



E-health secure message delivery



This Australian Standard® was prepared by Committee IT-014, Health Informatics. It was approved on behalf of the Council of Standards Australia on 4 December 2013.
This Standard was published on 17 December 2013.

The following are represented on Committee IT-014:

- Aged Care Association Australia
- Allied Health Professions Australia
- Australasian College of Health Informatics
- Australian and New Zealand College of Anaesthetists
- Australian Association of Pathology Practices
- Australian College of Nursing
- Australian Commission on Safety and Quality in Healthcare
- Australian Healthcare and Hospital Association
- Australian Industry Group
- Australian Information Industry Association
- Australian Institute of Health and Welfare
- Australian Institute of Radiography
- Australian Medical Association
- Australian Private Hospitals Association
- Commonwealth Department of Health
- Consumers' Federation of Australia
- Consumers' Health Forum of Australia
- CSIRO e-Health Research Centre
- Department of Health (SA)
- Department of Health (Vic.)
- Department of Health (WA)
- Department of Human Services
- Edith Cowan University
- Engineers Australia
- GS1 Australia
- Health Informatics Society of Australia
- Health Information Management Association of Australia
- HL7 Australia
- Integrating the Healthcare Enterprise Australia
- Medical Software Industry Association
- National E-Health Transition Authority
- National ICT Australia
- NSW Ministry of Health
- Queensland Health
- Royal Australian College of Medical Administrators
- Royal College of Pathologists of Australasia
- Services for Australian Rural and Remote Allied Health
- The Pharmacy Guild of Australia
- The Royal Australian and New Zealand College of Radiologists
- The University of Sydney
- University of Western Sydney

Additional Interests:

- ACT Health
- Australian Healthcare Messaging Laboratory
- Buderim Gastroenterology Centre
- CAL2CAL Australia
- Casprel
- Deontik
- DH4
- Flinders University Northern Territory
- Global Health
- Global Informatic Health
- Health Communication Network
- Healthscope
- HL7 Systems and Services
- Kestral Computing
- Lantana Group
- Laughing Mind
- Llewelyn Grain Informatics
- MacIsaac Informatics
- Macquarie Health Corporation
- Medical Objects
- Medisecure
- Michael Legg and Associates
- Montage Systems
- Norman Disney and Young
- Ocean Informatics
- Oridashi
- Primary Healthcare
- Semantic Identity
- Smart Health Solutions
- Sullivan Nicolaides Pathology
- University of Wollongong
- Victoria Avenue Medical Centre

This Standard was issued in draft form for comment as DR AS 5552.

Standards Australia wishes to acknowledge the participation of the expert individuals that contributed to the development of this Standard through their representation on the Committee and through the public comment period.

Keeping Standards up-to-date

Australian Standards® are living documents that reflect progress in science, technology and systems. To maintain their currency, all Standards are periodically reviewed, and new editions are published. Between editions, amendments may be issued.

Standards may also be withdrawn. It is important that readers assure themselves they are using a current Standard, which should include any amendments that may have been published since the Standard was published.

Detailed information about Australian Standards, drafts, amendments and new projects can be found by visiting www.standards.org.au

Standards Australia welcomes suggestions for improvements, and encourages readers to notify us immediately of any apparent inaccuracies or ambiguities. Contact us via email at mail@standards.org.au, or write to Standards Australia, GPO Box 476, Sydney, NSW 2001.

Documents

Document Sharing Hub

Australian Standard[®]

E-health secure message delivery

Originated as ATS 5822—2010.
Revised and redesignated as AS 5552—2013.

COPYRIGHT

© Standards Australia Limited

All rights are reserved. No part of this work may be reproduced or copied in any form or by any means, electronic or mechanical, including photocopying, without the written permission of the publisher, unless otherwise permitted under the Copyright Act 1968.

Published by SAI Global Limited under licence from Standards Australia Limited, GPO Box 476, Sydney, NSW 2001, Australia

ISBN 978 1 74342 641 8

PREFACE

This Standard was prepared by Standards Australia Technical Committee IT-014, Health Informatics, to supersede ATS 5822—2010, *E-health secure message delivery*.

This Standard is designed to be compatible with the implementation of ATS 5822—2010. The XML namespaces are unchanged and there have been only minor corrections to the Web Services Description Language (WSDL) and XML Schemas. The optional use of endpoints using the WS-Security and NIL Security has been removed. The changes are not expected to impact communications between implementations of ATS 5822—2010 and this Standard.

The objective of this Standard is to define an interoperable mechanism for clinical messaging over the Internet using the industry-standard Web services protocols.

Clinical messaging requires a network infrastructure, broad interconnectivity, end-to-end privacy and assurance of delivery. The Internet provides a network infrastructure that can support such messaging, but there is a need to adopt a set of standard interfaces that addresses the needs of both large and small businesses in order to ensure interconnectivity, privacy and assurance of delivery. Small businesses in particular cannot rely on significant infrastructure or technology expertise within the organization. Hence the standard interfaces need to cater for hosted services while retaining end-to-end privacy and delivery assurance.

The terms ‘normative’ and ‘informative’ have been used in this Standard to define the application of the appendix to which they apply. A ‘normative’ appendix is an integral part of a Standard, whereas an ‘informative’ appendix is for information and guidance only.

This publication has been developed with assistance from the Australian Government Department of Health. The Australian Government makes no representation or warranty that the information in this publication is correct and accurate.

Standards Australia wishes to thank the Department of Health for its continued financial support in helping to develop this Australian Standard.

CONTENTS

	<i>Page</i>
SECTION 1 SCOPE AND GENERAL	
1.1 SCOPE AND INTENDED AUDIENCE	5
1.2 OVERVIEW	5
1.3 NORMATIVE REFERENCES	6
1.4 TERMS AND DEFINITIONS	6
1.5 ACRONYMS AND ABBREVIATIONS	14
1.6 NAMESPACE PREFIXES	14
1.7 CONFORMANCE	15
SECTION 2 COMMON BEHAVIOURS	
2.1 INTRODUCTION	16
2.2 IDENTIFIERS FOR SECURE MESSAGE DELIVERY	16
2.3 WEB SERVICE PROFILES	16
2.4 PUBLIC KEY INFRASTRUCTURE (PKI)	16
2.5 DATE AND TIME VALUES	16
2.6 IDENTIFICATION	17
2.7 TRANSPORT RESPONSES	18
2.8 PRIVACY AND SECURITY	19
SECTION 3 ROLE SPECIFICATION: SENDER	
3.1 INTRODUCTION	21
3.2 IMPLEMENTATION	21
3.3 BEHAVIOUR	21
3.4 SENDING SEALED MESSAGES	22
3.5 RECEIVING TRANSPORT RESPONSES	25
SECTION 4 ROLE SPECIFICATION: RECEIVER	
4.1 INTRODUCTION	27
4.2 IMPLEMENTATION	27
4.3 BEHAVIOUR	27
4.4 RECEIVING SEALED MESSAGES	27
4.5 SENDING TRANSPORT RESPONSES	29
4.6 ENDPOINT LOCATION SERVICE PUBLICATION	30
SECTION 5 ROLE SPECIFICATION: SENDER INTERMEDIARY	
5.1 INTRODUCTION	31
5.2 IMPLEMENTATION	31
5.3 BEHAVIOUR	31
5.4 RECEIVING AND SENDING SEALED MESSAGES	32
5.5 RECEIVING AND SENDING TRANSPORT RESPONSES	33
5.6 ENDPOINT LOCATION SERVICE PUBLICATION	34
SECTION 6 ROLE SPECIFICATION: RECEIVER INTERMEDIARY	
6.1 INTRODUCTION	35
6.2 IMPLEMENTATION	35
6.3 BEHAVIOUR	35
6.4 RECEIVING AND SENDING SEALED MESSAGES	36
6.5 RECEIVING AND SENDING TRANSPORT RESPONSES	37
6.6 ENDPOINT LOCATION SERVICE PUBLICATION	38

SECTION 7 XML SCHEMAS	
7.1	MESSAGE PAYLOAD 39
7.2	SEALED MESSAGE 40
7.3	TRANSPORT METADATA EXTENSION 43
7.4	TRANSPORT RESPONSE 44
7.5	INTERACTION RECORD 46
7.6	QUALIFIED CERTIFICATE REFERENCE 47
SECTION 8 SERVICE INTERFACE: SEALED MESSAGE DELIVERY	
8.1	INTRODUCTION 48
8.2	INTERFACE 49
8.3	OPERATIONS 50
SECTION 9 SERVICE INTERFACE: SEALED IMMEDIATE MESSAGE DELIVERY	
9.1	INTRODUCTION 52
9.2	INTERFACE 53
9.3	OPERATIONS 54
SECTION 10 SERVICE INTERFACE: SEALED MESSAGE RETRIEVAL	
10.1	INTRODUCTION 56
10.2	INTERFACE 57
10.3	OPERATIONS 58
SECTION 11 SERVICE INTERFACE: TRANSPORT RESPONSE DELIVERY	
11.1	INTRODUCTION 63
11.2	INTERFACE 64
11.3	OPERATIONS 65
SECTION 12 SERVICE INTERFACE: TRANSPORT RESPONSE RETRIEVAL	
12.1	INTRODUCTION 67
12.2	INTERFACE 68
12.3	OPERATIONS 69
APPENDICES	
A	WSDL AND XML SCHEMAS FOR INTERFACE SPECIFICATIONS 74
B	SERVICE CATEGORIES 96
C	RESPONSE CODES 97
D	QUALIFIED IDENTIFIERS AND NAMESPACES 98
E	CERTIFICATE USE VALUES—SEALED MESSAGE ENCRYPTION CERTIFICATE 100
F	SAMPLE SOAP MESSAGES 101
BIBLIOGRAPHY 114	

STANDARDS AUSTRALIA

Australian Standard **E-health secure message delivery**

S E C T I O N 1 S C O P E A N D G E N E R A L

1.1 SCOPE AND INTENDED AUDIENCE

1.1.1 Scope

This Standard defines a set of roles in the Secure Message Delivery process and their associated interfaces and behaviour. The intent of these role specifications, service interfaces and behaviour is to support the transmission of electronic messages between software systems at two distinct organizations.

This Standard has the following key constraints:

- (a) This Standard is intended for transmission of message payloads from an identified sender organization to an identified receiver organization. It is not intended to provide long term storage of message payloads, or to transmit message payloads to an unknown or to-be-nominated recipient.
- (b) This Standard does not constrain the message payload, defining only the control and routing information necessary to transmit the message payload in a safe and secure manner.
- (c) This Standard does not attempt to capture business processes or business services, defining only the externally visible behaviour necessary to implement interconnected messaging.

While it is expected that Secure Message Delivery will have many applications, these constraints need to be considered when determining whether this Standard is suitable for a particular purpose.

1.1.2 Intended audience

This Standard is intended for—

- (a) solution architects who need to understand the role specifications in order to incorporate them into their designs;
- (b) developers who need to create implementations that conform to the role specifications; and
- (c) testers who need to evaluate whether an implementation conforms to the role specifications.

The reader is expected to understand XML, XML Schema, web services, Web Services Description Language (WSDL) and Public Key Infrastructure (PKI).

1.2 OVERVIEW

Common behaviours are specified in Section 2. These apply to all the role specifications, datatypes and service interfaces.

The four role specifications are detailed in Sections 3–6.

The datatypes specified in Section 7 are used by all the role specifications and service interfaces; these service interfaces are specified in Sections 8–12.

WSDL and datatypes, corresponding to the datatypes and service interfaces specified in Sections 7–12, are listed in Appendix A.

NOTES:

- 1 Example response codes are listed in Appendix C.
- 2 Example qualified identifiers and namespaces are listed in Appendix D.
- 3 Example certificate use values are listed in Appendix E.
- 4 Example SOAP messages are listed in Appendix F.

1.3 NORMATIVE REFERENCES

The following are the normative documents referenced in this Standard:

AS

5550 E-health web services profiles

5551 E-health payload profiles

IETF

RFC3986 Uniform Resource Identifiers: Generic Syntax
<http://www.ietf.org/rfc/rfc3986.txt>

W3C

WSDL2001 W3C, Web Services Description Language (WSDL) 1.1, W3C Note, 15 March 2001.

<<http://www.w3.org/TR/2001/NOTE-wsdl20010315> >

XSD2004a XML Schema Part 1: Structures Second Edition. W3C Recommendation 28 October 2004

<http://www.w3.org/TR/2004/REC-xmlschema-1-20041028/>

XSD2004b XML Schema Part 2: Datatypes Second Edition. W3C Recommendation 28 October 2004

<http://www.w3.org/TR/2004/REC-xmlschema-2-20041028/>

NOTE: Documents for informative purposes are listed in the Bibliography.

1.4 TERMS AND DEFINITIONS

For the purposes of this document, the following terms and definitions apply.

1.4.1 Application response

1.4.1.1 Definition

Data sent from the receiver organization back to the sender organization, in response to a message payload that was sent from the sender organization to the receiver organization.

NOTE: Whether application responses are used, and what data they contain, is defined by the business processes using Secure Message Delivery. Therefore the contents of application responses, and whether they are used or not, are outside the scope of this Standard.

1.4.1.2 Principles

Application responses can be handled differently by the two modes, as follows:

- (a) In immediate mode, the application response can be transmitted from the Receiver to the Sender in a sealed message in the SOAP response.
- (b) In deferred mode, application responses need to be transmitted as a new instance of the Message Delivery process that sends the application response in the other direction (i.e. reversing the roles of sender organization and receiver organization).

1.4.1.3 *Message acknowledgements*

This Standard is content agnostic, due to the end-to-end encryption of the sealed message. Handshakes and transport acknowledgements included in this Standard occur below layer seven (the application layer) of the OSI network protocol stack (ISO/IEC 7498-1). When transmitted by this Standard, message content will still require layer seven acknowledgements that are content specific. Clinical content will generally require at least a content specific application level acknowledgement and will optionally require layer seven delivery acknowledgements.

A typical example is HL7 Version 2 messages, which have a mandatory application level acknowledgement that is message type specific, content specific triggers that initiate workflow, and optional level seven delivery acknowledgements. While the form and content of layer seven acknowledgements are beyond the scope of this Standard, they are still required when using this Standard as the transport protocol, to ensure the Sender is informed as to whether there is an appropriate application at the Receiver endpoint that is capable of processing the transmitted semantic content, and implements the associated workflow.

1.4.2 **Authorization**

Authorization of communicating role instances is the responsibility of the role instances. This Standard identifies points at which authorization needs to be applied, but is not explicit about authorization mechanisms or policies.

NOTE: Authorization mechanisms and policies are outside the scope of this Standard, as are mechanisms for delegating to an authorized agent and for determining legitimate authorized agents.

1.4.3 **Endpoint location service**

Interaction records can be published to, and obtained from, an Endpoint Location Service. Roles that wish to invoke a service provider instance can obtain the interaction record for it by looking it up using the desired target, service category (payload scheme) and service interface.

Endpoint location services are an important part of the infrastructure for supporting the Message Delivery process in wide-spread deployments involving multiple organizations.

NOTES:

- 1 Further information about endpoint location services can be found in ATS 5546.
- 2 This Standard recommends publishing interaction records to an endpoint location service. Whether endpoint location services are used by a deployment, which endpoint location service to use, and how roles find that endpoint location service are outside the scope of this Standard.

1.4.4 **Interaction record**

Technical information needed by a service invoker instance to invoke a service provider instance.

An interaction record contains the following:

- (a) *Target*—identifies the receiver organization for operations that deliver sealed messages.
- (b) *Service category*—identifies the business process associated with service invocations.

It is expected that service category values will be defined by the specifications that define the use of Secure Message Delivery with particular message payloads.

NOTES:

- 1 Service category specifications and examples are described in Appendix B.
- 2 Service category is referred to as payload scheme in ATS 5546. The term ‘service category’ has been retained in this Standard to avoid changes to the WSDL and XML schemas.

- (c) *Service interface*—identifies the service interface for the service invocations.
Values for service interfaces are defined in Clauses 8.1.2.2, 9.1.2.2, 10.1.2.2, 11.1.2.2 and 12.1.2.2.
- (d) *Service endpoint*—the location for invoking the service provider instance.
- (e) *Service provider*—the organization operating the service provider instance, possibly on behalf of the target.
- (f) *Qualified certificate references*—a set of paired fields, as follows:
 - (i) Certificate use qualifier—value indicating purpose of the certificate reference.
NOTE: Values for certificate use qualifiers can be found in Appendix E.
 - (ii) Certificate reference—value indicating a certificate to use.

NOTES:

- 1 The interaction records used for delivering a sealed message are expected to contain one qualified certificate reference that identifies the certificate to be used for encrypting the sealed message. The other interaction records are expected to contain zero qualified certificate references.
- 2 Further information about interaction records can be found in ATS 5546.
- 3 This Standard refers to the use of values from interaction records. How a role obtains an interaction record is outside the scope of this Standard; however, one possible method is to obtain it from an endpoint location service.

1.4.5 Message Delivery process

1.4.5.1 Definition

The process of transmitting a message payload from a Sender to a Receiver, and providing the Sender with confirmation that the transmission was successful.

Secure Message Delivery uses a set of roles to perform the Message Delivery process.

Confirmation of a successful transmission in Secure Message Delivery means that a copy of the message payload has been received by the Receiver. In normal operation, exactly one copy will be received. However, there is no guarantee that more than one copy will not be received. If a guarantee of exactly one copy is required, the guarantee will have to be provided by the application using Secure Message Delivery.

The absence of a confirmation of a successful transmission does not mean that a copy has not been received by the Receiver. It is possible that one or more copies of the message payload could have been received.

The Message Delivery process can be used to guarantee that at least one copy of the message payload will be delivered to the Receiver by having the Sender repeat the process until it has obtained successful confirmation of delivery. The Message Delivery process can be used to prevent more than one copy of the message payload being processed by the Receiver, by having the Receiver detect and ignore the duplicates.

1.4.5.2 Identification

An invocation identifier uniquely identifies an instance of the Message Delivery process. Invocation identifiers are always assigned by a Sender, who initiates the Message Delivery process. The invocation identifier is then used by all the role instances involved in that instance of the Message Delivery process.

NOTE: An instance of the Message Delivery process involves one or more SOAP Web services invocations, so an invocation identifier will correspond to one or more SOAP invocations. Therefore, an invocation identifier does not uniquely identify SOAP invocations or SOAP messages.

1.4.5.3 *Roles in the Message Delivery process*

The deployment of role implementations will determine which role instances are involved in each particular instance of the Message Delivery process.

Every instance of the Message Delivery process will always involve exactly one Sender, zero or more Sender Intermediaries, zero or more Receiver Intermediaries, and exactly one Receiver role instance. The simplest scenario involves direct transmission from a Sender to a Receiver—without involving any intermediaries.

Typical scenarios that involve intermediaries will usually involve no more than one Sender Intermediary and no more than one Receiver Intermediary—for example, one Sender, one Sender Intermediary, one Receiver Intermediary and one Receiver.

NOTE: Deployments involving more than one Sender Intermediary or more than one Receiver Intermediary are permitted, but require additional routing mechanisms, which are outside the scope of this Standard.

1.4.5.4 *Terminology*

1.4.5.4.1 *Deliver*

The transmission of data directly from one role to another role, where the first role is responsible for performing the transmission. The first role is the service invoker. The second role is the service provider.

1.4.5.4.2 *Forward*

The transmission of data either by delivering it or by making it available for retrieving. The choice will depend on the role, since only some roles have service providers to make data available for retrieval.

1.4.5.4.3 *Retrieve*

The transmission of data directly from one role to another role, when the second role is responsible for performing the transmission. The first role is a service provider that makes the data available for retrieval. The second role is the service invoker.

1.4.5.4.4 *Send and receive*

These terms are informally used, and do not imply which service interface is being used.

1.4.6 **Message payload**

The data being transmitted in the Message Delivery process.

NOTE: The mechanisms defined in this Standard work with any data format. The format of the message payload is outside the scope of this Standard.

1.4.7 **Modes**

Each instance of the Message Delivery process can function in one of the following two modes:

- (a) *Deferred mode*—where the Message Delivery process delivers a sealed message using a series of SOAP invocations, and the status is conveyed using a separate series of SOAP invocations. Therefore the status of the Message Delivery process is not known until the separate SOAP invocations conveying the status information are completed.
- (b) *Immediate mode*—where the Message Delivery process delivers a sealed message using the SOAP request, and the status is conveyed in the SOAP response of the same SOAP invocation. Therefore, the status of the Message Delivery process is known immediately at the conclusion of the SOAP invocation that delivers the sealed message. Immediate mode requires the Receiver role instances to have service provider instances.

The support for deferred mode is mandatory, but support for immediate mode is optional.

1.4.8 Organization

1.4.8.1 *Authorized agent*

Organization authorized to act on behalf of a sender organization or a receiver organization.

It will be obvious when the sender/receiver organization is not associated with the Sender/Receiver role instance, since the certificate used for communicating with the Sender/Receiver role instance will not be the sender/receiver organization's certificate. It will be the certificate of another organization. However, determining whether that other organization is a legitimate authorized agent for that sender/receiver organization is beyond the scope of this Standard.

1.4.8.2 *Intermediary organization*

Organization contracted by a sender organization or receiver organization to assist it with the Message Delivery process.

1.4.8.3 *Receiver organization*

Where the message payload is being transmitted to by the Message Delivery process.

Receiver organizations can be represented legitimately by the Receiver organization's authorized agents. For example, an authorized agent could be an application service provider operating on behalf of the Receiver organization.

1.4.9 Roles

1.4.9.1 *General*

Used to specify the required behaviour of parties involved in a message delivery interaction. Four roles are used for the delivery of messages.

The roles in Secure Message Delivery are as follows:

- (a) *Sender*—the role that is sending a message payload.
- (b) *Receiver*—the role that is the recipient of the message payload.
- (c) *Sender Intermediary*—a role that performs functions on behalf of a Sender.
- (d) *Receiver Intermediary*—a role that performs functions on behalf of a Receiver.

In this Standard, the following terms pertain to roles:

- (i) *Role specification*—the definition of a role. A role is defined by its behaviours, which are specified as conformance points. In this Standard, roles are constructed from services. Therefore, the behaviours in a role specification consist of service provider specifications, service invoker specifications and additional, role-specific conformance points.
- (ii) *Role implementation*—software that conforms to a role specification.
- (iii) *Role instance*—deployment of a role implementation.

1.4.9.2 *Sender role*

Associated with either a sender organization or an authorized agent for the sender organization.

1.4.9.3 *Receiver role*

Associated with either a receiver organization or an authorized agent for the receiver organization.

1.4.9.4 *Sender Intermediary role*

Typically associated with an intermediary organization contracted by the receiver organization. However, can also be associated with the sender organization or an authorized agent for the sender organization.

1.4.9.5 *Receiver Intermediary role*

Typically associated with an intermediary organization contracted by the receiver organization. However, can also be associated with the receiver organization or an authorized agent for the receiver organization.

NOTES:

- 1 Software can implement one or more role specifications. For example, software can implement both Sender Intermediary and Receiver Intermediary roles.
- 2 Each deployment of software is associated with a single organization. It is possible for an organization to have multiple deployments of software, with each deployment containing different sets of role instances.

1.4.10 **Sealed message**

1.4.10.1 *Definition*

A message payload that has been digitally signed and then encrypted, along with sealed message metadata.

1.4.10.2 *Purpose*

A sealed message seals the message payload to address issues of tampering and revelation. The sealed message's digital signature does not prevent tampering, but provides a mechanism that helps the Receiver to detect if the message payload has been modified after it was signed. A digital signature can also be used to authenticate the Sender. Encryption defends against the contents of the message payload being accessed by any party without the key to decrypt it.

Message payloads are transmitted as sealed messages to protect them from unauthorized parties. These unauthorized parties include any Sender Intermediaries and Receiver Intermediaries. Although they play a role in the Message Delivery process, Sender Intermediaries and Receiver Intermediaries are precluded from accessing the contents of the message payload or tampering with it.

The sealed message metadata is protected only by Transport Layer Security (TLS) and not by the signing and encryption of the sealed message, so it can be accessed and modified by those who have access to the sealed message. Sealed message metadata is intended purely for routing purposes.

1.4.10.3 *Identifying sealed messages*

There is no single value that identifies instances of sealed messages. The Message Delivery process functions without requiring sealed messages to be explicitly identified.

Although the sealed message metadata contains an invocation identifier, that value identifies an instance of the Message Delivery process and not any particular sealed message. The invocation identifier does not uniquely identify sealed messages. This is clearly illustrated in immediate mode when two different sealed messages, in the request and the response, both have the same invocation identifier.

1.4.11 **Sender organization**

Where the message payload is being transmitted from by the Message Delivery process.

Sender organizations can be represented legitimately by the Sender organization's authorized agents. For example, an authorized agent could be an application service provider operating on behalf of the Sender organization.

1.4.12 Services

In this Standard, the following terms pertain to services:

- (a) A *service interface*, which is a contract between a service provider and a service invoker. It comprises the following:
 - (i) A *service provider specification*—the definition of how to provide a service, specified as a set of conformance points.
 - (ii) A *service invoker specification*—the definition of how to use a service, specified as a set of conformance points.

NOTE: The behaviours of a service interface are grouped into one or more operations.

- (b) A *service implementation*, which is one or both of the following:
 - (i) A *service provider*—software that conforms to a service provider specification.
 - (ii) A *service invoker*—software that conforms to a service invoker specification.
- (c) A *service instance*, which is one or both of the following:
 - (i) A *service provider instance*—deployment of a service implementation.
 - (ii) A *service invoker instance*—deployment of a service invoker instance.
- (d) *SOAP Web services*—This Standard uses SOAP Web services as profiled by AS 5550. In this profile, an *invocation* consists of a SOAP *request* sent from a service invoker to the service provider, followed by a SOAP *response* sent from the service provider to the service invoker. A special type of response for indicating errors is a SOAP *fault*.

SOAP Web services can be secured using Transport Layer Security.

1.4.13 Shall

Indicates that a statement is mandatory.

1.4.14 Should

Indicates a recommendation.

1.4.15 Transport responses

1.4.15.1 Definition

Used to indicate the status of the Message Delivery process; used in deferred mode, and not in immediate mode.

1.4.15.2 Identification

A transport response is uniquely identified by its transport response identifier.

A transport response can be used in one or more SOAP Web services invocations, so a transport response identifier will correspond to one or more SOAP invocations. Therefore, a transport response identifier does not uniquely identify SOAP invocations or SOAP messages.

1.4.15.3 Types

1.4.15.3.1 General

There are two types of transport responses: final transport responses and intermediate transport responses.

1.4.15.3.2 *Final transport responses*

Final transport responses indicate that the Message Delivery process has been successful or that an error has occurred. A final transport response indicating success can only be created by the Receiver, but a final transport response indicating an error can be created by Sender Intermediaries, Receiver Intermediaries and Receivers.

The status provided by final transport responses reflects imperfect knowledge of a distributed system.

A final transport response indicating success always means that the Message Delivery process has delivered the message payload to the Receiver.

A final transport response created by the Receiver indicating an error means that the message payload was not successfully delivered. However, a final transport response that was created by a Sender Intermediary or Receiver Intermediary indicating an error means only that successful delivery of the message payload is unlikely—it does not mean that the message payload will not arrive at the Receiver. For example, if the SOAP request was processed, but the SOAP response did not arrive back, the service invoker might treat this as an error, even though, unknown to it, the message payload was delivered. Similarly, if a final response is not forwarded, this does not imply that the message payload was not delivered.

Support for final transport responses is mandatory. Therefore, in the deferred mode Message Delivery process, final transport responses will always be created by the Receiver and forwarded to the Sender. Final transport responses will be delivered to every role identified to be delivered to those roles.

1.4.15.3.3 *Intermediate transport responses*

Intermediate transport responses can be used to indicate additional status information. They can be created by Sender Intermediaries, Receiver Intermediaries and Receivers.

Support for intermediate transport responses is optional. Therefore, a role instance can ask for them, but there is no guarantee that the other role instances will create or forward them. The only guarantee is that role instances that do not want them to be delivered will not get them.

1.4.15.4 *Delivery of transport responses*

A role instance determines where transport responses are to be transmitted using the ordered list of route records in the sealed message metadata. As a sealed message is forwarded from the Sender through Sender Intermediaries and Receiver Intermediaries, route records are appended to the sealed message metadata. The route records indicate the service instances to which transport responses are to be sent.

Since support for final transport responses is mandatory, final transport responses will be transmitted to all the service provider instances identified by the list of route records, in reverse order to the order in which they were added.

Intermediate transport responses are not guaranteed to be transmitted. Although the list of route records is used in reverse order, some or all of them could be skipped. This is because support for intermediate transport responses is optional.

1.5 ACRONYMS AND ABBREVIATIONS

CRL	Certificate Revocation List
OCSP	Online Certificate Status Protocol
PKI	Public Key Infrastructure
TLS	Transport Layer Security
URI	Uniform Resource Identifier
URL	Uniform Resource Location
URN	Uniform Resource Name
UUID	Universally Unique Identifier
WSDL	Web Services Description Language
XML	Extensible Markup Language

1.6 NAMESPACE PREFIXES

The following prefixes are used in this Standard to refer to the WSDL namespaces and XML namespaces listed:

ds	http://www.w3.org/2000/09/xmldsig#
ep	http://ns.electronichealth.net.au/xsp/xsd/EncryptedPayload/2010
ir	http://ns.electronichealth.net.au/els/xsd/DataTypes/2010
msg	http://ns.electronichealth.net.au/smd/xsd/Message/2010
qcr	http://ns.electronichealth.net.au/qcr/xsd/QualifiedCertificate/2010
simd	http://ns.electronichealth.net.au/smd/svc/SealedImmediateMessageDelivery/2010
smd	http://ns.electronichealth.net.au/smd/svc/SealedMessageDelivery/2010
smr	http://ns.electronichealth.net.au/smd/svc/SealedMessageRetrieval/2010
smsg	http://ns.electronichealth.net.au/smd/xsd/SealedMessage/2010
sp	http://ns.electronichealth.net.au/xsp/xsd/SignedPayload/2010
trd	http://ns.electronichealth.net.au/smd/svc/TransportResponseDelivery/2010
trr	http://ns.electronichealth.net.au/smd/svc/TransportResponseRetrieval/2010
trsp	http://ns.electronichealth.net.au/smd/xsd/TransportResponse/2010
xsd	http://www.w3.org/2001/XMLSchema

1.7 CONFORMANCE

1.7.1 Interpretation of conformance points

A conformance point is a provision or possible action against which the conformance of a system can be attested. A requirement, indicated by the use of the word 'shall', is mandatory for compliance with this Standard. A recommendation, indicated by the word 'should', provides best practice solutions that are not mandatory.

1.7.2 Dimensions of conformance

This Standard has many possible dimensions of conformance.

Conformance dimensions can be applied to different products, such as role implementations (e.g. software) and role instances (e.g. deployments of software).

For example, conformance dimensions for role implementations could be defined by specifying these conformance parameters:

- (a) The roles which are supported. One or more of—
 - (i) Sender;
 - (ii) Receiver;
 - (iii) Sender Intermediary; and
 - (iv) Receiver Intermediary.
- (b) For each role, the modes supported. Exactly one of—
 - (i) deferred mode; or
 - (ii) deferred mode and immediate mode.
- (c) For each role (except the Receiver), whether it—
 - (i) accepts intermediate transport responses; or
 - (ii) does not accept intermediate transport responses.

SECTION 2 COMMON BEHAVIOURS

2.1 INTRODUCTION

This Section contains conformance points for common behaviours.

The conformance points in this Section apply to the four role specifications in Sections 3–6, the XML Schemas in Section 7 and the five service interfaces in Sections 8–12.

2.2 IDENTIFIERS FOR SECURE MESSAGE DELIVERY

This Standard can be identified by the following URI:

`http://ns.electronichealth.net.au/smd/pkg/2010`

NOTE: This identifier is not used in the Message Delivery process. It has been defined for use by other specifications to identify Secure Message Delivery.

2.3 WEB SERVICE PROFILES

2.3.1 Web service profiles for service providers

The following conformance point applies to roles when providing a service provider:

The role shall have the service provider conform to both the Web Services Base Profile and the TLS Profile from AS 5550.

2.3.2 Web service profiles for service invokers

The following conformance point applies to roles when providing a service invoker:

The role shall have the service invoker conform to both the Web Services Base Profile and the TLS Profile from AS 5550.

2.4 PUBLIC KEY INFRASTRUCTURE (PKI)

In Secure Message Delivery, certificates are used to secure sealed messages (both signing and encrypting them) and to establish the transport security of service invocations.

The following conformance points apply to roles when handling PKI X.509v3 certificates. They provide recommendations for handling certificates to ensure that the PKI is used in a scalable and robust manner while maintaining a reasonable degree of security.

- (a) The role should conform to RFC 5280 for the management of certificates.
- (b) The role should cache certificate status information that has been obtained using a CRL for the period of time recommended by the CRL.
- (c) The role should cache certificate status information that has been obtained using the OCSP for the period of time recommended by the OCSP nextUpdate field.
- (d) The role should not contact the certificate issuer each time a certificate is used (i.e. certificate checks should occur out-of-band wherever possible).

2.5 DATE AND TIME VALUES

2.5.1 Time zone

The following conformance point applies to roles when setting the value of XML elements whose datatype is `xsd:dateTime`:

All `xsd:dateTime` elements defined in the XML Schemas of this Standard shall be transmitted as time-zoned values as defined in XSD2004b, Clause 3.2.7. That is, the value needs to indicate its time zone explicitly.

2.5.2 Comparing date and time values

Allowances should be made for possible clock skew and transmission delays when comparing date and time values that were obtained from different role instances. Clock skew arises when two role instances use two different clocks. Transmission delays arise because of the time it takes for data to traverse the network connecting two role instances.

In the absence of any external guarantees about clock synchronization and transmission delays, role instances cannot assume that date and time values can be directly compared.

In a situation where a creation time has been provided by a creation role instance, another role instance can safely assume that the clock skew plus transmission delay will not be greater than the difference between the indicated creation time and the local time at the consumer role instance when the data arrived at the consumer role instance. This is always guaranteed because data can never arrive before it was created.

An example might be a role instance that receives at 3:15pm (according to its local clock) data containing an indicated creation time of 3:00pm and an indicated expiry time of 3:05pm (both according to the other role instance's clock). The difference between the indicated creation time and the received local time is 15 minutes. The Receiver has no way of knowing how much of this is due to a difference between clocks or how much it is due to transmission delays. Although the Receiver cannot determine exactly when the expiry time occurs, it will be correct to treat the expiry time as having passed by 3:20pm (according to its local clock)—it might have passed sometime before 3:20pm (perhaps even before it received the data), but it definitely will not pass any later than 3:20pm.

2.6 IDENTIFICATION

2.6.1 Qualified identifiers

Identifiers are needed to identify organizations, individuals, instances of the Message Delivery process and transport responses; URIs can satisfy this need.

To support subsequent requirements, a qualified identifier is defined as the following:

- (a) A qualified identifier shall match the 'URI' production as defined in Section 3 of RFC3986.
- (b) Two qualified identifiers shall be equal if and only if their literal string values are equal.

2.6.2 Schemes for qualified identifiers

The following conformance points apply to qualified identifier creators and qualified identifier consumers:

- (a) If the qualified identifier creator publishes or identifies a scheme for qualified identifiers that it has created, that scheme shall define how to split a qualified identifier into a qualifier and an identifier, and also indicate whether or not qualified identifier consumers are permitted to split the identifiers.
- (b) The qualified identifier consumer shall not split a qualified identifier unless explicitly permitted by the scheme identified or published by the qualified identifier creator.

NOTE: For qualified identifiers based on URLs, further information and recommendations are provided in Appendix D.

2.6.3 Identifiers for organizations

The following conformance point applies to roles when identifying organizations participating in the Message Delivery process (these identifiers are used in sealed message metadata and transport response metadata):

The role shall identify organizations using a qualified identifier as defined in Clause 2.6.1.

2.6.4 Identifiers for Message Delivery processes and transport responses

The following conformance points apply to roles when creating identifiers for instances of the Message Delivery process and transport responses:

- (a) The creating role shall create a qualified identifier as the invocation identifier and transport response identifier. See Clause 2.6.1.
- (b) The creating role shall ensure that invocation identifiers and transport response identifiers are unique across the community of role instances.
- (c) The creating role should create invocation identifiers and transport response identifiers as exactly one of the following options:
 - (i) A UUID encoded as a URN according to RFC 4122.
 - (ii) A URL based on a domain name registered by the creating role instance and an identifier that is unique at the creating role instance.

2.7 TRANSPORT RESPONSES

2.7.1 Delivering transport responses using route records

The term ‘corresponding sealed message’ refers to a sealed message that the role has received with the same invocation identifier as that indicated in the transport response. Sender Intermediaries and Receiver Intermediaries need to keep track of sealed messages received to ensure they can deliver corresponding transport responses.

The following conformance points apply to roles when delivering transport responses (in Secure Message Delivery, they apply to Receivers, Receiver Intermediaries and Sender Intermediaries):

- (a) If the transport response is a final transport response and there is at least one route record in the corresponding sealed message, the role shall deliver the final transport response to the service provider instance indicated by the last route record of the corresponding sealed message.
- (b) If the transport response is an intermediate transport response and there is at least one route record in the corresponding sealed message, the role should deliver it to the service provider instance indicated by the route record closest to the end of the corresponding sealed message that has indicated that intermediate transport responses can be sent to it.
- (c) If the transport response is an intermediate transport response, the role shall not deliver it to any service provider instance in the route records of the corresponding sealed message where the route record indicates intermediate transport responses are not wanted.

NOTE: These conformance points allow a role instance that does not wish to be delivered intermediate transport responses to be skipped. This allows role instances to opt out of being delivered intermediate transport responses without blocking the path for other role instances that wish to be delivered intermediate transport responses.

2.7.2 Receiving transport responses

The following conformance point applies to roles that expect to be delivered intermediate transport responses:

Roles that support being delivered intermediate transport responses shall be capable of being delivered zero or more transport responses corresponding to a single invocation identifier.

2.8 PRIVACY AND SECURITY

2.8.1 Privacy of sealed messages

The following applies to roles when determining whether a sealed message can be sent (they always apply to Senders; in immediate mode, they also apply to Receivers, for the response sealed message):

- (a) It is advisable for the role not to forward a sealed message if the privacy obligations of the role relating to the message payload are not satisfied. Privacy obligations are defined in the *Privacy Act 1988* (Cwlth) and in relevant state and territory legislation.
- (b) It is advisable for the role not to forward a sealed message if the encryption certificate used to create the sealed message is not valid.
- (c) It is advisable for the role not to forward a sealed message if the encryption certificate used to create the sealed message does not identify the receiver organization (or sender organization, in the case of the response sealed message) or their authorized agent in a manner sufficient to satisfy privacy obligations.

NOTE: Items (b) and (c) highlight two situations in which the privacy obligations might not be satisfied, but additional rules could apply to the role.

2.8.2 Confidentiality of sealed messages

The following items, (a) to (d), apply to roles when handling sealed messages they have received.

Transport-level certificate management associated with the invocation of Sender Intermediary interfaces is adequately covered by AS 5550, and the PKI conformance points in Clause 2.4. The following additional suggestions outline the steps associated with storage and the supplier interfaces:

- (a) The Sender is recommended to ensure that the decrypted content (i.e. the message payload) of response sealed messages is handled in a manner that prevents unauthorized access.
- (b) The Receiver is recommended to ensure that the decrypted content (i.e. the message payload) of sealed messages is handled in a manner that prevents unauthorized access.
- (c) The Sender Intermediary is recommended to not decrypt any sealed messages. In other words, in the unlikely event of the Sender Intermediary having a copy of the Receiver's private key, using this key to decrypt any sealed messages would violate this point.
- (d) The Receiver Intermediary is recommended to not decrypt any sealed messages. In other words, in the unlikely event of the Receiver Intermediary having a copy of the Receiver's private key, using this key to decrypt any sealed messages would violate this point.

2.8.3 Certificate validity

The following applies to roles when determining whether a certificate is valid or not:

It is suggested that the role determine whether a certificate is valid or not according to a defined set of conditions for certificate validity.

NOTE: It is outside the scope of this Standard to specify the conditions for certificate validity. Those conditions need to take into account many factors—for example, type of certificates involved, deployment environment, and business purpose. The mechanisms specified by RFC 5280 could be used as the basis for specifying conditions for certificate validity.

2.8.4 Acceptance of transport security

2.8.4.1 Service providers

The following conformance points apply to service providers when using a transport security binding and determining whether to process an invocation request:

- (a) The service provider shall not accept a service request where the transport security mechanism cannot be securely established.
- (b) The service provider should not accept a service request where the service invoker instance's transport security certificate (the TLS client certificate) is not valid (see Clause 2.8.3).
- (c) The service provider shall not accept a service request if the service invoker instance's transport security certificate does not identify the expected service invoker instance or an authorized agent of the service invoker instance.

2.8.4.2 Service invokers

The following conformance points apply to service invokers when using a transport security binding and determining whether to process an invocation response:

- (a) The service invoker shall not accept the response where the transport security mechanism cannot be securely established.
- (b) The service invoker should not accept the response where the service provider instance's transport security certificate (the TLS server certificate) is not valid (see Clause 2.8.3).
- (c) The service invoker shall not accept the response if the service provider instance's transport security certificate does not identify the expected service provider instance or an authorized agent of the service provider instance.

2.8.5 Acceptance of sealed messages

The following conformance points apply to roles when determining whether to accept a sealed message the roles have received (they apply to Receivers and Senders: Receivers when processing a sealed message they have received, either delivered or retrieved in deferred mode, or delivered in immediate mode; and Senders when processing a response sealed message):

- (a) The role shall not accept the sealed message when its digital signature cannot be successfully verified.
- (b) The role should not accept the sealed message when the sealed message's signing certificate is not valid. (See Clause 2.8.3.)
- (c) The role shall not accept the sealed message when the digital signature's certificate does not identify the sender organization (or receiver organization in the case of the response sealed message) or the sender organization's authorized agent in a manner sufficient to satisfy privacy obligations.

SECTION 3 ROLE SPECIFICATION: SENDER

3.1 INTRODUCTION

This Section serves as the role specification for the Sender role.

In the Message Delivery process, Senders send message payloads for sender organizations to receiver organizations. They support the functionality described in Clause 3.2 and Clause 3.3. They create a sealed message with the message payload and forward it, either direct to the Receiver or via Sender Intermediaries and/or Receiver Intermediaries (Clause 3.4). The Senders are also forwarded transport responses that indicate the status of the Message Delivery process (Clause 3.5).

For example, this role could be implemented in software installed at a general practice clinic that sends referrals to a specialist practice.

For additional conformance points that apply to Senders, see Section 2.

3.2 IMPLEMENTATION

The following conformance points apply to Senders:

- (a) The Sender shall have a Sealed Message Delivery service invoker in conformance with Section 8.
- (b) If the Sender supports immediate mode, the Sender shall have a Sealed Immediate Message Delivery service invoker in conformance with Section 9.
- (c) The Sender shall have at least one of the following options:
 - (i) A Transport Response Delivery service provider in conformance with Section 11.
 - (ii) A Transport Response Retrieval service invoker in conformance with Section 12.

3.3 BEHAVIOUR

The following conformance points apply to Senders.

The Sender shall act as follows:

- (a) The Sender shall obtain the message payload to be delivered (designers of message payloads need to take note of Clause 3.4.2).
- (b) The Sender shall determine the service provider instance to invoke (Clause 3.4.3), which also determines whether deferred mode or immediate mode is used.
- (c) The Sender shall create a new instance of the Message Delivery process (Clause 3.4.4).
- (d) The Sender shall create a new sealed message to deliver (Clause 3.4.5).
- (e) The Sender shall deliver the sealed message (Clause 3.4.6).
- (f) If using immediate mode, the Sender shall process the response sealed message that is returned (Clause 3.4.7).

- (g) The Sender shall, if using deferred mode, handle transport responses as follows:
 - (i) Be delivered transport responses (Clause 3.5.2) or retrieve transport responses (Clause 3.5.3).
 - (ii) Process transport responses (Clause 3.5.4).
 - (iii) Detect when expected transport responses are not received (Clause 3.5.5).

3.4 SENDING SEALED MESSAGES

3.4.1 General

The conformance points in Clause 3.4 specify the required behaviour of a Sender when delivering a message payload.

3.4.2 Message payload

The following applies to Senders when obtaining the message payload to deliver:

If the Sender is the creator of the message payload, it is advisable to ensure that the receiver organization is identified as the Message Delivery process recipient in the contents of the message payload.

NOTE: This identification aims to ensure that there is no confusion of responsibility if the message payload is subsequently transmitted (i.e. the second recipient can detect that it had been retransmitted). Addressing information is carried in the sealed message metadata, but that information is not signed by the sealed message and it is not usually visible to clinicians. It is acknowledged that where the Sender is not able to manipulate the message payload, it might not be possible to apply this control.

3.4.3 Determining service invocation

The following conformance points apply to Senders when determining how they will deliver a message payload:

- (a) The Sender shall deliver message payloads by exactly one of the following options—
 - (i) invoking a Sealed Message Delivery deliver operation; or
 - (ii) invoking the Sealed Immediate Message Delivery deliver operation.

NOTES:

- 1 If the Sender does not support immediate mode, then option (ii) is not available to it.
- 2 These operations will be on a service provider instance either nominated by the Sender (in which case it will be on a Sender Intermediary) or nominated by the Receiver (in which case it will be on a Receiver or Receiver Intermediary).

- (b) The Sender should obtain from an Endpoint Location Service the interaction record or equivalent that indicates the service provider instance that the Receiver has nominated for being delivered the type of message payload that the Sender is delivering.

NOTE: Interaction records will indicate whether Sealed Immediate Message Delivery service instances or Sealed Message Delivery service instances are available.

3.4.4 Message Delivery process

The following conformance point applies to Senders when creating a new instance of the Message Delivery process:

The Sender shall assign a new invocation identifier for the new instance of the Message Delivery process in conformance with Clause 2.6.4.

See also Clause 2.8.1 in relation to the message delivery process.

3.4.5 Sealed message

In this Clause, the term ‘the sealed message’ refers to the sealed message created by conformance point (a) in Clause 3.4.5.

The following conformance points apply to Senders when creating a new sealed message for an instance of the Message Delivery process:

- (a) The Sender shall create a new sealed message for the Message Delivery process in conformance with Clause 7.2.3.
- (b) The sealed message shall contain the message payload being sent by the Message Delivery process. (See Clause 3.4.2.)
- (c) Expiry time—
 - (i) if the Sender is delivering the sealed message in deferred mode, the sealed message shall have an expiry time indicating the date and time by which a final transport response for the Message Delivery process is expected to arrive; and
 - (ii) if the Sender is delivering the sealed message in immediate mode, the sealed message shall not have an expiry time.
- (d) The sealed message shall use the invocation identifier of the instance of the Message Delivery process. (See Clause 3.4.4.)
- (e) Service category value—
 - (i) the sealed message shall contain a service category value that corresponds to the message payload; and
 - (ii) the service category value in conformance point 3.4.5(e)(i) should be a health industry-standard service category value.

NOTE: See Appendix B.
- (f) Service interface value—
 - (i) if the Sender is delivering the sealed message in deferred mode, the service interface value of the sealed message shall be the value defined in Clause 8.1.2.2; and
 - (ii) if the Sender is delivering the sealed message in immediate mode, the service interface value of the sealed message shall be the value defined in Clause 9.1.2.2.
- (g) Route records—
 - (i) if the Sender is delivering the sealed message in deferred mode, the sealed message shall have exactly one route record that identifies a Transport Response Delivery service instance, such that—
 - (A) if the Sender intends to be delivered transport responses on its Transport Response Delivery service interface (see conformance point 3.2(c)(i)), the route record should identify that service provider instance; and
 - (B) if the Sender is delivering the sealed message to a Sender Intermediary, the route record should identify that Sender Intermediary’s Transport Response Delivery service provider instance; and
 - (ii) if the Sender is delivering the sealed message in immediate mode, the sealed message shall not contain any route records.

- (h) If the Sender is delivering the sealed message in immediate mode, the sealed message shall be signed with a certificate that can also be used for encrypting data. This is so that the Receiver can use that certificate to encrypt the response sealed message.

NOTE: The Transport Response Delivery service provider instance in the route record is provided by a role instance that could be a Sender Intermediary that the sealed message is being sent to, a Sender Intermediary that the sealed message is not being sent to, or the Sender itself. If the role instance is not the Sender itself, the Sender would need to obtain the transport responses from that role instance (e.g. retrieving them using the Transport Response Retrieval service interface).

3.4.6 Delivering the sealed message

The following conformance point applies to Senders when delivering the sealed message:

The Sender shall attempt to deliver the sealed message created in conformance with Clause 3.4.5 by invoking the service provider instance determined in Clause 3.4.3.

3.4.7 Immediate response handling

The following conformance points apply to Senders when handling sealed messages received in the response to an invocation of the Sealed Immediate Message Delivery deliver operation:

- (a) If the sealed message in the response is successfully decrypted and accepted, the Sender shall ensure that the contained message payload is made available to an application or individual that can take appropriate action in relation to the message payload.
- (b) If the sealed message in the response cannot be successfully decrypted or is not accepted, the Sender shall ensure that a record of the response is stored such that a responsible person can determine that an error has occurred. The intent of this requirement is to ensure that the status of the instance of the Message Delivery process is accessible to the sender organization: the nature of the user interface is not constrained and might provide significantly more information.
- (c) If the sealed message in the response cannot be successfully decrypted or is not accepted, the Sender should escalate the issue to a responsible person.

Refer to Clause 2.8.5 for additional conformance points on when a sealed message can be accepted.

3.4.8 Local handling and storage

Refer to Clause 2.8.2 for additional suggestions on handling the decrypted data from the response sealed message.

3.4.9 Failures

3.4.9.1 Failure behaviour

The following conformance points apply to Senders when the invocation to deliver a sealed message is not successful (see Clause 3.4.9.2):

- (a) If an invocation is not successful, the Sender shall perform exactly one of the following options:
 - (i) Escalate the issue to a responsible person.
 - (ii) Retry delivering the sealed message. The retry is another invocation, so if it also fails then this conformance point also applies to it and the Sender will need to decide whether to escalate or retry again.

- (b) The Sender should not retry delivering the sealed message after the expiry time indicated in the sealed message metadata has been passed.

NOTE: This limits the length of time that service provider instances need to retain information to detect duplicate sealed messages. A service provider could reject all sealed messages after their expiry time, regardless of whether they are duplicate sealed messages or not.

- (c) If the delivery of a sealed message is retried, the Sender shall reuse the sealed message from the original invocation in conformance with Clause 7.2.4.

3.4.9.2 Definition of invocation success

The following conformance points apply to Senders when determining whether an invocation is successful or not:

- (a) If a Sender receives an 'ok' response, the Sender shall treat the invocation as successful.
- (b) If a Sender receives a 'duplicate' response and the Sender was retrying a previous invocation, the Sender shall treat the invocation as successful.
- (c) If a Sender receives a transport response (final or intermediate) where the invocation identifier corresponds to an instance of the Message Delivery process where the Sender has attempted to deliver the sealed message, the Sender shall treat all invocations of the Sealed Message Delivery `deliver` operation for that instance of the Message Delivery process as successful. This means it has to stop any retries of the corresponding sealed message as per conformance point 3.4.9.1(a).

3.5 RECEIVING TRANSPORT RESPONSES

3.5.1 General

The conformance points in Clause 3.5 specify the required behaviour of a Sender when being delivered transport responses.

3.5.2 Direct transport response receipt

The following conformance point applies to Senders when being delivered transport responses on its Transport Response Delivery service provider instance:

The Sender shall be delivered transport responses at the Transport Response Delivery service provider instance identified in the sealed message of conformance point 3.4.5(g)(i)(A).

3.5.3 Indirect transport response receipt

The following conformance points apply to Senders when retrieving transport responses from a Sender Intermediary:

- (a) The Sender shall attempt to retrieve transport responses at defined intervals by invoking the Transport Response Retrieval `retrieve` operation of its nominated Sender Intermediary.
- (b) The Sender shall remove transport responses from the Sender Intermediary, by invoking the Transport Response Retrieval `remove` operation on it, after they have been successfully retrieved and processed.

NOTE: The nominated Sender Intermediary is determined by agreement between the Sender and the Sender Intermediary. Usually it will be the Sender Intermediary of conformance point 3.4.5(g)(i)(B).

3.5.4 Local handling and storage

The following conformance points apply to Senders when processing transport responses that have been forwarded to them:

- (a) The Sender shall ensure that a record of transport responses is stored such that a responsible person can determine whether a message payload has been successfully delivered to the Receiver. The intent of this requirement is to ensure that the status of the Message Delivery process is accessible to the sender organization: the nature of the user interface is not constrained and might provide significantly more information.
- (b) If the Sender processes a final transport response that indicates that an error occurred, the Sender should escalate the issue to a responsible person.
- (c) If the invocation identifier associated with a transport response does not match any Message Delivery process delivery attempts by the Sender, the Sender should escalate the issue to a responsible person.

3.5.5 Non-receipt of transport responses

The following conformance point applies to Senders when a final transport response for a sealed message they have sent has not been received by them:

If the Sender has not received a final transport response for a sealed message it has sent by the expiry time indicated in the sealed message, the Sender should escalate the issue to a responsible person.

SECTION 4 ROLE SPECIFICATION: RECEIVER

4.1 INTRODUCTION

This Section serves as the role specification for the Receiver role.

In the Message Delivery process, Receivers are sent message payloads for receiver organizations from sender organizations. They support the functionality described in Clause 4.2 and Clause 4.3. They are forwarded sealed messages, either directly from the Sender or indirectly via Sender Intermediaries and/or Receiver Intermediaries (Clause 4.4). They also create and deliver transport responses (Clause 4.5).

For example, the Receiver could be implemented in software installed in a specialist practice to receive referrals from general practice clinics.

Additional conformance points that apply to Receivers are found in Section 2.

4.2 IMPLEMENTATION

The following conformance points apply to Receivers:

- (a) The Receiver shall have one or both of the following options:
 - (i) A Sealed Message Delivery service provider in conformance with Section 8.
 - (ii) A Sealed Message Retrieval service invoker in conformance with Section 10.
- (b) If the Receiver supports immediate mode, the Receiver shall have a Sealed Immediate Message Delivery service provider in conformance with Section 9.
- (c) The Receiver shall have a Transport Response Delivery service invoker in conformance with Section 11.

4.3 BEHAVIOUR

The following conformance points apply to Receivers. The Receiver shall act as follows:

- (a) Depending on the options in conformance point 4.2(a)—
 - (i) The Receiver shall be delivered sealed messages (Clause 4.4.2.1); and/or
 - (ii) The Receiver shall retrieve sealed messages (Clause 4.4.2.2).
- (b) If immediate mode is supported, the Receiver shall be delivered sealed messages and respond with a response sealed message (Clause 4.4.3).
- (c) The Receiver shall create and deliver transport responses (Clause 4.5).

4.4 RECEIVING SEALED MESSAGES

4.4.1 General

The conformance points in Clause 4.4 specify the required behaviour of a Receiver for being forwarded sealed messages.

4.4.2 Deferred mode

4.4.2.1 Direct message receipt

The following conformance point applies to Receivers that have chosen to have the Sealed Message Delivery service provider as per conformance point 4.2(a)(i):

The Receiver shall be delivered sealed messages via the Sealed Message Delivery service provider instance(s) published in an Endpoint Location Service.

4.4.2.2 Indirect message receipt

The following conformance point applies to Receivers that have chosen to have the Sealed Message Retrieval service invoker as per conformance point 4.2(a)(ii):

The Receiver shall attempt to retrieve sealed messages at defined intervals by invoking operations on the Sealed Message Retrieval service provider instance of its nominated Receiver Intermediary.

NOTE: The nominated Receiver Intermediary is determined by agreement between the Receiver and the Receiver Intermediary. Usually it will be the Receiver Intermediary published according to the advice in Clause 4.6.1.

4.4.3 Immediate mode

4.4.3.1 Service provision

The following conformance points apply to Receivers that have chosen to provide the Sealed Immediate Message Delivery service provider as per conformance point 4.2(b):

- (a) The Receiver shall be forwarded sealed messages and respond with response sealed messages via the Sealed Immediate Message Delivery service interface(s) published in an endpoint location service.
- (b) If the Receiver is responding with a response sealed message, it shall be in conformance with Clause 4.4.3.2.

If the Receiver is responding with a response sealed message, refer to Clause 2.8.1 for additional suggestions.

Refer to Clause 2.8.5 for additional conformance points relating to when a sealed message can be accepted.

4.4.3.2 Response sealed message

The Sealed Immediate Message Delivery interface responds with a response sealed message, whose existence also indicates that the message payload was delivered. As such, no transport response is required for sealed messages delivered in this manner.

In this Clause, the term 'response sealed message' refers to the sealed message created by conformance point 4.4.3.2(a).

The following conformance points apply to Receivers when creating a response sealed message:

- (a) The Receiver shall create a new sealed message for the response in conformance with Clause 7.2.3.
- (b) The response sealed message should contain an application response as its message payload. That is, the response should not be synthesized by the Message Delivery process, but should be an application response to the message payload.
- (c) The response sealed message should not have an expiry time.
- (d) The response sealed message shall have the same invocation identifier as the invocation identifier in the corresponding request sealed message. They are both a part of the same instance of the Message Delivery process.

- (e) If the `smmsg:senderIndividual` from the request sealed message exists, the response sealed message shall use that value as the receiving individual at the organization to which the response sealed message will be sent (i.e. as the receiver individual for the response sealed message).
- (f) The response sealed message shall use the value of the `smmsg:senderOrganisation` from the request sealed message as the qualified identifier value for the organization to which the response sealed message will be sent (i.e. as the receiver organization for the response sealed message).
- (g) The response sealed message should not have a sending individual. The intent of the immediate mode response is to carry a response that would not be explicitly generated by an individual.
- (h) The response sealed message shall use the value of the `smmsg:receiverOrganisation` from the request sealed message as the qualified identifier value for the organization creating the response sealed message (i.e. as the sender organization for the response sealed message).
- (i) The response sealed message shall use the value of the `smmsg:serviceCategory` element from the request sealed message as its service category value.
- (j) The response sealed message shall use the value of the `smmsg:serviceInterface` element from the request sealed message as its service interface value.
- (k) The response sealed message shall not contain any route records.
- (l) The response sealed message shall be encrypted using the signing certificate of the request sealed message, if it is suitable for encryption.

4.4.4 Local handling and storage

The following conformance point applies to Receivers when handling sealed messages they have received:

If the sealed message is successfully decrypted and accepted, the Receiver shall ensure that the contained message payload is made available to an application or individual that can take appropriate action in relation to the message payload.

Refer to Clause 2.8.2 for additional suggestions on handling the decrypted data from the request sealed message.

4.5 SENDING TRANSPORT RESPONSES

4.5.1 General

The conformance points in Clause 4.5 specify the required behaviour of a Receiver for creating and delivering transport responses.

4.5.2 Service invocation

The following conformance points apply to Receivers when invoking the Transport Response Delivery `deliver` operation:

- (a) The Receiver shall create exactly one final transport response for each unique instance of the Message Delivery process (as indicated by the invocation identifier in received sealed messages) in conformance with Clause 7.4.3, and deliver it in conformance with Clause 2.7.1.
- (b) If the Receiver supports the creation of intermediate transport responses, the Receiver shall deliver all the intermediate transport responses it creates in conformance with Clause 2.7.1.

4.5.3 Failures

The following conformance points apply to Receivers when handling the response to an invocation of the Transport Response Delivery `deliver` operation:

- (a) If an invocation of the Transport Response Delivery `deliver` operation fails, the Receiver should perform exactly one of the following options:
 - (i) Escalate the issue to a responsible person.
 - (ii) Retry delivering the transport response(s). The retry is another invocation, so if it also fails then this conformance point also applies to it, and the service invoker will need to decide whether to escalate or retry again.
- (b) If the delivery of a transport response is retried, the Receiver shall use the same transport response in conformance with Clause 7.4.4.

4.6 ENDPOINT LOCATION SERVICE PUBLICATION

4.6.1 Publication

The following is suggested to ensure that message payload types (indicated by service category values) supported by Receiver role instances are adequately identified in an endpoint location service, allowing a Sender or Sender Intermediary to determine what message payloads can be sent:

It is advisable for the Receiver role instance to ensure publication of interaction records identifying its Sealed Message Delivery, and (if supported) Sealed Immediate Message Delivery service provider instances in an endpoint location service.

4.6.2 Interaction records

In the following conformance points, the Receiver obligations apply to the Receiver's Intermediary if the Receiver has delegated its publication responsibility as advised in conformance point 6.6.1(b):

- (a) If the service provider instance is the deferred mode Sealed Message Delivery service provider instance, the Receiver shall set a service category in the interaction record to identify the type of message payload that can be transmitted to that identified service provider instance.
- (b) If the service provider instance is the immediate mode Sealed Immediate Message Delivery service provider instance, the Receiver shall set a service category in the interaction record to identify the types of message payloads transmitted to and from that identified service provider instance.
- (c) Where more than one service category is supported by the Receiver, the Receiver shall publish a distinct interaction record for each supported service category.
- (d) The Receiver should use service category identifiers nominated by a standards organization or similar industry body in all published interaction records.

NOTE: It is permitted to have multiple interaction records that refer to the same service provider instance.

As noted in Clause 1.4.4, the definition of the format of message payloads is outside the scope of this Standard. The mechanisms defined by conformance points 4.6.2(a), (b), (c) and (d) provide a means for identification and standardization of message payloads without constraining them. It should also be noted that the service interface identifiers in interaction records distinguish the interfaces through which this content might be delivered.

The service interface identifiers for each interface are defined in the relevant interface specifications: Clause 8.1.2.2 for deferred mode; and Clause 9.1.2.2 for immediate mode.

SECTION 5 ROLE SPECIFICATION: SENDER INTERMEDIARY

5.1 INTRODUCTION

This Section serves as the role specification for the Sender Intermediary role.

In the Message Delivery process, Sender intermediaries assist Senders by providing services that allow those Senders to function with a limited network presence or minimal directory capability, or without directly hosting Web services. They support the functionality described in Clause 5.2 and Clause 5.3. They can relay sealed messages (Clause 5.4). They can also relay transport responses (Clause 5.5).

For example, this role could be implemented by a messaging gateway service acting on behalf of a general practice clinic that sends referrals to specialist practices.

Additional conformance points that apply to Sender Intermediaries are found in Section 2.

NOTE: Messaging gateway services will typically implement both Sender Intermediary and Receiver Intermediary roles.

5.2 IMPLEMENTATION

The following conformance points apply to Sender Intermediaries:

- (a) The Sender Intermediary shall have a Sealed Message Delivery service provider in conformance with Section 8.
- (b) The Sender Intermediary shall have a Sealed Message Delivery service invoker in conformance with Section 8.
- (c) If the Sender Intermediary supports immediate mode, it shall have a Sealed Immediate Message Delivery service provider in conformance with Section 9.
- (d) If the Sender Intermediary supports immediate mode, it shall have a Sealed Immediate Message Delivery service invoker in conformance with Section 9.
- (e) The Sender Intermediary shall have a Transport Response Delivery service provider in conformance with Section 11.
- (f) The Sender Intermediary shall have a Transport Response Delivery service invoker in conformance with Section 11.
- (g) The Sender Intermediary shall have a Transport Response Retrieval service provider in conformance with Section 12.

NOTE: The Sender Intermediary can be forwarded and can forward sealed messages: in deferred mode because of (a) and (b); and in immediate mode because of (c) and (d). The Sender Intermediary can be delivered and can forward transport responses because of (e), (f) and (g).

5.3 BEHAVIOUR

The following conformance points apply to Sender Intermediaries:

- (a) The Sender Intermediary shall be delivered and deliver sealed messages in deferred mode (Clause 5.4.2).
- (b) If immediate mode is supported, the Sender Intermediary shall be delivered and deliver sealed messages in immediate mode (Clause 5.4.3).
- (c) The Sender Intermediary shall be delivered and forward transport responses (Clause 5.5).

5.4 RECEIVING AND SENDING SEALED MESSAGES

5.4.1 General

The conformance points in Clause 5.4 specify the required behaviour of a Sender Intermediary for being delivered and delivering sealed messages.

5.4.2 Deferred mode

The following conformance points apply to a Sender Intermediary in relation to its Sealed Message Delivery service provider:

- (a) Upon successful receipt of a sealed message on its Sealed Message Delivery service provider instance, the Sender Intermediary shall attempt to deliver a modified sealed message to the receiver organization by using exactly one of the following options:
 - (i) If the Sender Intermediary is also a Receiver Intermediary for the nominated Receiver, forward the sealed message as defined for a Receiver Intermediary as per Clause 6.4 (in particular conformance point 6.4.2(a));
 - (ii) Deliver the sealed message to a Sealed Message Delivery service provider instance nominated by the Receiver; or
 - (iii) Deliver the sealed message to another Sender Intermediary.
- (b) The modified sealed message in conformance point 5.4.2(a) shall be the same sealed message (in conformance with Clause 7.2.4) with exactly one of the following options:
 - (i) If the Sender has already included a route record for the Sender Intermediary's Transport Response Delivery service provider instance, no additional route record needs to be appended; or
 - (ii) If the Sender has already included a route record for the Sender Intermediary's Transport Response Delivery service provider instance, with exactly one additional route record appended for the Sender Intermediary's Transport Response Delivery service provider instance.
- (c) If invoking an operation to deliver a sealed message received on its Sealed Message Delivery interface fails, the Sender Intermediary shall perform exactly one of the following options:
 - (i) Assume that the sealed message was not delivered to the Receiver, and then both—
 - (A) create a final transport response indicating an error occurred in conformance with Clause 7.4.3; and
 - (B) forward that final transport response according to conformance point 5.5.2(d); or
 - (ii) Retry delivering the sealed message.
 NOTE: The retry is another invocation, so if it also fails then this conformance point also applies to it and the service invoker will need to decide whether to treat it as an error or retry again.
- (d) If a sealed message received on a Sealed Message Delivery interface cannot be delivered to the Receiver, the Sender Intermediary shall indicate that an error has occurred according to conformance point 5.4.2(c)(i) (i.e. create a final transport response and forward it).

5.4.3 Immediate mode

The following conformance points apply to a Sender Intermediary in relation to its Sealed Immediate Message Delivery service provider:

- (a) When the Sender Intermediary receives an invocation on its Sealed Immediate Message Delivery service provider, it shall attempt to forward the same sealed message (in conformance with Clause 7.2.4) by invoking a Sealed Immediate Message Delivery deliver operation nominated by the Receiver, and pass the response from that invocation back to the invoker as its response.
- (b) If an invocation of the Sealed Immediate Message Delivery deliver operation fails, the Sender Intermediary shall perform exactly one of the following options:
 - (i) Respond to the original invocation with a fault.
 - (ii) Retry delivering the sealed message. The retry is another invocation, so if it also fails then this conformance point also applies to it and the service invoker will need to decide whether to respond to the original invocation with a fault or retry again.

5.4.4 Local handling and storage

Refer to Clause 2.8.2 for additional suggestions that apply to the handling of sealed messages.

5.5 RECEIVING AND SENDING TRANSPORT RESPONSES

5.5.1 General

The conformance points in Clause 5.5 specify the required behaviour of Sender Intermediaries for being delivered and delivering transport responses.

5.5.2 Service invocation

The following conformance points apply to the Sender Intermediary handling invocations of its Transport Response Delivery service instance:

- (a) Upon successful receipt of a final transport response on its Transport Response Delivery service provider (which will be from a Receiver, Receiver Intermediary or another Sender Intermediary), the Sender Intermediary shall forward it according to conformance point 5.5.2(d).
- (b) Upon successful receipt of an intermediate transport response on its Transport Response Delivery service provider (which will be from a Receiver, Receiver Intermediary or another Sender Intermediary), the Sender Intermediary should forward it according to conformance point 5.5.2(d).
- (c) If the Sender Intermediary supports the creation of intermediate transport responses, the Sender Intermediary shall forward all the intermediate transport responses it creates in conformance with conformance point 5.5.2(d).
- (d) The Sender Intermediary shall forward the transport response to the sender organization by exactly one of the following options:
 - (i) Make the transport response available for retrieval by the sender organization through its Transport Response Retrieval service provider.
 - (ii) Deliver the transport response in conformance with Clause 2.7.1.

5.5.3 Local handling and storage

The following conformance point applies to Sender Intermediaries when they are handling transport responses they have been delivered and are making them available according to conformance point 5.5.2(d)(i):

The Sender Intermediary should not remove a transport response from storage unless the Sender has invoked the `remove` operation for that transport response.

5.6 ENDPOINT LOCATION SERVICE PUBLICATION

5.6.1 Publication

The following conformance point relates to publication to service directories:

The Sender Intermediary should publish an interaction record identifying its Transport Response Retrieval service provider instance in an endpoint location service.

NOTE: This interaction record is not used in the Message Delivery process, but could be used to assist with the deployment of Sender role instances.

5.6.2 Service category

The following conformance point relates to the service category value:

If the Sender Intermediary is publishing an interaction record identifying its Transport Response Retrieval service provider instance in an endpoint location service, the Sender Intermediary shall use the following service category identifier in that interaction record:

`http://ns.electronichealth.net.au/smd/sc/TransportResponseRetrieval/2010`

SECTION 6 ROLE SPECIFICATION: RECEIVER INTERMEDIARY

6.1 INTRODUCTION

This Section is the role specification for the Receiver Intermediary role.

In the Message Delivery process, Receiver Intermediaries assist Receivers by providing services that allow those Receivers to function with a limited network presence or without directly hosting Web services. Receiver Intermediaries support the functionality described in Clause 6.2 and Clause 6.3. They can relay sealed messages (Clause 6.4). They can also relay transport responses (Clause 6.5).

For example, this role could be implemented by a messaging gateway service acting on behalf of a specialist clinic that is sent referrals from general practice clinics. Messaging gateway services will typically implement both Sender Intermediary and Receiver Intermediary roles.

Additional conformance points that apply to Receiver Intermediaries are found in Section 2.

6.2 IMPLEMENTATION

The following conformance points apply to Receiver Intermediaries:

- (a) The Receiver Intermediary shall have a Sealed Message Delivery service provider in conformance with Section 8.
- (b) The Receiver Intermediary shall have a Sealed Message Retrieval service provider in conformance with Section 10.
- (c) The Receiver Intermediary shall have a Sealed Message Delivery service invoker in conformance with Section 8.
- (d) If the Receiver Intermediary supports immediate mode, the Receiver Intermediary shall have a Sealed Immediate Message Delivery service provider in conformance with Section 9.
- (e) If the Receiver Intermediary supports immediate mode, the Receiver Intermediary shall have a Sealed Immediate Message Delivery service invoker in conformance with Section 9.
- (f) The Receiver Intermediary shall have a Transport Response Delivery service provider in conformance with Section 11.
- (g) The Receiver Intermediary shall have a Transport Response Delivery service invoker in conformance with Section 12.

NOTE: The Receiver Intermediary can be delivered and forward sealed messages: in deferred mode because of (a), (b) and (c); and in immediate mode because of (d) and (e). The Receiver Intermediary can be delivered and can deliver transport responses because of (f) and (g).

6.3 BEHAVIOUR

The following conformance points apply to Receiver Intermediaries:

- (a) The Receiver Intermediary shall be delivered and shall forward sealed messages in deferred mode (Clause 6.4.2).
- (b) If immediate mode is supported, the Receiver Intermediary shall be delivered and deliver sealed messages in immediate mode (Clause 6.4.3).
- (c) The Receiver Intermediary shall be delivered and deliver transport responses (Clause 6.5).