transmit the message to the RMD for some reason, or if the RMD cannot reach the AD, the RMS must raise an exception or otherwise indicate to the AS that the message was not transmitted.

The Reliable Messaging Sequence

This is an example of the Reliable Messaging protocol as it operates “behind the scenes” of a SOAP business message delivery. This example has a failure which is overcome by the protocol. In most cases pertaining to this document, there will only be one Message per transaction, not the 3 shown here.



1. The protocol preconditions are established. These include policy exchange, endpoint resolution, and establishing trust.
2. The RM Source requests creation of a new Sequence.
3. The RM Destination creates a new Sequence and returns its unique identifier.
4. The RM Source begins Transmitting messages in the Sequence beginning with MessageNumber 1. In the figure above, the RM Source sends 3 messages in the Sequence.
5. The 2nd message in the Sequence is lost in transit.
6. The 3rd message is the last in this Sequence and the RM Source includes an AckRequested header to ensure that it gets a timely SequenceAcknowledgement for the Sequence. (Note: in WS-ReliableMessaging the headers sent from the EHR to the RMS are augmented, not replaced or enveloped).
7. The RM Destination acknowledges receipt of message numbers 1 and 3 as a result of receiving the RM Source's AckRequested header.
8. The RM Source retransmits the unacknowledged message with MessageNumber 2. This is a new message from the perspective of the underlying transport, but it has the same Sequence Identifier and MessageNumber so the RM Destination can recognize it as a duplicate of the earlier message, in case the original and retransmitted messages are both

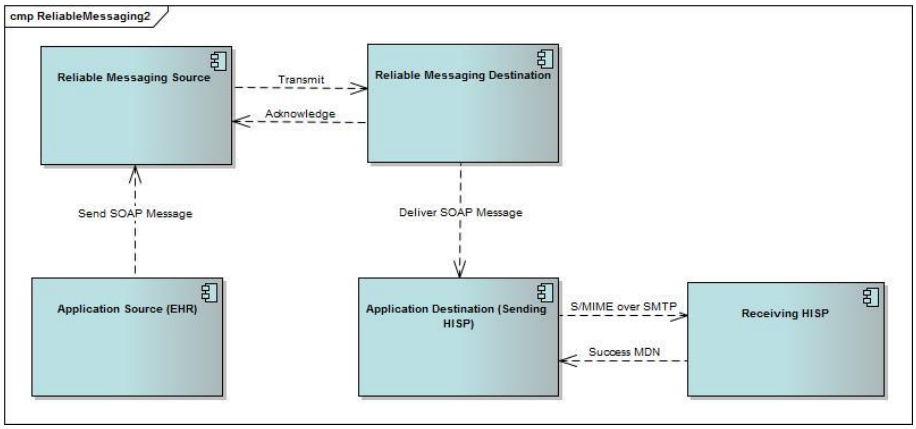
Received. The RM Source includes an AckRequested header in the retransmitted message so the RM Destination will expedite an acknowledgement.

9. The RM Destination Receives the second transmission of the message with MessageNumber 2 and acknowledges receipt of message numbers 1, 2, and 3.
10. The RM Source Receives this Acknowledgement and sends a TerminateSequence message to the RM Destination indicating that the Sequence is completed. The TerminateSequence message indicates that message number 3 was the last message in the Sequence. The RM Destination then reclaims any resources associated with the Sequence.
11. The RM Destination Receives the TerminateSequence message indicating that the RM Source will not be sending any more messages. The RM Destination sends a TerminateSequenceResponse message to the RM Source and reclaims any resources associated with the Sequence.

The RM Source will expect to Receive Acknowledgements from the RM Destination during the course of a message exchange. Should an Acknowledgement not be Received in a timely fashion, or not be successful after a configured number of tries, the RM Source MUST re-transmit the message or the Application Source must be notified that the delivery was unsuccessful through an exception, failure message, or some other fashion.

HISP Implementation Guidance

The next few paragraphs are provided as guidance to implementers. For the purposes of the Sending HISP implementation description, we have added a fifth component to our Model, the Receiving HISP. The only requirements on the Receiving HISP are those it already has – upon successful receipt and processing of a Direct message, to send a `processed` Message Disposition Notification back to the Sending HISP and, when requested, to send either a positive or negative delivery notification back to the Sending HISP.



In order for the WS-Reliable Messaging to serve the purpose in the Direct HISP to HISP scenario, we need to tie in Direct notifications with the Reliable Message Acknowledgement. This can be done with several steps.

1. A relationship must be persisted between the original SOAP MessageID (see requirement for MessageID) and the Message ID of the outgoing S/MIME message (required).
2. The Direct notification must be parsed to get the Original S/MIME message ID
3. The success of the overall transaction is determined by relating the Direct notification back to the original SOAP MessageID through the persisted relationship.
4. A timer must be set up to monitor the receipt of Direct notifications within a configurable period of time. The recommended period of time is 60 minutes. This same amount of time should be part of the WS-RM configuration.
5. The WS-ReliableMessaging Acknowledgement must be held until:
    a. A positive delivery notification is received (will arrive only upon request, represent as a successful ack)
    b. A negative delivery notification is received or the recommended period of time is exceeded without receiving a `processed` MDN or other Direct delivery notification (represent as an unsuccessful nack).

If the SOAP Message recipient is within the Sending HISP, determining the WS-RM Acknowledgement ack or nack is a matter of simple internal processing.

Edge Implementation Guidance

The Edge (EHR) Implementation has two pieces.

1. A mutually agreed upon implementation of WS-RM, the Recipient HISP must be configured. The EHR must implement the standard as well.
2. A header to document that the transaction expects to use WS-RM. This header currently is described to be placed with the other Direct XD headers

```
<direct:addressBlock xmlns:direct="urn:direct:addressing"
env:role="urn:direct:addressing:destination"
env:relay="true">
    <direct:from>mailto:entity1@direct.example.org</direct:from>
    <direct:to>mailto:entity2@direct.example.org</direct:to>
   <direct:X-DIRECT-FINAL-DESTINATION-DELIVERY>true</direct:X-DIRECT-
FINAL-DESTINATION-DELIVERY>
</direct:addressBlock>
```