nehta

Secure Message Delivery

Overview

Version 1.0 Draft — 28 September 2009

For review and comment

National E-Health Transition Authority Ltd
Level 25
56 Pitt Street
Sydney, NSW, 2000
Australia.
www.nehta.gov.au

Document Information

Change History

Version	Date	Author	Comments
1.0 Draft	2009-09-25	Andrew Shrosbree	Verified Andy Berry's changes, removed old sections that have been superseded, including section on Infrastructure. Inserted CCA text. Refreshed all diagrams. Added new document map.
1.0 Draft	2009-09-24	Andrew Berry	Reviewed first draft of changes made after finalisation of the Endpoint spec.
1.0 Draft	2009-09-23	Andrew Shrosbree	Applied new spec name "SMD".
1.0 Draft	2009-05-12	Andrew Shrosbree	Major upgrade based on feedback from PIP-WG.
1.0 Draft	2009-03-31	Andrew Berry	Fixed minor inconsistencies. Draft release to community.
0.4	2009-03-17	Andrew Berry	Applied new spec name "SMD"
0.3	2009-03-03	Andrew Berry	Updated for consistency with other specification documents.
0.2	2009-02-04	Andrew Berry	Added scenario (process) diagrams, removed conformance criteria and revised text to reflect diagrams and address review comments
0.1	2009-01-21	Andrew Berry	Straw man draft for initial review

Table of Contents

Document Information ..... **iii**
Change History iii

Table of Contents ..... **iv**

Preface ..... **vii**
Document Purpose vii
Intended Audience vii
Document Map vii
Definitions, Acronyms and Abbreviations viii
References and Related Documents viii

1 Introduction **9**
1.1 Background 9
1.2 Purpose 9
1.3 Scope 9
1.4 Overview 9

2 Roles **10**
2.1 Sender 10
2.2 Receiver 10
2.3 Sender Intermediary 10
2.4 Receiver Intermediary 10

3 Context **11**
3.1 Community Model 11
3.2 Interaction Modes 11
3.3 Deferred Mode Messaging 11
3.3.1 Direct Interaction 12
3.3.2 Interaction via a Receiver Intermediary 12
3.3.3 Interaction via two Intermediaries 13
3.4 Immediate Mode Messaging 14
3.4.1 Direct Interaction 14
3.4.2 Interaction via an Intermediary 15

4 Conformance **17**

Definitions **18**
Shortened Terms 18
Glossary 18

References **19**
Specification Documents 19
References 19

This page is intentionally left blank.

Preface

Document Purpose

The purpose of this document is to introduce and contextualise the body of work facing software vendors and organisations who choose to implement NEHTA Secure Message Delivery (SMD). It is a supporting document for the endpoint specification [SMD-ES], which defines detailed requirements and behaviour for implementations of SMD.

Intended Audience

This document should be read and understood by:

- Software Vendors and Messaging Service Providers:
  - To understand the NEHTA approach
  - To identify the requirements for conformance of messaging software and services with NEHTA SMD.
- Practice Managers for GP Clinics and Specialists
  - To understand the NEHTA approach

This document is a draft and has been released for comment and feedback purposes.

Document Map

This diagram represents the relationship between this document and others within the SMD Specification.

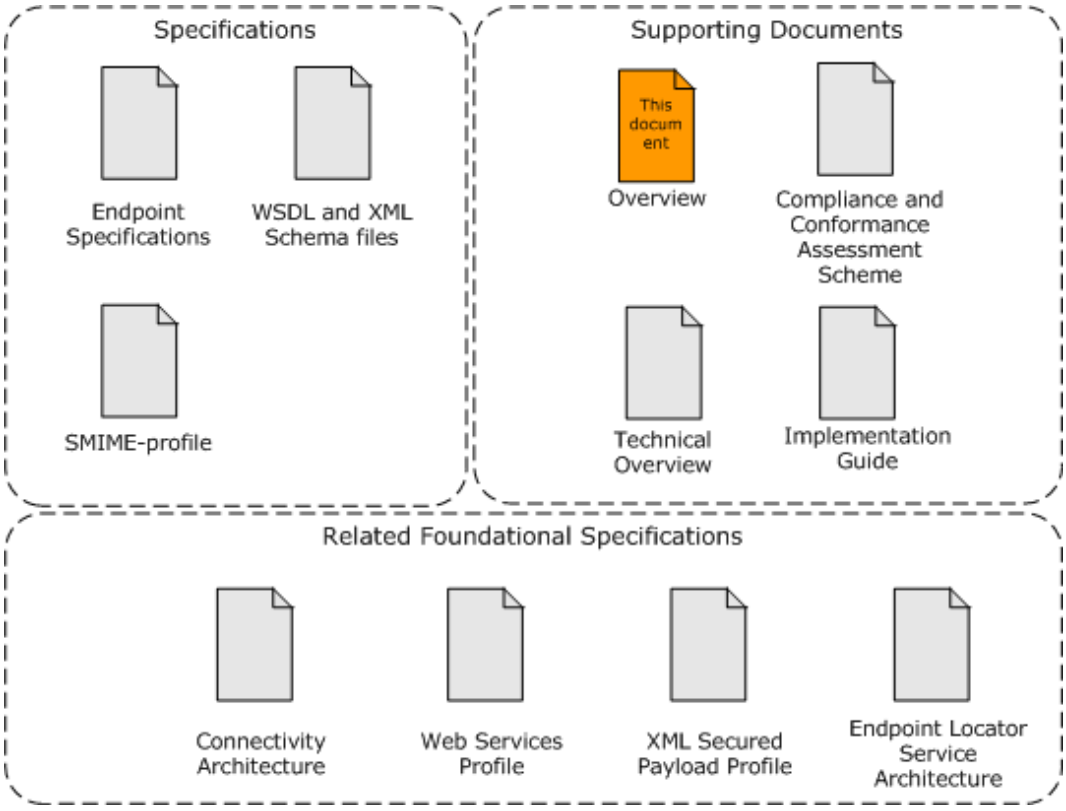


Table 1 SMD Specification – Document Map

Definitions, Acronyms and Abbreviations

For a lists of abbreviations, acronyms and abbreviations, see the Definitions section at the end of the document, on page 18.

References and Related Documents

For a list of all referenced documents, see the References at the end of the document, on page 19.

1 Introduction

1.1 Background

NEHTA has developed a set of specifications and infrastructure to support secure messaging between health care providers. While the NEHTA vision identifies end-to-end specifications for communication in specific clinical domains (e.g. pathology, discharge summary), there is a business need to implement NEHTA messaging specifications using a staged approach, and also to facilitate communication between health care providers in situations where no domain-specific standard exists.

1.2 Purpose

This document describes the implementation of secure message delivery (SMD) using NEHTA messaging specifications and infrastructure. In particular it identifies the community roles in SMD and the endpoint specifications associated with those roles. The referenced specifications define interfaces, behaviour and conformance criteria for software implementing SMD according to NEHTA specifications.

The document is intended to provide a starting point for software vendors and developers implementing the specifications.

1.3 Scope

SMD focuses on the application of NEHTA messaging specifications and the use of NEHTA infrastructure services to transfer unspecified, opaque content between health care providers. Message content is defined sufficient to support the messaging interaction. No clinical domain content is included in any content specifications.

This document provides a high-level description of the roles and interactions and provides references to detailed specifications and conformance criteria.

1.4 Overview

Section 2 defines software roles associated with community roles and identifies the detailed specifications of interfaces and behaviour. In effect, each Role encapsulates the required behaviour of a software system that implements the identified role. Description of conformance test procedures and compliance checks for implementations of the Role are also identified.

Section 3 of the document defines the context for messaging, including a community model and typical end-to-end messaging processes. The NEHTA infrastructure required to support these processes is also identified.

2 Roles

The specifications for SMD are organised by roles. Healthcare providers implement one or more of these roles, either through purchase and installation of conformant messaging software or through their own software development. The following subsections briefly describe each of the roles and identify their associated specifications.

2.1 Sender

The Sender role applies to any health care provider that sends clinical documents to another health care provider, with or without the use of Intermediaries.

Software implementing the Sender role must conform to the Sender endpoint specification documented in SMD Endpoint Specifications [SMD-ES].

In addition to the transmission of a secure payload, this specification provides an overview of various response mechanisms, including Immediate Responses, Direct Transport Responses and Indirect Transport Responses.

2.2 Receiver

The Receiver role applies to any health care provider that receives messages from other healthcare providers, with or without the use of Intermediaries.

Software implementing the Receiver role must conform to the Receiver endpoint specification in the document SMD Endpoint Specifications [SMD-ES].

2.3 Sender Intermediary

The Sender Intermediary role applies to any operator of a messaging service that sends messages on behalf of a Sender and either delivers associated transport responses back to the Sender or makes them available for retrieval by the Sender.

Software implementing the Sender Intermediary role MUST conform to the Sender Intermediary endpoint specification in the document SMD Endpoint Specifications [SMD-ES].

Note that although the interfaces offered by a Sender Intermediary for receiving messages and transport responses are the same as those used by Receivers and Senders respectively, there are additional requirements associated with intermediary behaviour, as described in [SMD-ES].

2.4 Receiver Intermediary

The Receiver Intermediary role applies to any operator of a messaging service that receives messages on behalf of a Receiver and either delivers those messages to the Receiver or makes them available for retrieval by the Receiver.

Software implementing the Receiver Intermediary role MUST conform to the Receiver Intermediary endpoint specification in the document SMD Endpoint Specifications [SMD-ES].

Note that although the interfaces offered by a Receiver Intermediary for receiving messages and transport responses are the same as those used by receivers and senders respectively, there are additional requirements associated with intermediary behaviour, as described in [SMD-ES].

3 Context

The following subsections summarise the context for SMD, describing the key roles and high-level models for message exchange. The descriptions identify responsibilities and behaviour associated with the roles. A detailed description of the roles and processes is provided in the Secure Message Delivery - Technical Overview [SMD-TO]. The set of scenarios presented is no exhaustive but introduces the key features and behaviours.

3.1 Community Model

There are four key roles in the SMD community:

- *Senders*
- *Receivers*
- *Receiver Intermediaries*
- *Sender Intermediaries*.

What follows is not an exhaustive list of potential configurations, but it explains architectural concepts in sufficient detail to be extrapolated to more complex scenarios.

Senders are health care providers wanting to send clinical documents to other health care providers, that is, Receivers. Most health care providers will operate as both senders and receivers at different times.

Intermediaries provide storage and retrieval services for senders and receivers, reducing the cost and complexity of software and hardware installed at health care provider premises. Intermediaries also implement delivery services on behalf of message senders.

In all cases, the messages are secured from Sender to Receiver through signing and encryption of the message content.

3.2 Interaction Modes

Two distinct modes of interaction are supported by the specification;

1. *Deferred mode*, which provides one-way messaging, often delivered in a store and forward fashion with no expectation of an immediate or synchronous response.
2. *Immediate mode*, which provides two-way messaging with an expectation of an immediate and synchronous response.

Deferred mode is mandatory for all roles and includes a confirmation interaction (*transport response*) to provide delivery assurance. Immediate mode is optional. The following subsections describe scenarios associated with each mode.

3.3 Deferred Mode Messaging

Referring to a messaging transaction as “deferred” concerns the separation of the interaction into two separate actions

- message transmission
- transport response transmission (confirmation of delivery).

This means that a message is transmitted by invoking a web service operation, and the receiver of that message subsequently confirms its delivery by transmitting a transport response through a separate web service invocation.

The following subsections present various scenarios associated with deferred mode messaging.

3.3.1 Direct Interaction

This interaction pattern involves the transmission of a message from a Sender to a Receiver, without the use of any intermediate services. The following diagram demonstrates the transaction sequence:

1. a message is created by a Sender
2. the Sender transmits the message to a web service hosted by a Receiver
3. after processing, a transport response is created by the Receiver
4. the Receiver transmits the transport response to a web service hosted by the Sender

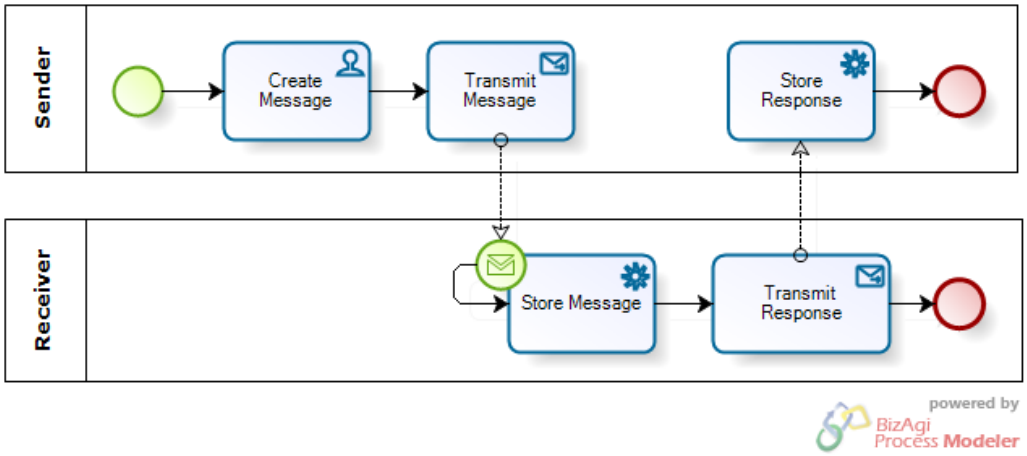


Figure 1: Deferred Mode – Direct Interaction

3.3.2 Interaction via a Receiver Intermediary

This interaction pattern involves the use of an intermediary operating on behalf of a Receiver. The transaction sequence is as follows:

1. a message is created by a Sender
2. the Sender transmits the message to a web service hosted by a Receiver Intermediary
3. The Receiver Intermediary delivers the message to the Receiver, either by:
   a) making the message available for download by the Receiver through invoking a web service hosted by the Receiver Intermediary;
   b) transmitting the message directly to a web service hosted by a Receiver.
4. after a processing delay, a transport response is created by the Receiver
5. the Receiver transmits the transport response to a web service hosted by the Receiver Intermediary

The two delivery options listed at step 3 above do not affect the overall process, but allow the receiver intermediary to satisfy multiple needs. For the first, instead of hosting web services, a Receiver uses a Receiver Intermediary to do the hosting on its behalf. Alternatively, a Receiver that does host web services itself only allows direct calls to its services by trusted parties. The

latter usage is appropriate in cases where a large organisation wants to mitigate firewall restrictions by hosting a Receiver Intermediary inside a DMZ, or in a case where messages are being exchanged between parties without a direct trust relationship.

The following diagram illustrates the process.

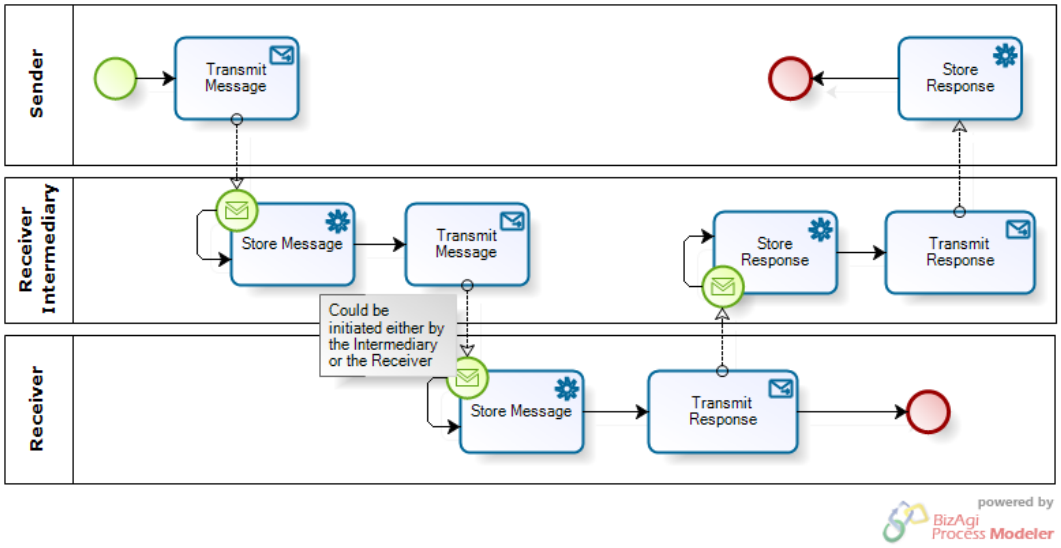


Figure 2: Deferred Mode – Interaction via one Intermediary

3.3.3 Interaction via two Intermediaries

This interaction pattern extends the previous interaction by introducing an intermediary operating on behalf of the Sender. Since the interaction between Receiver and Receiver Intermediary is identical to what was laid out in the preceding scenario, only the interaction between the Sender and the Sender Intermediary will be explained.

The Sender/Sender Intermediary interaction may represent this possible scenario: instead of invoking web services hosted by a Receiver or its Intermediary, the Sender chooses to delegate that function to an Intermediary of its own.

This interaction pattern involves the transmission of a message from a Sender to a Sender Intermediary. The Sender Intermediary transmits the message to the Receiver Intermediary by invoking a web service hosted by the Receiver Intermediary.

This scenario would be appropriate in cases where a large organisation wants to mitigate firewall restrictions by allowing messages to be transmitted only to a specific, trusted Intermediary, or in a case where messages are being exchanged between parties who use different Intermediaries.

The following diagram demonstrates the transaction sequence:

- a message is created by a Sender
- the Sender transmits the message to a web service hosted by a Sender Intermediary
- the Sender Intermediary transmits the message to a web service hosted by a Receiver Intermediary
- the Receiver Intermediary either transmits the message to a web service hosted by a Receiver, or the Receiver downloads the message by invoking a web service hosted by the Receiver Intermediary
- after a processing delay, a transport response is created by the Receiver

- the Receiver transmits the transport response to a web service hosted by the Receiver Intermediary
- the Receiver Intermediary transmits the transport response to a web service hosted by the Sender Intermediary
- the transport response is either transmitted to a web service hosted by the Sender, or the Sender downloads the transport response itself by invoking a web service hosted by the Sender Intermediary

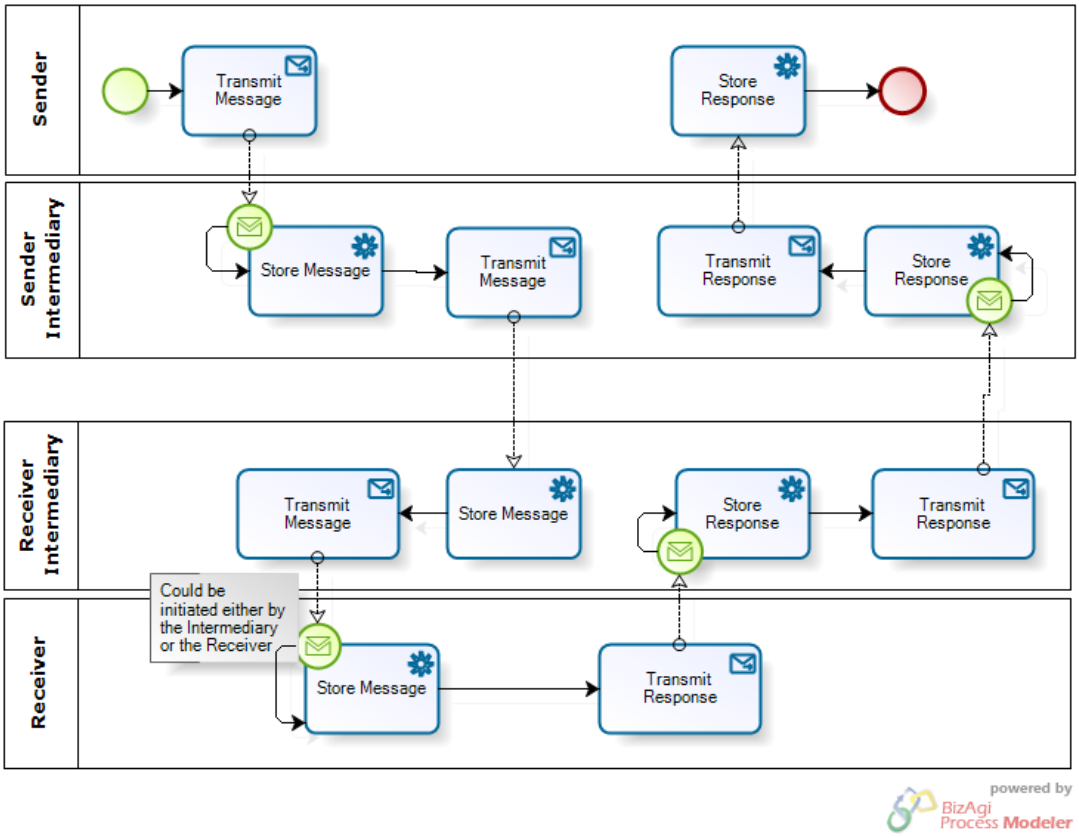


Figure 3: Deferred Mode – Interaction via two Intermediaries

3.4 Immediate Mode Messaging

Immediate Mode Messaging provides a request/response style of interaction and does not require transport responses. In other words, one transaction involves a single web service call, not two, and includes delivery of an immediate application response. The transport response is implied by the application response.

Immediate Mode Messaging is well suited to transactions such as querying repositories, in which the success of the transaction can be determined instantly based on what the query actually returns. There is no need for a separate transport response interaction.

3.4.1 Direct Interaction

This interaction pattern involves the transmission of a message (possibly a query message) from a Sender to a Receiver (possibly a repository), without the use of any intermediate services. The following diagram demonstrates the transaction sequence:

- a message is created by a Sender

- the Sender transmits the message to a web service, hosted by a Receiver
- the Receiver web service operation executes a business transaction and generates an application response that is returned immediately to the Sender.
- the Sender receives the response synchronously.
- the Sender processes the response message.

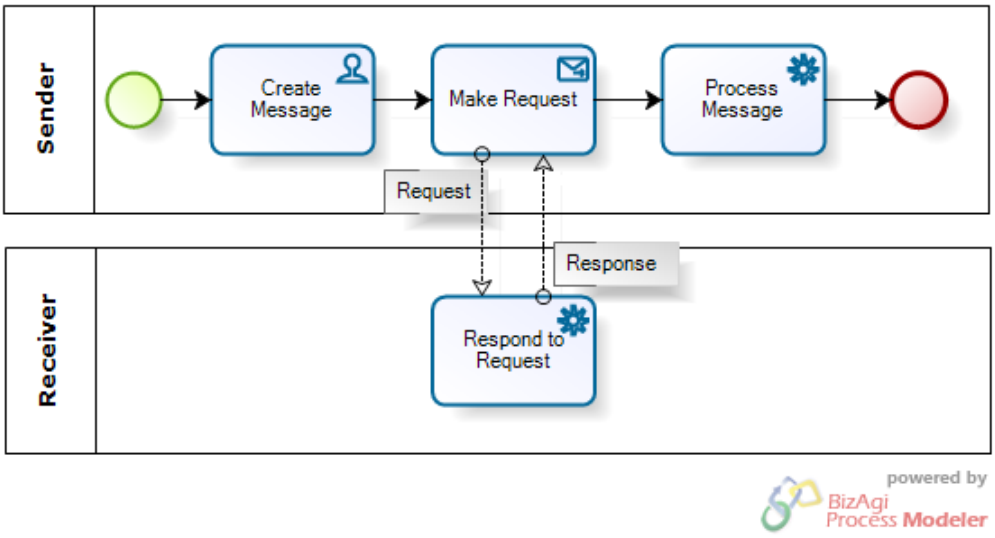


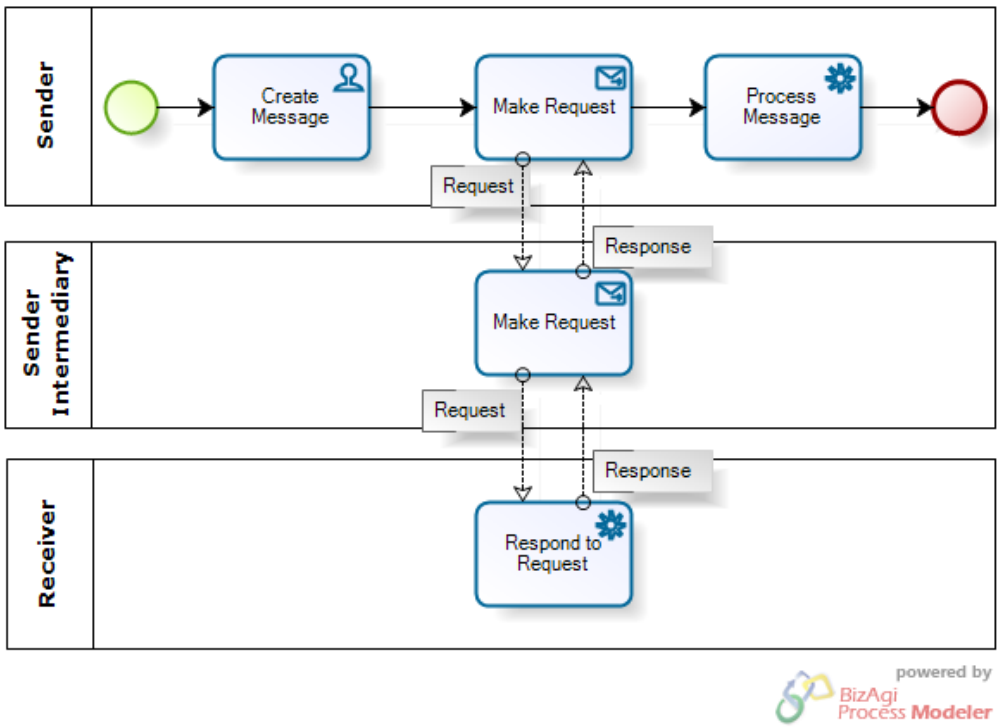
Figure 4: Immediate Mode – Direct Interaction

3.4.2 Interaction via an Intermediary

This interaction pattern involves the transmission of a message (possibly a query message) from a Sender to a Receiver (possibly a repository), through an intermediary. An intermediary would be used to mitigate issues relating to firewall traversal for either the Sender or the Receiver. For example, large healthcare organisations do not typically allow applications behind the firewall to directly invoke external services without prior arrangement. An intermediary in the DMZ or provided by a trusted third party can be used to traverse the firewall.

The following diagram demonstrates the transaction sequence:

- a message is created by a Sender
- the Sender invokes a web service hosted by a Sender Intermediary.
- the Sender Intermediary retransmits the message by invoking a web service hosted by a Receiver.
- the Receiver web service operation invoked by the Sender Intermediary executes a business transaction and generates an application response that is returned immediately to the Sender Intermediary.
- the Sender Intermediary returns that application response immediately to the Sender.
- the Sender receives the response synchronously.
- the Sender processes the response message.



-

Figure 5: Immediate Mode –Interaction via one Intermediary

4 Conformance

The Secure Message Delivery specifications define conformance for four distinct messaging roles:

1. Senders
2. Receivers
3. Sender intermediaries
4. Receiver intermediaries

A conformant secure message implementation MUST implement at least one of these roles. To conform with the Secure Message Delivery specifications an implementation:

1. MUST implement the mandatory requirements for one of these roles; and
2. MUST NOT implement any prohibited capabilities for the role.

Implementation of any of the capabilities designated by the keywords SHOULD, SHOULD NOT or MAY is optional and is not required for conformance. However if a supplier wants to claim conformance of their implementation to any optional capabilities they must implement the capabilities in the manner specified.

In addition to conformance described above any secure message delivery service MUST be operated in a manner that complies with any compliance requirements specified for the relevant role.

The process for assessment conformance and compliance is described in the Secure Message Delivery Compliance and Conformance Assessment Scheme [SMD-AS].

Definitions

This section explains the specialised terminology used in this document.

Shortened Terms

This table lists abbreviations and acronyms in alphabetical order.

Term	Description
CC	Core Connectivity
CI	Clinical Information
CT	Clinical Terminology
EHR	Electronic Health Record
ICT	Information and Communication Technology
NASH	National Authentication Service for Health
ELS	Endpoint Location Service
UHI	Unique Healthcare identifiers

Glossary

This table lists specialised terminology in alphabetical order.

Term	Description
Endpoint	Where a web service connects to the network. Source: http://www.looselycoupled.com/glossary/endpoint
Interoperability	The ability of software and hardware on multiple machines from multiple vendors to communicate. Source: The Free On-line Dictionary of Computing. Denis Howe. 21 Apr. 2008. From: Dictionary.com - http://dictionary.reference.com/browse/Interoperability
Solutions Architect	The Solutions Architect is typically responsible for matching technologies to the problem being solved. Source: http://www.developer.com
Technical Architect	The technical architect is responsible for transforming the requirements into a set of architecture and design documents that can be used by the rest of the team to actually create the solution. Source: http://www.developer.com
Business Architect	A Business Architect is anyone looks at the way work is being directed and accomplished, and then identifies, designs and oversees the implementation of improvements that are harmonious with the nature and strategy of the organisation. Source: http://www.businessarchitects.org
Development Team	The Developer writes the code for the specifications that the Development leads provide. Source: http://www.developer.com

References

This section lists NEHTA specifications and other documents that provide information for or about this document.

At the time of publication, the document versions indicated are valid. However, as all documents listed below are subject to revision, readers are encouraged to use the most recent versions of these documents.

Specification Documents

The documents listed below are part of the suite delivered in the SMD Specification.

SMD Specification Documents			
[REF]	Document Name	Publisher	Link
[SMD-O]	Secure Message Delivery - Overview	NEHTA 2009	
[SMD-TO]	Secure Message Delivery - Technical Overview	NEHTA 2009	
[SMD-ES]	Secure Message Delivery - Endpoint Specifications	NEHTA 2009	
[SMD-WX]	Secure Message Delivery Service Interface Specification WSDL and XML Schema files v1.0.	NEHTA 2009	
[SMD-AX]	Secure Message Delivery - Compliance and Conformance Assessment Scheme	NEHTA 2009	
[SMD-SPP]	Secure Message Delivery - S/MIME Payload Profile	NEHTA 2009	
[SMD-IG]	Secure Message Delivery - Implementation Guide	NEHTA 2009	To be produced

References

The documents listed below are additional documents that have been cited in this document.

Reference Documents			
[REF]	Document Name	Publisher	Link
[INTER2007]	Interoperability Framework v2.0	NEHTA 2008	http://www.nehta.gov.au/ (Home > Publications)
[NASH-PMP]	National Authentication Service for Health – Project Management Plan	NEHTA 2008	Reference in preparation for future release.
[NATA2005]	National Association of Testing Authorities, April 2005, ISO 15189 - The New Standard for Medical Testing Laboratories	NATA 2005	
[CPIS2008]	Concepts and Patterns for Implementing Services v2.0	NEHTA 2008	http://www.nehta.gov.au/ (Home > Publications)
[WSP2009]	Web Services Profile v3.1	NEHTA 2009	Reference in preparation for future release.
[XSP2009]	XML Secured Payload Profile v1.1	NEHTA 2009	
[QI2008]	Qualified Identifiers v1.0	NEHTA	

Reference Documents			
		2008	
[CA2008]	Connectivity Architecture v1.0	NEHTA 2008	http://www.nehta.gov.au/component/docman/doc_download/624-connectivity-architecture-v10-
[ELS2009]	Endpoint Locator Service	NEHTA 2009	Reference in preparation for future release.