Implementation Guide for Direct Edge Protocols

Version 1.0, January 10, 2014

Contents

Change Control

Date	Version	Description of changes
10-30-2013	0.1	Initial Draft
01-10-2014	1.0	Published

Status of this Guide

This document is PUBLISHED.

Introduction

Overview

The Direct Applicability Statement 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

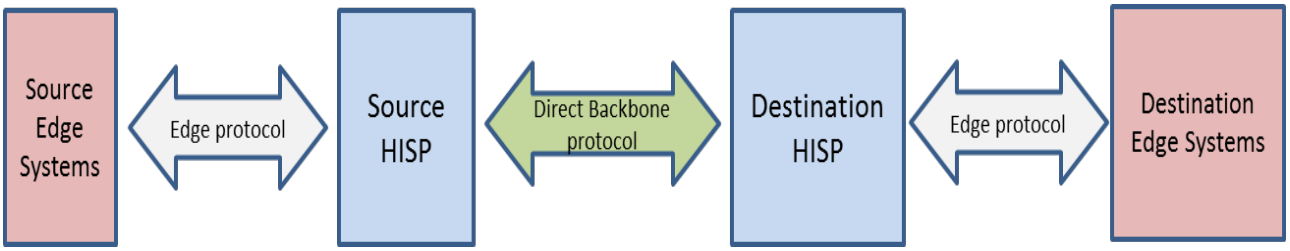
This guide details options for Direct edge protocols and specifies requirements for Edge systems and HISPs. The document also specifies preferred mechanisms that can be used for tracking and counting transactions, such as for ensuring the timely and reliable delivery of laboratory results reports or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

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 RFC2119.

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 the following edge protocols:
    - IHE XDR profile for Limited Metadata Document Sources
    - SMTP
- HISPs MAY support the following edge protocols:
    - IMAP4
    - POP3

1.1 IHE XDR Edge Protocol

A HISP or an Edge system may consider supporting 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 XDR and XDM for Direct Messaging 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, both the Direct HISP and the Edge system MUST conform to the Connection Authentication requirements as specified by IHE ATNA profile.

1.2 SMTP Edge protocol

A HISP or an Edge system may consider supporting 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 and Authentication requirements between HISP and Edge

- In order to minimize the security risks, both the Direct HISP and the Edge system MUST support the SMTP STARTTLS extension as defined in RFC 2487.

1.3 IMAP4 Edge protocol

A HISP or an Edge system may consider supporting IMAP4 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.

1.3.1 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 support the STARTTLS capabilities as defined in RFC 3501.

1.3.4 Authentication requirements between HISP and Edge

- In order to minimize the security risks, both the HISP and Edge system SHOULD choose appropriate SASL authentication mechanism from RFC 4422.

1.4 POP3 Edge protocol

A HISP or an Edge system may consider supporting POP3 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.

1.4.1 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 support the POP3 STARTTLS capabilities as defined in Section 4 of RFC 2595.

1.4.4 Authentication requirements between HISP and Edge

- In order to minimize the security risks, both the HISP and Edge system SHOULD choose appropriate SASL authentication mechanism from RFC 4422.

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 use the standardized edge protocols and track the messages from the source to destination.

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 Message Disposition Notification (MDN) messages to the Source HISP. By sending an MDN, the Destination HISP is asserting that 1) bilateral message trust has been verified and 2) that the receiving user agent has received the message and is taking responsibility to deliver the message to the intended recipient. However, the *Applicability Statement* provides minimal guidance regarding how MDNs should be handled once received by the Source HISP.

- *Implementation Guide for Delivery Notification in Direct v1.0* -- Due to the lack of specifications and guidance in the *Applicability Statement* regarding deviations from normal message flow, HISPs implementing only requirements denoted as MUST in Section 3 of the *Applicability Statement* cannot provide a high level of assurance that a message has arrived at its destination. To address this limitation, The Direct Project created the *Implementation Guide for Delivery Notification in Direct v1.0* that 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.

In both of these cases, the *Applicability Statement* and the *Delivery Notification in Direct* outline the functional requirements of the Source HISP and Destination HISP. However, these documents do not prescribe the mechanisms for handling a message's delivery notification requests/statuses between an Edge system and the Edge system's HISP as these depend on the edge protocols used between the Edge system and its respective HISP.

Appendix A provides additional information on the use of both tracking mechanisms.

The requirements for the tracking of Direct messages for the various edge protocols are identified in the next couple of sections.

1.5.1 Tracking Messages for IMAP4/POP3/SMTP Edge protocols

1.5.1.1 HISP specific requirements

A HISP that supports tracking of messages for IMAP4/POP3/SMTP Edge protocols can do so using processed MDNs implemented based on the Direct Applicability Statement and using the notifications defined in the *Implementation Guide for Delivery Notification in Direct v1.0*. The requirements for these specific cases are outlined below:

- A Direct HISP MUST support Tracking of Messages for IMAP4/POP3/SMTP Edge protocols using processed MDN's and the *Implementation Guide for Delivery Notification in Direct v1.0*.

Tracking Using Processed MDNs:

- A Direct HISP SHALL support `Disposition-Notification-Options` header as specified by Section 2.2 of RFC 3798 with a parameter named support X-DIRECT-DELIVER-PROCESSED-MDN.
    - The X-DIRECT-DELIVER-PROCESSED-MDN parameter SHALL have an importance of "optional" and a value of "true".
- A Direct HISP SHALL notify or indicate back to the sender successful delivery to destinations based on a received positive delivery notification messages it receives from Receiving HISP.
- A Direct HISP SHALL notify or indicate back to the sender failed delivery to a destination if no processed MDN is received from the Receiving HISP within a reasonable timeframe.
    - *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).

Tracking Using Implementation Guide for Delivery Notification in Direct:

- A Direct HISP SHALL conform to *Implementation Guide for Delivery Notification in Direct v1.0* to implement the necessary tracking mechanisms.

1.5.1.2 Edge specific requirements

An Edge system that requires tracking of messages for IMAP4/POP3/SMTP Edge protocols can do so using processed MDNs implemented based on the Direct Applicability Statement or may support the *Implementation Guide for Delivery Notification in Direct v1.0*. The requirements for these specific cases are outlined below:

- An Edge system SHOULD use either processed MDNs or the *Implementation Guide for Delivery Notification in Direct v1.0* to track messages.

Tracking Using Processed MDNs:

- An Edge system SHALL request processed MDN via the `Disposition-Notification-Options` header as specified by Section 2.2 of RFC 3798 with a parameter named support X-DIRECT-DELIVER-PROCESSED-MDN.
    - The X-DIRECT-DELIVER-PROCESSED-MDN parameter SHALL have an importance of "optional" and a value of "true".
- The Edge system SHALL include a `message-id` header as specified in RFC5322 to permit automatic correlation with its associated `processed` MDN message and delivery notification message when used for tracking purposes.
    - *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.

Tracking Using Implementation Guide for Delivery Notification in Direct:

- An Edge system SHALL conform to *Implementation Guide for Delivery Notification in Direct v1.0* to implement the necessary tracking mechanisms.
    - *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 protocols

The mechanism for obtaining a successful delivery notification across an XDR Edge scenario and including a HISP to HISP transaction is to use WS-ReliableMessaging. For an overview of the WS-ReliableMessaging please refer to Appendix B.

1.5.2.1 HISP specific requirements

A HISP that supports tracking of messages for the IHE XDR Edge protocol can do so using processed MDNs implemented based on the Direct Applicability Statement and using the notifications defined in the *Implementation Guide for Delivery Notification in Direct v1.0*. The requirements for these specific cases are outlined below:

- A Direct HISP MUST support Tracking of Messages for the IHE XDR Edge protocol using *processed* MDNs and the *Implementation Guide for Delivery Notification in Direct v1.0*.
    - *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.

Tracking Using Processed MDNs:

- The Direct HISP MUST implement the Reliable Messaging Destination requirements of the WS-ReliableMessaging 1.2 Protocol.
- A Direct HISP SHALL support a SOAP header named support X-DIRECT-DELIVER-PROCESSED-MDN.
    - The X-DIRECT-DELIVER-PROCESSED-MDN header SHALL have a value of "true".
- A Direct HISP SHALL notify or indicate back to the sender via WS-ReliableMessaging successful delivery to destinations based on a received positive delivery notification messages from the Receiving HISP.
- A Direct HISP SHALL notify or indicate back to the sender via WS-ReliableMessaging failed delivery to a destination if no processed MDN is received from the Receiving HISP within a reasonable timeframe.
    - *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).

Tracking Using Implementation Guide for Delivery Notification in Direct:

- The Direct HISP MUST implement the Reliable Messaging Destination requirements of WS-ReliableMessaging 1.2 Protocol.
- A Direct HISP SHALL support a SOAP header named support X-DIRECT-FINAL-DESTINATION-DELIVERY.
    - The X-DIRECT-FINAL-DESTINATION-DELIVERY header SHALL have a value of "true".
- A Direct HISP MUST conform to *Implementation Guide for Delivery Notification in Direct v1.0* to implement the necessary tracking mechanisms.

1.5.2.2 Edge specific requirements

An Edge system that requires tracking of messages for IHE XDR Edge protocols can do so using processed MDNs implemented based on the Direct Applicability Statement or may support the *Implementation Guide for Delivery Notification in Direct v1.0*. The requirements for these specific cases are outlined below:

- An Edge system SHOULD use either processed MDNs or the *Implementation Guide for Delivery Notification in Direct v1.0* to track messages.

Tracking Using Processed MDNs:

- 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.
- An Edge system SHALL request delivery notification based on processed MDN via a SOAP header named support X-DIRECT-DELIVER-PROCESSED-MDN as part of the direct addressBlock header.
    - The X-DIRECT-DELIVER-PROCESSED-MDN header SHALL have a value of "true".
- The Edge system SHALL include the MessageID WS-Addressing header to permit automatic correlation with its associated processed MDN message and delivery notification message when used for tracking purposes.
    - *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.

Tracking Using Implementation Guide for Delivery Notification in Direct:

- 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.
- An Edge system SHALL request delivery notification based on the Implementation Guide for Delivery Notification in Direct via a SOAP header named support X-DIRECT-FINAL-DESTINATION-DELIVERY as part of the direct addressBlock header.
    - The X-DIRECT-FINAL-DESTINATION-DELIVERY header SHALL have a value of "true".
- The Edge system SHALL include the MessageID WS-Addressing header to permit automatic correlation with its associated Direct delivery notification messages.
    - *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.
- An Edge system SHOULD conform to *Implementation Guide for Delivery Notification in Direct v1.0* to implement the necessary tracking mechanisms.

2.0 References

1. Applicability State for Secure Health Transport
2. Implementation Guide for Delivery Notification in Direct v1.0
3. RFC 1738 - Uniform Resource Locators
4. RFC 2119 - Keywords to use in RFC's for Requirement Levels
5. RFC 2246 - TLS Protocol
6. RFC 2315 – PKCS#7 Specification (Cryptographic Message Syntax Version 1.5)
7. RFC 2487 – SMTP Service Extension for Secure SMTP over TLS
8. RFC 2616 - Hyper Text Transfer Protocol
9. RFC 2821 – Simple Mail Transfer Protocol
10. RFC 3798 – Message Disposition Notification
11. RFC 5322 – Internet Message Format
12. RFC 5652 - Cryptographic Message Syntax
13. RFC 5751 - S/MIME v 3.2
14. RFC 5752 - Multiple Signatures in Cryptographic Message Syntax
15. 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 Message Disposition Notification (MDN) messages to the Source HISP. By sending an 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 their respective HISP supports both options, Edge systems may utilize either or both of these methods. However, implementers and end-users may be unclear as to which option 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 Delivery Notification in Direct.

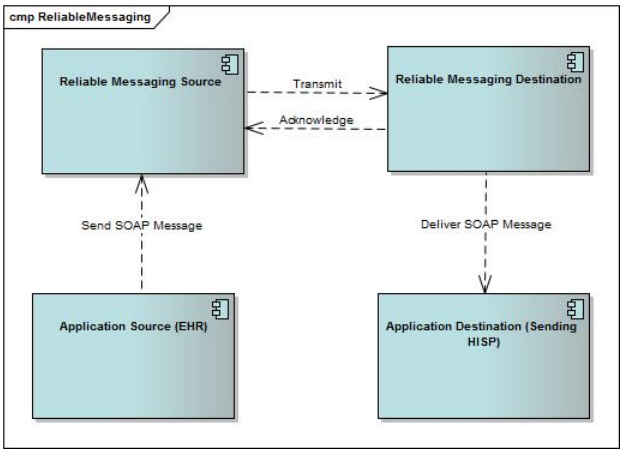
An analogy may be helpful to clarify this. If Direct were a package delivery service, 'Processed' MDNs would be roughly equivalent to knowing that a package is 'out for delivery' on the local truck. While the probability of a successful delivery to the destination may be high, one wouldn't know with certainty that the package ultimately reached its destination nor the time at which that delivery occurred. In contrast, following the Delivery Notification in Direct guide 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 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, an Edge system 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.

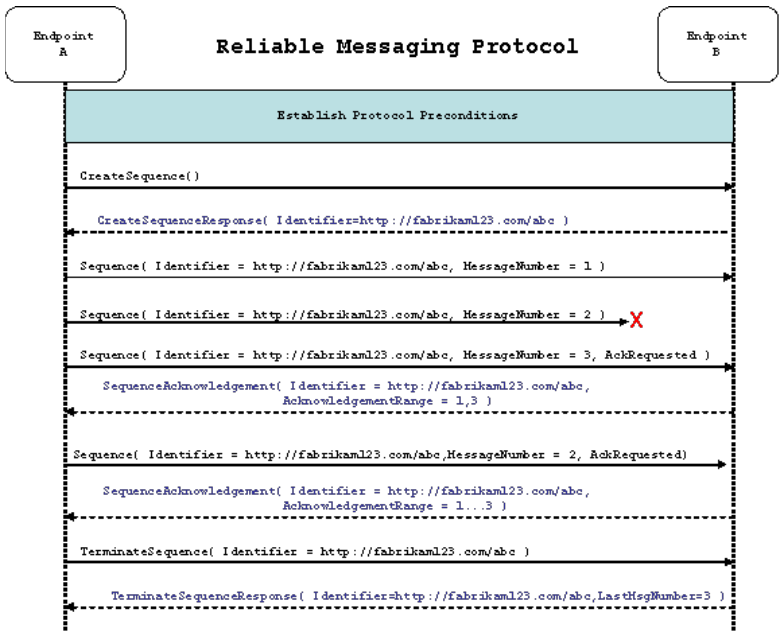
The Reliable Messaging Model



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.



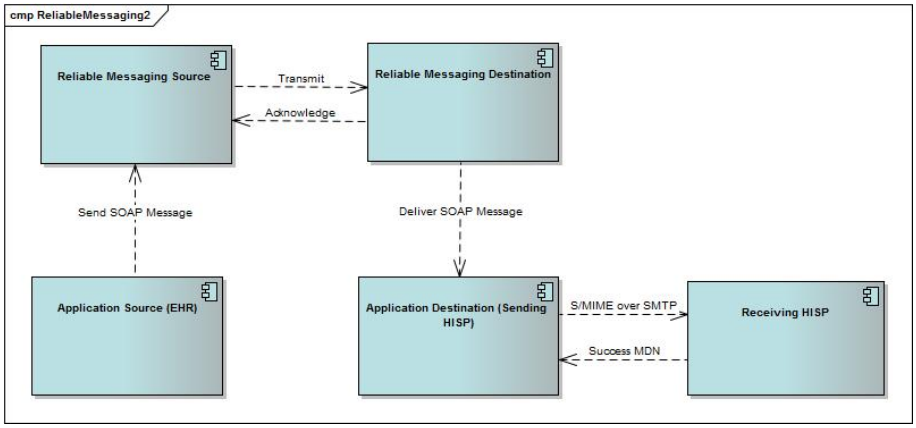
1. The protocol preconditions are established. These include policy exchange, endpoint resolution, and establishing trust.
2. The RM Source requests creation of a new Sequence.
3. The RM Destination creates a new Sequence and returns its unique identifier.
4. The RM Source begins Transmitting messages 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 requirement on the Receiving HISP is one it already has, to send a Success MDN upon receipt of the S/MIME encrypted Direct Message 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 the Success MDN 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 Success MDN must be parsed to get the Original S/MIME message ID
3. The success of the overall transaction is determined by relating the Success MDN back to the original SOAP MessageID through the persisted relationship.

4. A timer must be set up to monitor the receipt of the Success MDN 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. the MDN is received (successful ack)
   b. the recommended period of time is exceeded without receiving the MDN(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-deliver-processed-mdn>true</direct: x-direct-
deliver-processed-mdn>
</direct:addressBlock>
```