



Pathology Result Reporting

Endpoint Specifications

Version 3.0 Draft — 30 June 2009

National E-Health Transition Authority Ltd

Level 25

56 Pitt Street

Sydney, NSW, 2000

Australia.

www.nehta.gov.au**Disclaimer**

NEHTA makes the information and other material ('Information') in this document available in good faith but without any representation or warranty as to its accuracy or completeness. NEHTA cannot accept any responsibility for the consequences of any use of the Information. As the Information is of a general nature only, it is up to any person using or relying on the Information to ensure that it is accurate, complete and suitable for the circumstances of its use.

Document Control

This document is maintained in electronic form. The current revision of this document is located on the NEHTA Web site and is uncontrolled in printed form. It is the responsibility of the user to verify that this copy is of the latest revision.

Copyright © 2009, NEHTA.

This document contains information which is protected by copyright. All Rights Reserved. No part of this work may be reproduced or used in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or information storage and retrieval systems—without the permission of NEHTA. All copies of this document must include the copyright and other information contained on this page.

Document Information

Change History

Version	Date	Comments
3.0 Draft	2009-06-30	NEHTA Draft for Comment
2.1	2008-09-04	NEHTA Correction
2.0	2008-09-01	NEHTA Package v1.0 Draft update
1.0 Draft	2008-08-27	NEHTA Internal Draft

Table of Contents

Document Information	iii
Change History	iii
Table of Contents	iv
Preface	1
Document Purpose	1
Scope	1
Intended Audience.....	1
Document status	1
Document Map.....	2
References and Related Documents	2
Definitions, Acronyms and Abbreviations.....	2
Conformance	2
Overview	2
1 Common Behaviours	4
1.1 Introduction.....	4
1.2 Web Services Profile.....	4
1.3 Public Key Infrastructure	4
1.4 Authorisation	4
1.5 Identification.....	4
1.5.1 Endpoints	4
1.5.2 Documents and Invocations.....	5
1.6 Assured Delivery	5
2 Endpoint: Sender	6
2.1 Introduction.....	6
2.1.1 Purpose	6
2.1.2 Overview	6
2.2 Pathology Result Report Delivery	6
2.2.1 Service Invocation	6
2.2.2 Payload	7
2.2.3 Privacy and Authentication	7
2.2.4 Failures	7
2.3 Acknowledgement Receipt	7
2.3.1 Implementation	7
2.3.2 Direct Acknowledgement Receipt.....	8
2.3.3 Indirect Acknowledgement Receipt	8
2.3.4 Local Handling and Storage	8
2.3.5 Privacy and Authentication	9
2.3.6 Failures	9
3 Endpoint: Receiver	10
3.1 Introduction.....	10
3.1.1 Purpose	10
3.1.2 Overview	10
3.2 Pathology Result Report Receipt	10
3.2.1 Implementation	10
3.2.2 Direct Pathology Result Report Receipt.....	11
3.2.3 Indirect Pathology Result Report Receipt	11
3.2.4 Local Handling and Storage	11
3.2.5 Privacy and Authentication	11
3.3 Acknowledgement Delivery	12
3.3.1 Service Invocation	12
3.3.2 Payload	12

3.3.3	Privacy and Authentication	12
3.3.4	Failures	13
4	Endpoint: Intermediary	14
4.1	Introduction	14
4.1.1	Purpose	14
4.1.2	Overview	14
4.2	Common Intermediary Conformance Points	14
4.2.1	Delivery	14
4.2.2	Privacy and Authentication	15
4.3	Pathology Result Report Receipt and Supply	15
4.3.1	Implementation	15
4.3.2	Endpoint publication	15
4.3.3	Local Handling and Storage	15
4.4	Acknowledgement Receipt and Supply	16
4.4.1	Implementation	16
4.4.2	Endpoint publication	16
4.4.3	Local Handling and Storage	16
5	WSDL: Common Components.....	17
5.1	Introduction	17
5.2	Namespace	17
5.2.1	XML Schema Namespace.....	17
5.3	ELS Publication Requirements.....	17
5.4	XML Schemas.....	17
5.4.1	XSD: Pathology Result Report	17
5.4.2	XSD: Sealed Pathology Result Report Instance	18
5.4.3	XSD: Acknowledgement Document	19
5.4.4	XSD: Sealed Acknowledgement	19
6	WSDL: Sealed Pathology Result Report Consumer	20
6.1	Introduction	20
6.1.1	Purpose	20
6.1.2	Identity	20
6.1.3	Service Overview	20
6.2	Operations.....	20
6.2.1	deliver	21
7	WSDL: Sealed Pathology Result Report Supplier.....	23
7.1	Introduction	23
7.1.1	Purpose	23
7.1.2	Identity	23
7.1.3	Overview	23
7.2	Operations.....	24
7.2.1	Common Behaviours.....	24
7.2.2	list	25
7.2.3	retrieve	26
7.2.4	remove.....	27
8	WSDL: Sealed Acknowledgement Consumer	29
8.1	Introduction	29
8.1.1	Purpose	29
8.1.2	Identity	29
8.1.3	Overview	29
8.2	Operations.....	30
8.2.1	deliver	30
9	WSDL: Sealed Acknowledgement Supplier.....	32
9.1	Introduction	32
9.1.1	Purpose	32
9.1.2	Identity	32

9.1.3	Overview	32
9.2	Operations.....	33
9.2.1	Common Behaviours	33
9.2.2	retrieve	34
9.2.3	remove.....	35
Definitions	37
Shortened Terms	37
References	38
Specification Documents	38
References	38
Known Issues	40

Preface

Document Purpose

The purpose of this document is to partially define the role behaviours and service interfaces for Pathology Result Reporting. The complete endpoint specifications are made up of:

- this document; and
- the files in the *Pathology Result Reporting : Endpoint Specifications: WSDL and XML Schema files v3.0 draft 2009-06-30* [PRR-WX].

Scope

This endpoint specification only describes services that are invoked by external entities and the related behaviour. Services that are invoked by internal entities are not covered.

For example, management interfaces are not defined. In the process of delivering a pathology result report, one organisation does not invoke another organisation's management services. If required, products can define their own management interfaces.

This service interface specification does not define how these service interfaces are to be implemented and which business processes they participate in. Analysis of the Request-Test-Report "To Be" process is continuing and will be presented subsequently in [PRR-TBP].

Intended Audience

This is a technical document.

This document should be read and understood by:

- Solution Architect:
 - To understand the endpoint specifications to incorporate them into their designs.
- Developer:
 - To implement the service and/or clients which conform to the endpoint specifications.
- Tester:
 - To evaluate whether an implementation conforms to the endpoint specifications.

The reader is expected to understand XML, XML Schema, Web services, and WSDL.

Document status

This document is a draft release. Attention is also drawn to requirements PRR.16 and PRR.54, which state that the payloads for documents and acknowledgements must conform with the relevant payload schemas. This means that, until the Structured Document Template [PRR-SDT] is finalised, and the resulting specification stating how it must be implemented in a messaging structure [PRR-IF] is finalised, it will not be possible to build a "compliant" version of this interface. However, it does allow the industry to understand how it is expected that Pathology Result Reports will be delivered, following a node-to-node delivery approach.

This document contains a number of implementation requirements that will be subject to further review in a subsequent “to be” analysis of the pathology reporting domain [PRR-TBP]. A list of known issues is presented on page 40.

Document Map

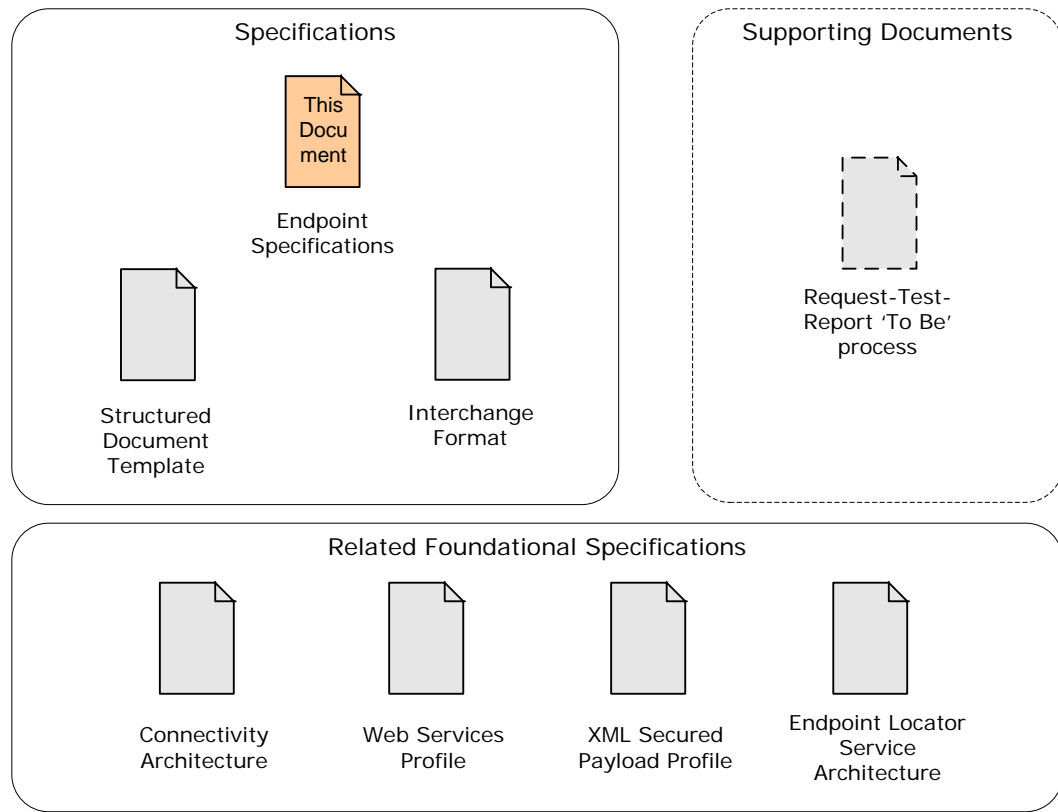


Figure 1: Pathology Result Reporting Endpoint Specification document map

References and Related Documents

For a list of all referenced documents, see the [References](#) at the end of the document, on page 38.

Definitions, Acronyms and Abbreviations

For a lists of abbreviations, acronyms and abbreviations, see the [Definitions section](#) at the end of the document, on page 37.

Conformance

The keywords **MUST**, **MUST NOT**, **SHOULD**, **SHOULD NOT**, and **MAY** in this document are to be interpreted as described in IETF’s RFC 2119 [RFC2119].

Overview

The Pathology Result Reporting Endpoint Specification defines three endpoints:

- Sender;
- Receiver; and
- Intermediary.

Four service interfaces are implemented by one or more of the endpoints:

- Sealed Pathology Result Report Consumer (Receiver or Intermediary);
- Sealed Pathology Result Report Supplier (Intermediary);
- Sealed Acknowledgement Consumer (Sender or Intermediary); and
- Sealed Acknowledgement Supplier (Intermediary).

The specification also defines four XML Schemas:

- Pathology Result Report;
- Sealed Pathology Result Report;
- Acknowledgement Document; and
- Sealed Acknowledgement.

This document describes the necessary behaviour of the endpoints identified above, the associated interface specifications and the message schemas for those interfaces.

As previously stated, this document forms one part of the endpoint specifications. It must be read in conjunction with the other part: the WSDL and XML Schema files from [PRR-WX], because this document does not attempt to duplicate the concepts and relationships that are formally represented in those files.

1 Common Behaviours

1.1 Introduction

This section defines behaviours and conformance requirements for all endpoints, that is, Sender, Receiver and Intermediary.

1.2 Web Services Profile

The following conformance points identify NEHTA standards necessary to ensure that Web service implementations can interconnect.

- PRR.1 Endpoints **MUST** conform to the Web Services Base Profile from the NEHTA Web Services Profile v3.1 [WSP2009] for all specified interactions.
- PRR.2 Endpoints **MUST** implement the TLS Security Profile from the NEHTA Web Services Profile v3.1 [WSP2009] for all specified interactions. Endpoints **SHOULD** also implement the WS-Security Profile from the NEHTA Web Service Profile for all specified interactions. Where both profiles are implemented, the distinct endpoints **MUST** have distinct interaction records if published in ELS [ELS2009].

1.3 Public Key Infrastructure

The following conformance points provide recommendations for handling certificates to ensure that the public key infrastructure is used in a scalable and robust manner while maintaining a reasonable degree of security.

- PRR.3 Endpoints **MUST** be capable of using separate signing and encryption certificates when applying the XSP [XSP2009] signing and encryption procedures to payload.
- PRR.4 Endpoints **MUST** comply with RFC 5280 for local validation and management of all certificates.
- PRR.5 Endpoints **SHOULD** cache certificate status information for the period of time recommended by the certificate revocation list or OCSP 'nextUpdate' field.
- PRR.6 Endpoints **SHOULD NOT** contact the certificate issuer each time a certificate is used (i.e. certificate checks should occur out-of-band wherever possible).

1.4 Authorisation

Authorisation will be the responsibility of web service providers. Minimum requirements are to be determined.

1.5 Identification

1.5.1 Endpoints

The following conformance points specify how Sender and Receiver will be identified. This identification will be used for both addressing in messages and for retrieval of interaction records from ELS.

- PRR.7 Senders and Receivers **MUST** be identified using an HPI-O if an HPI-O is available.
- PRR.8 If an HPI-O is not available, Senders and Receivers **MUST** be identified using one or more of the following identifiers:

- Medicare RA number
 - Email address
- PRR.9 Senders, Receivers and Intermediaries MUST be capable of using HPI-O and any of the nominated identifiers for ELS publications and queries, and in any visible (not opaque) message payload.
- PRR.10 Senders, Receivers and Intermediaries MUST encapsulate identifiers, including HPI-O, in a qualified identifier [QI2008] whenever these identifiers are transmitted as visible (not opaque) payload in a message.

1.5.2 Documents and Invocations

Two levels of identification are used in the pathology result report payload: *invocation identifiers* are used to support the end-to-end messaging process, pairing a particular pathology result report delivery with its matching acknowledgement; and *pathology result report identifiers* are used to identify the pathology result reports that are being transmitted. The same pathology result report might be sent to multiple Receivers, and the same pathology result report might be sent more than once to the same Receiver (e.g. to address encoding and other issues in a previous delivery). Note that these identifiers are distinct from any identifiers used in SOAP headers.

Specific conformance points relating to the use of these identifiers are specified for each of the roles and interfaces.

1.6 Assured Delivery

Conformance points in subsequent sections ensure that documents and acknowledgements are delivered by placing a responsibility on service invokers to ensure that service invocations are successful, and placing a responsibility on service providers to handle duplicates in cases where a SOAP response is lost or corrupted.

2 Endpoint: Sender

2.1 Introduction

2.1.1 Purpose

The Sender endpoint implements the behaviour necessary to send a sealed pathology result report to the intended recipient, either directly or through an intermediary. This includes receipt of acknowledgements for that pathology result report.

The term “sealed” refers to a report that has been digitally signed and then encrypted, as described in chapter 5.4.2. It is sealed from tampering by the digital signature, and it is sealed from being revealed to other entities by the encryption.

For example, this endpoint could be implemented by the Pathology Laboratory Systems software that sends pathology result reports to GP Practices.

2.1.2 Overview

Sender endpoint implementations that conform to this specification will invoke a Sealed Pathology Result Report Consumer interface to deliver pathology result reports and either provide a Sealed Acknowledgement Consumer interface or retrieve acknowledgements from a Sealed Acknowledgement Supplier interface provided by an Intermediary.

The Sender will also invoke infrastructure interfaces necessary to identify the Receiver, obtain security certificates, publish interface endpoints and locate interface endpoints. These interactions are specified in the Connectivity Architecture [CA2008]. In particular, the Sender must ensure that the location of a Sealed Acknowledgement Consumer interface that can be used to receive acknowledgments or negative acknowledgments is published in the Endpoint Location Service (ELS) [ELS2009]. This acknowledgement receipt interface can be provided either directly or by an intermediary.

2.2 Pathology Result Report Delivery

The following conformance points specify the required behaviour of a sender when delivering a pathology result report. The pathology result report is delivered to a Sealed Pathology Result Report Consumer service interface nominated by the Receiver in an ELS. This service interface could be provided by the Receiver or an Intermediary.

2.2.1 Service Invocation

- PRR.11 The Sender **MUST** invoke a Sealed Pathology Result Report Consumer interface to deliver pathology result reports to a Receiver.
- PRR.12 The Sender **SHOULD** use an ELS to initially locate the interaction record identifying the Sealed Pathology Result Report Consumer service interface for a Receiver. The Sender **SHOULD** cache this record at least until an acknowledgement is received for the associated message interaction.
- PRR.13 The Sender **MAY** use a third-party delivery agent to send the pathology result report but **MUST NOT** allow the third-party to access the unencrypted pathology result report. Note the implication that XSP (see section 2.2.3) must be applied within the Sender organisation.

2.2.2 Payload

- PRR.14 The Sender MUST include an invocation identifier that is unique at the sending site using the `invocationId` element in the sealed pathology result report payload schema defined in section 5.4.2.
- PRR.15 The Sender MUST identify the pathology result report using an identifier that is unique at the sending site in the `reportId` element in the pathology result report schema defined in section 5.4.1.
- PRR.16 The Sender MUST use the NEHTA specified document format for the pathology result report payload.

2.2.3 Privacy and Authentication

- PRR.17 The Sender MUST initially verify the authenticity of Receiver encryption certificates. These certificates will usually be returned with the ELS interaction record, or retrieved through certificate references returned with the ELS interaction record. This verification SHOULD ensure that the identity information contained in the certificate matches local identity information for the Receiver.
- PRR.18 The Sender MUST sign and then encrypt the pathology result report payload according to the signing and encryption methods defined in XSP [XSP2009], using a valid certificate of the Sender to sign, and a verified certificate of the Receiver for encryption.

2.2.4 Failures

- PRR.19 If an invocation is retried due to a communication or addressing failure, the Sender MUST use the same invocation identifier.
- PRR.20 Except when an invocation is retried, each invocation MUST use a different invocation identifier.
- PRR.21 The Sender is responsible for ensuring that an invocation is successful. Thus, the Sender MUST either retry an invocation until it is successful or escalate the issue to a responsible person. Note that if the Sender receives a `duplicate` status in a SOAP response (see section 6.2.1.3), this indicates that a previous invocation was successful and that no further retry is necessary.
- PRR.22 The Sender MUST NOT use the same invocation identifier if resending a pathology result report *after* a negative acknowledgement is received (e.g. to address payload errors indicated in the acknowledgement). The Sender MAY use the same pathology result report identifier when resending a pathology result report after a negative acknowledgement has been received.

2.3 Acknowledgement Receipt

The following conformance points specify the required behaviour of a Sender when receiving acknowledgements and negative acknowledgements.

2.3.1 Implementation

- PRR.23 The Sender MUST either:
1. Implement the Sealed Acknowledgement Consumer interface; or
 2. Implement a service invoker for the Sealed Acknowledgement Supplier interface provided by an Intermediary.

- PRR.24 The Sender MAY implement both a Sealed Acknowledgement Consumer interface and a service invoker for the Sealed Acknowledgement Supplier interface.

2.3.2 Direct Acknowledgement Receipt

The conformance points in the following subsections apply to Sender implementations that directly receive acknowledgements on a Sealed Acknowledgement Consumer interface (option 1 above).

2.3.2.1 Endpoint publication

- PRR.25 The Sender MUST publish an interaction record identifying its Sealed Acknowledgement Consumer interface in an ELS according to [ELS2009].

2.3.2.2 Service Provision

- PRR.26 The Sender MUST receive acknowledgements via the identified Sealed Acknowledgement Consumer interface.

2.3.3 Indirect Acknowledgement Receipt

The conformance points apply to Sender implementations that retrieve acknowledgements by invoking a Sealed Acknowledgement Supplier interface (option 2 above) offered by a nominated Intermediary.

2.3.3.1 Endpoint publication

- PRR.27 The Sender MUST ensure publication of an interaction record identifying the Sealed Acknowledgement Consumer interface of the nominated Intermediary in an ELS according to [ELS2009]. The ELS publication action MAY be performed by the Intermediary on behalf of a Sender.

2.3.3.2 Service Invocation

- PRR.28 The Sender SHOULD attempt to retrieve acknowledgements at least once each business day using the Sealed Acknowledgement Supplier interface of the nominated Intermediary.
- PRR.29 The Sender MUST remove acknowledgements from the Intermediary after they have been successfully retrieved and stored locally.

2.3.4 Local Handling and Storage

- PRR.30 The Sender MUST ensure that a record of the Acknowledgement is stored such that a laboratory administrator or other responsible person can determine whether the identified pathology result report has been successfully processed by the Receiver. The intent of this requirement is to ensure that acknowledgements are visible to laboratory administrator: the nature of the user interface is not constrained and might provide significantly more information.
- PRR.31 If a negative acknowledgement is received, the Sender SHOULD escalate the issue to a Laboratory Administrator or other responsible person.
- PRR.32 If the invocation identifier or Sender identifier associated with a Sealed Acknowledgement does not match any invocation made by the Sender, the issue SHOULD be escalated to a Laboratory Administrator or other responsible person.

PRR.33 If the pathology result report identifier associated with a Sealed Acknowledgement is invalid or cannot be extracted, the issue SHOULD be escalated to a Laboratory Administrator or other responsible person. This might occur, for example, if the acknowledgement payload is corrupt, cannot be decrypted or contains an invalid pathology result report identifier.

2.3.5 Privacy and Authentication

PRR.34 The Sender MUST verify that the signature on a Sealed Acknowledgement was made with the signing certificate identified in the XSP payload [XSP2009], and also verify the authenticity of the signing certificate. This verification SHOULD ensure that the identity information contained in the certificate matches local identity information for the Receiver.

PRR.35 The Sender MUST verify that a pathology result report identifier contained in an Acknowledgement matches the pathology result report identifier sent with the nominated invocation identifier. Since the pathology result report identifier is contained in the sealed payload of the original message, this provides an assurance of authenticity for the acknowledgement.

2.3.6 Failures

PRR.36 If no acknowledgement for a message has been received within an agreed period since sending, the Sender SHOULD escalate the issue to a laboratory administrator or other responsible person.

3 Endpoint: Receiver

3.1 Introduction

3.1.1 Purpose

The Receiver endpoint implements the behaviour necessary to receive a Sealed Pathology Result Report from the Sender, either directly or through an Intermediary. This includes sending an acknowledgement for that pathology result report.

The term “sealed” refers to a pathology result report that has been digitally signed and then encrypted, as described in chapter 5.4.2. It is sealed from tampering by the digital signature, and it is sealed from being revealed to other entities by the encryption.

For example, this endpoint could be implemented by GP practice management software for receiving pathology result reports.

3.1.2 Overview

Receiver endpoint implementations that conform to this specification will either:

- provide a Sealed Pathology Result Report Consumer interface to receive pathology result reports directly from the Sender; or
- invoke a Sealed Pathology Result Report Supplier interface to retrieve pathology result reports from an Intermediary nominated by the Receiver.

The Receiver will also invoke a Sealed Acknowledgement Consumer interface to deliver acknowledgements.

The Receiver will invoke infrastructure interfaces necessary to authenticate the Sender, obtain security certificates, publish interface endpoints and locate interface endpoints. These interactions are specified in the Connectivity Architecture [CA2008]. In particular, the Receiver must ensure that the location of a Sealed Pathology Result Report Consumer interface that can be used to receive pathology result reports is published in the Endpoint Location Service (ELS) [ELS2009]. As noted above, this interface can be provided either directly or by an intermediary.

3.2 Pathology Result Report Receipt

The following conformance points specify the required behaviour of a Receiver when receiving pathology result reports.

3.2.1 Implementation

PRR.37 The Receiver **MUST** either:

1. Implement the Sealed Pathology Result Report Consumer interface; or
2. Implement a service invoker for the Sealed Pathology Result Report Supplier interface.

PRR.38 The Receiver **MAY** implement both a Sealed Pathology Result Report Consumer interface and a service invoker for the Sealed Pathology Result Report Supplier interface.

3.2.2 Direct Pathology Result Report Receipt

The conformance points in the following subsections apply to Receiver implementations that directly receive pathology result reports on a Sealed Pathology Result Report Consumer interface (option 1 above).

3.2.2.1 Endpoint publication

PRR.39 The Receiver MUST publish an interaction record identifying its Sealed Pathology Result Report Consumer interface in an ELS according to [ELS2009].

3.2.2.2 Service Provision

PRR.40 The Receiver MUST receive pathology result reports via the identified Sealed Pathology Result Report Consumer interface.

3.2.3 Indirect Pathology Result Report Receipt

The conformance points apply to Receiver implementations that retrieve pathology result reports by invoking a Sealed Pathology Result Report Supplier interface (option 2 above) offered by a nominated Intermediary.

3.2.3.1 Endpoint publication

PRR.41 The Receiver MUST ensure publication of an interaction record identifying the Sealed Pathology Result Report Consumer interface of the nominated Intermediary in an ELS according to [ELS2009]. The ELS publication action MAY be performed by the Intermediary on behalf of the Receiver.

3.2.3.2 Service Invocation

PRR.42 The Receiver MUST attempt to retrieve pathology result reports at least once each business day using the Sealed Pathology Result Report Supplier interface of the nominated Intermediary.

PRR.43 The Receiver MUST remove pathology result reports from the Intermediary after they have been successfully retrieved and stored locally.

3.2.4 Local Handling and Storage

PRR.44 If the Sealed Pathology Result Report is successfully decrypted and verified, the Receiver MUST ensure that the contained pathology result report is stored such that a Clinician or other responsible person can access and take appropriate action in relation to the pathology result report.

3.2.5 Privacy and Authentication

PRR.45 The Receiver MUST verify that the signature on a Sealed Pathology Result Report was made with the nominated signing certificate, and also verify the authenticity of the signing certificate. This verification SHOULD ensure that the identity information contained in the certificate matches identity information for the Sender contained in the pathology result report.

PRR.46 The Receiver MUST ensure that the pathology result report is stored in a manner that prevents unauthorised access to the pathology result report. If the receiving software passes the pathology result report to another software system in the receiving organisation, this access control SHOULD also be enforced by that system.

- PRR.47 The Receiver MUST ensure that the Sealed Pathology Result Report can be decrypted using the Receiver's encryption certificate. A negative acknowledgement MUST be sent if the document cannot be decrypted.

3.3 Acknowledgement Delivery

The following conformance points specify the required behaviour of a Receiver when delivering an acknowledgement for a pathology result report. The acknowledgement is delivered to a Sealed Acknowledgement Consumer interface nominated by the Sender in the Sealed Pathology Result Report or published by the Sender in an ELS.

3.3.1 Service Invocation

- PRR.48 The Receiver MUST invoke a Sealed Acknowledgement Consumer interface to deliver acknowledgements to a Sender.
- PRR.49 If the Sealed Pathology Result Report does not include an ELS interaction record for acknowledgements or that interaction record is not compatible with the Receiver implementation, the Receiver SHOULD use an ELS to locate a compatible interaction record identifying the Sealed Acknowledgement Consumer interface for a Sender. The Receiver SHOULD cache this record.
- PRR.50 The Receiver MAY use a third-party delivery agent to send the acknowledgement but MUST NOT allow the third-party to access the encrypted acknowledgement payload. Note the implication that XSP (see section 2.2.3) must be applied to the payload within the Receiver organisation.

3.3.2 Payload

- PRR.51 The Receiver MUST send a positive acknowledgement if the Sealed Pathology Result Report was successfully decrypted, verified and delivered to the application or data store used to present such information to the target clinician. Otherwise, the Receiver MUST send a negative acknowledgement.
- PRR.52 The Receiver MUST include the invocation identifier from the corresponding sealed pathology result report using the `invocationId` element in the sealed acknowledgement schema defined in section 5.4.4.
- PRR.53 If the pathology result report identifier was accessible in the Sealed Pathology Result Report, the Receiver MUST include the pathology result report identifier from the corresponding sealed pathology result report using the `reportId` element in the acknowledgement document schema defined in section 5.4.3.
- PRR.54 If an acknowledgement payload is carried in the optional `ep:encryptedPayload` field defined in 5.4.4, the Receiver MUST use the NEHTA specified acknowledgement format for the acknowledgement document.

3.3.3 Privacy and Authentication

- PRR.55 The Receiver MUST initially verify the authenticity of Sender authentication and encryption certificates. These certificates will be included in the Sealed Pathology Result Report Consumer invocation, returned with an ELS interaction record, or retrieved through certificate references returned with the ELS interaction record. This verification SHOULD ensure that the identity

information contained in the certificate matches local identity information for the Receiver.

- PRR.56 The Receiver MUST sign and then encrypt the acknowledgement payload defined in 5.4.4 according to the signing and encryption methods defined in XSP [XSP2009], using a valid certificate of the Receiver to sign, and a verified certificate of the Sender for encryption.

3.3.4 Failures

The Receiver is responsible for ensuring that an acknowledgement delivery invocation is successful. Thus, the Receiver MUST either retry an invocation until it is successful or escalate the issue to a responsible person. Note that if the Sealed Acknowledgement Consumer returns a `duplicate` status in the SOAP response (see section 8.2.1.3), this indicates that a previous invocation was successful and that no further retry is necessary.

4 Endpoint: Intermediary

4.1 Introduction

4.1.1 Purpose

An Intermediary provides pathology result report and acknowledgement storage services that allow Senders and Receivers to function without directly hosting Web services. It therefore offers both Sealed Pathology Result Report Consumer and Sealed Acknowledgement Consumer interfaces, with corresponding supplier interfaces for retrieval of pathology result reports and acknowledgements.

An Intermediary is nominated by the recipient of messages and acknowledgements. In the exchange of a pathology result report, there will often be two Intermediaries: one acting on behalf of the Receiver to receive the Sealed Pathology Result Report, and another acting on behalf of the Sender to receive the Sealed Acknowledgement Payload.

The term “sealed” refers to a document that has been digitally signed and then encrypted, as described in chapter 5.4.2. It is sealed from tampering by the digital signature, and it is sealed from being revealed to other entities by the encryption.

For example, this endpoint could be implemented by a messaging gateway service acting on behalf of a GP clinic that is to receive pathology result reports.

4.1.2 Overview

Intermediary endpoint implementations that conform to this specification provide four interfaces:

- A Sealed Pathology Result Report Consumer interface to receive pathology result reports on behalf of a Receiver;
- A Sealed Pathology Result Report Supplier interface that allows a Receiver to retrieve pathology result reports;
- A Sealed Acknowledgement Consumer interface to receive acknowledgements on behalf of a Sender; and
- A Sealed Acknowledgement Supplier interface that allows a Sender to retrieve acknowledgements and negative acknowledgements.

The Intermediary will invoke infrastructure interfaces necessary to authenticate the Sender, obtain security certificates, publish interface endpoints and locate interface endpoints. These interactions are specified in the Connectivity Architecture [CA2008].

The following conformance points specify the required behaviour of an Intermediary when receiving pathology result reports and acknowledgements on behalf of a health care provider.

4.2 Common Intermediary Conformance Points

The conformance points in this section apply to all interactions with the Intermediary.

4.2.1 Delivery

PRR.57 If a message or acknowledgement received on a Consumer interface is not retrieved by the identified recipient within the period specified in the `sdi:expiryTime` field, the issue **MUST** be

escalated to a responsible person. The responsible person SHOULD contact the identified recipient to determine the cause of the delay and ensure that the message or acknowledgement is received.

4.2.2 Privacy and Authentication

Transport-level certificate management associated with the invocation of Intermediary consumer interfaces is adequately covered by the Web Services Profile [WSP2009] and public key infrastructure conformance points in section 1.3. The following additional conformance points specify the privacy and authentication steps associated with storage and the supplier interfaces.

PRR.58 The Intermediary MUST NOT decrypt any sealed payload. In other words, in the unlikely event of the Intermediary having a copy of the Sender or Receiver private key, this key must not be used to decrypt any messages or acknowledgements.

PRR.59 The Intermediary MUST verify the certificate of any invoker of its service interfaces. This verification SHOULD ensure that the identity information contained in the certificate matches identity information contained in the invocation.

4.3 Pathology Result Report Receipt and Supply

4.3.1 Implementation

PRR.60 The Intermediary MUST implement the Sealed Pathology Result Report Consumer interface and the Sealed Pathology Result Report Supplier interface.

4.3.2 Endpoint publication

PRR.61 The Intermediary SHOULD ensure publication of an interaction record identifying its Sealed Pathology Result Report Supplier in an ELS according to [ELS2009].

PRR.62 The Intermediary MAY publish one or more interaction records for the Sealed Pathology Result Report Consumer interface associated with a Receiver at the request of that Receiver. The intermediary MUST NOT publish any interaction records on behalf of a Receiver without an explicit request from that Receiver.

4.3.3 Local Handling and Storage

PRR.63 Upon successful receipt of an invocation from a Sender on the Sealed Pathology Result Report Consumer interface, the Intermediary MUST make the Sealed Pathology Result Report in that request available to the identified Receiver through the associated Sealed Pathology Result Report Supplier interface.

PRR.64 An Intermediary MUST NOT make a Sealed Pathology Result Report available to any party other than the identified Receiver.

PRR.65 The Intermediary SHOULD NOT remove Sealed Pathology Result Report instances from storage unless explicitly requested by the Receiver, either through the `remove` operation or an out-of-band request.

4.4 Acknowledgement Receipt and Supply

4.4.1 Implementation

PRR.66 The Intermediary **MUST** implement the Sealed Acknowledgement Consumer interface and the Sealed Acknowledgement Supplier interface.

4.4.2 Endpoint publication

PRR.67 The Intermediary **SHOULD** ensure publication of an interaction record identifying its Sealed Acknowledgement Supplier in an ELS according to [ELS2009].

PRR.68 The Intermediary **MAY** publish one or more interaction records for the Sealed Acknowledgement Consumer interface associated with a Sender at the request of that Sender. The intermediary **MUST NOT** publish any interaction records on behalf of a Sender without an explicit request from that Sender.

4.4.3 Local Handling and Storage

Upon successful receipt of an acknowledgement from a Receiver on the Sealed Acknowledgement Consumer interface, the Intermediary **MUST** make the Sealed Acknowledgement or Sealed Negative Acknowledgement in that invocation available to the identified Sender through the associated Sealed Pathology Result Report Supplier interface.

PRR.69 An Intermediary **MUST NOT** make a Sealed Acknowledgement available to any party other than the identified Sender.

PRR.70 The Intermediary **SHOULD NOT** remove Sealed Acknowledgement instances from storage unless explicitly requested by the Sender.

5 WSDL: Common Components

5.1 Introduction

The service interface specifications share a number of common components. This section specifies those common components.

5.2 Namespace

This release of the pathology result reporting endpoint specification is identified by the following URL:

<http://ns.neht.gov.au/Pth/Pkg/3.0-draft-20090630>

The specific components identified in subsequent sections will be referenced by a specification document available at this URL.

5.2.1 XML Schema Namespace

Four schemas are defined for this specification. These schemas and their associated namespace prefixes are identified in the following table.

Prefix	Schema
sri:	http://ns.nehta.gov.au/Pth/Xsd/SealedPathologyResultReportInstance/3.0-draft-20090630
pri:	http://ns.nehta.gov.au/Pth/Xsd/PathologyResultReportInstance/3.0-draft-20090630
sack:	http://ns.nehta.gov.au/Pth/Xsd/SealedAcknowledgementInstance/3.0-draft-20090630
ackd:	http://ns.nehta.gov.au/Pth/Xsd/AckDocument/3.0-draft-200906300

These schemas are defined further in sections 5.4.1 through 5.4.4.

5.3 ELS Publication Requirements

The following conformance points define common requirements for publication of service instances in an ELS. More specific conformance points are defined in subsequent sections as required.

- PRR.71 All services instances implementing pathology result reporting related interfaces **MUST** be published in an ELS using the default service category names and interface names identified in subsequent sections.
- PRR.72 If service instances are offered by an Intermediary on behalf of multiple Senders and/or Receivers, distinct interaction record publications for each Sender or Receiver that has engaged the Intermediary **MUST** be published in an ELS. Interaction records for different Senders and Receivers **MAY** reference the same service instance.

5.4 XML Schemas

5.4.1 XSD: Pathology Result Report

This schema is used to carry pathology result reporting related payloads.

This schema is used by the definition of a sealed pathology result report, which represents a signed and then encrypted pathology result report. See chapter 5.4.2 for more information about sealed pathology result report.

This schema has the namespace of:

<http://ns.nehta.gov.au/Pth/Xsd/PathologyResultReportInstance/3.0-draft-20090630>

This schema is illustrated in Figure 2.

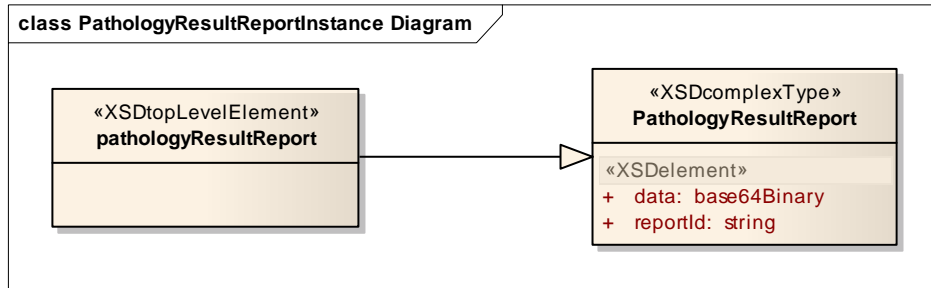


Figure 2: Components of the Pathology Result Report schema

PRR.73 The data field MUST contain an HL7 report as defined in the Pathology Result Reporting - Interchange Format [PRR-IF].

5.4.2 XSD: Sealed Pathology Result Report Instance

This schema is used to represent instances of pathology result reports wrapped in a sealed pathology result report. An *instance* of a sealed pathology result report is an occurrence of a pathology result report that is being delivered from a Sender to a Receiver. Each time a pathology result report is delivered (e.g. to different receivers or multiple copies of the same pathology result report delivered to one receiver) that is a new instance.

The term “sealed” refers to a pathology result report that has been digitally signed and then encrypted, as described in chapter 5.4.2. It is sealed from tampering by the digital signature, and it is sealed from being revealed to other entities by the encryption.

This XML Schema is used by the following service interfaces:

- Sealed Pathology Result Report Consumer; and
- Sealed Pathology Result Report Supplier.

This schema has the namespace of:

<http://ns.nehta.gov.au/Pth/Xsd/SealedPathologyResultReportInstance/3.0-draft-20090630>

This schema is illustrated in Figure 3.

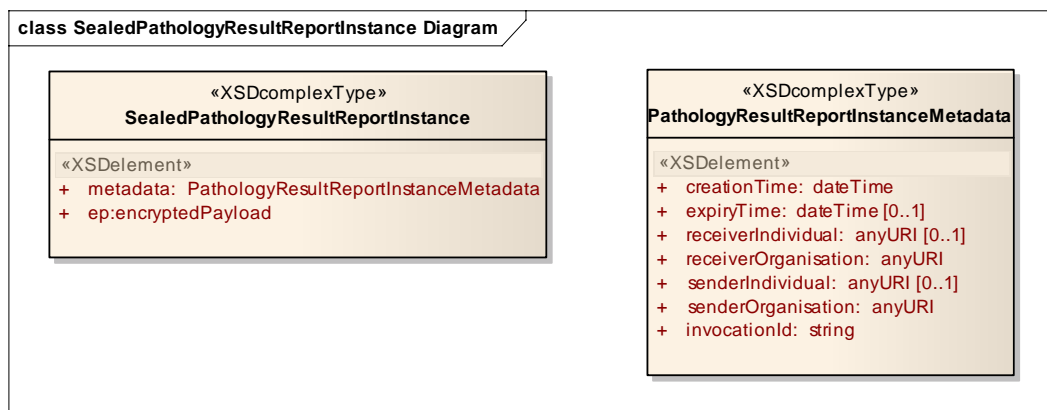


Figure 3: Components of the Sealed Pathology Result Report schema

5.4.3 XSD: Acknowledgement Document

This schema is used to carry acknowledgement documents.

This schema is used by the definition of a sealed acknowledgement, which represents a signed and then encrypted acknowledgement document. See chapter 5.4.4 for more information about sealed acknowledgement.

This schema has the namespace of:

`http://ns.nehta.gov.au/Pth/Xsd/AckDocument/3.0-draft-20090630`

This schema is illustrated in Figure 2.

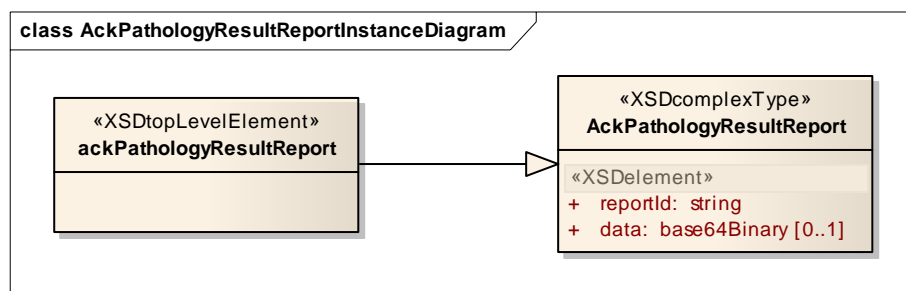


Figure 4: Components of the Acknowledgement Document schema

PRR.74 If populated, the data field MUST contain an acknowledgement as specified in the Pathology Result Reporting - Interchange Format [PRR-IF].

5.4.4 XSD: Sealed Acknowledgement

This schema is used to represent acknowledgements of the delivery of a pathology result report instance.

It is used by the following service interfaces:

- Sealed Acknowledgement Consumer (section 8); and
- Sealed Acknowledgement Provider (chapter 9).

This schema has the namespace of:

`http://ns.nehta.gov.au/Pth/Xsd/SealedAcknowledgementInstance/3.0-draft-20090630`

This schema is illustrated in Figure 5.

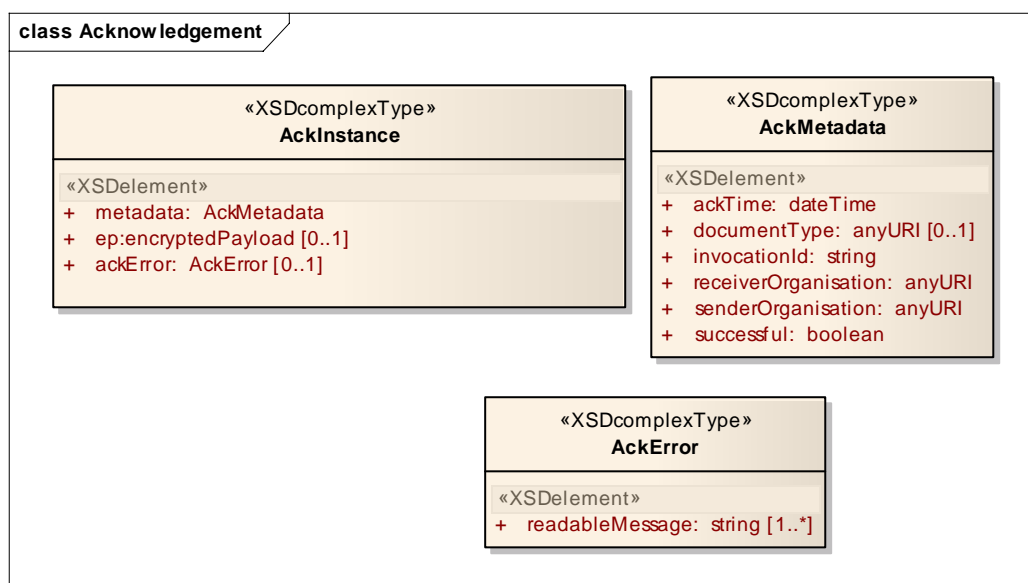


Figure 5: Components of the Sealed Pathology Result Report Acknowledgement schema

6 WSDL: Sealed Pathology Result Report Consumer

6.1 Introduction

6.1.1 Purpose

This service interface is implemented by Receivers or their Intermediaries to receive pathology result reports from Senders.

6.1.2 Identity

This service is identified by the following service category:

```
http://ns.nehta.gov.au/Pth/Sc/SealedPathologyResultReportConsumer/3.0-draft-20090630
```

PRR.75 A Receiver **MUST** publish sealed pathology result report consumer service instances in an ELS under this service category. Note that the publication action might be performed by an Intermediary on behalf of a Receiver.

The WSDL schema for this service is defined in the following namespace:

```
http://ns.nehta.gov.au/Pth/Wsd1/SealedPathologyResultReportConsumer/3.0-draft-20090630
```

This namespace is subsequently identified using the namespace prefix `sdc`.

The service interface for implementations that comply with the TLS Security Profile is identified by:

```
http://ns.nehta.gov.au/Pth/Intf/SealedPathologyResultReportConsumer/TLS/3.0-draft-20090630
```

PRR.76 Receivers **MUST** use this interface identifier when publishing sealed pathology result report consumer service instances implementing the TLS security profile in an ELS.

6.1.3 Service Overview

This service interface is illustrated in Figure 6.

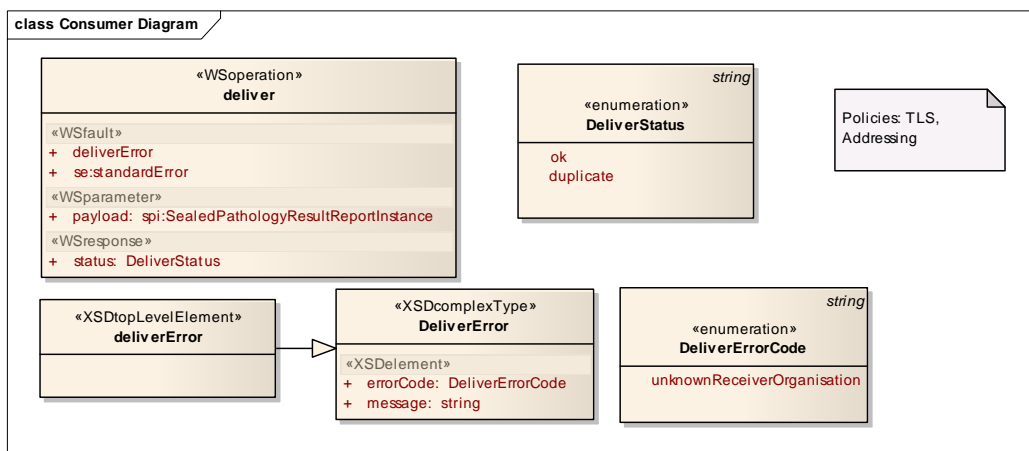


Figure 6: Components of the Sealed Pathology Result Report Consumer service interface

6.2 Operations

This service interface defines one operation:

- `deliver`

A Sender invokes `deliver` for each pathology result report being sent to a Receiver. The following conformance points associated with the `deliver` operation are in addition to the endpoint conformance points defined in sections 2, 3 and 4.

In the following subsections, the service invoker is a Sender, and the service provider is a Receiver or Intermediary.

6.2.1 `deliver`

6.2.1.1 Purpose

This operation is used to deliver a message containing the Sealed Pathology Result Report to a Receiver or the Receiver's Intermediary. It is invoked by a Sender that has a pathology result report to send to a Receiver.

6.2.1.2 Request

The request contains a signed and encrypted pathology result report and metadata to assist in delivering the pathology result report. The following conformance points apply:

- PRR.77 The service invoker MUST send a `sdm:deliver` request.
- PRR.78 The service invoker MUST set the encrypted payload `sdi:ep` using XSP [XSP2009] to sign then encrypt an `dsi:PathologyResultReport` instance.
- PRR.79 The service invoker SHOULD set the `sdi:invocationId` to be a UUID formatted as a URN as defined in [RFC4122].
- PRR.80 The service invoker SHOULD set the `sdi:creationTime` to indicate the date and time that the pathology result report was created.
- PRR.81 The service invoker MAY set the `sdi:expiryTime` to indicate the date and time by which an acknowledgement is expected for the pathology result report.
- PRR.82 The service invoker MUST set the `sdi:senderOrganisation` and `sdi:receiverOrganisation` elements to qualified identifier values [QI2008] for the Sender and Receiver respectively using one of the identifier types specified by PRR.7 in section 1.5.
- PRR.83 The service invoker SHOULD identify the sending clinician and intended receiving clinician using the `sdi:receiverIndividual` and `sdi:senderIndividual` elements respectively. If used these elements MUST be encoded as URIs according to [RFC3986]. These elements MAY be encoded as qualified identifiers [QI2008] (which are also valid URIs).

6.2.1.3 Response

The response indicates whether the operation succeeded or not. The operation is a delivery mechanism only, so it does not indicate whether or not the pathology result report content has been processed: this is indicated through a separate acknowledgement interaction. The following conformance points apply to the service provider.

- PRR.84 The service provider MUST return a `sdm:deliverResponse`.
- PRR.85 The service provider MUST NOT return a successful response until after the sealed pathology result report is successfully stored in non-volatile storage.
- PRR.86 The service provider MUST NOT store more than one sealed pathology result report from a particular service invoker with the same `sdi:invocationId` (i.e. no duplicates stored).

- PRR.87 If request has the same `sdi:invocationId` as a previous request from the same service invoker and processing of the previous request was successful, then the service provider MUST return a status of `sdc:duplicate` in the response.

6.2.1.3.1 *Faults*

Faults indicate that an error has occurred at the service provider.

- PRR.88 The service provider MUST respond with a `sdc:deliverError` or `se:standardError` fault if an error occurs in processing the `deliver` operation.
- PRR.89 The service provider MUST respond with a `sdc:deliverError` fault if the `sdi:receiverOrganisation` element of the request does not identify the service provider or a Receiver that has explicitly engaged the service provider as per PRR.61 in section 4.3.2 In this case the service provider MUST also discard the sealed pathology result report.

7 WSDL: Sealed Pathology Result Report Supplier

7.1 Introduction

7.1.1 Purpose

This service interface is implemented by Intermediaries to make sealed pathology result report available for Receivers to retrieve.

7.1.2 Identity

This service is identified by the following service category:

`http://ns.nehta.gov.au/Pth/Sc/SealedPathologyResultReportSupplier/3.0-draft-20090630`

PRR.90 An Intermediary **MUST** publish sealed pathology result report supplier service instances in an ELS under this service category.

The WSDL schema for this service is defined in the following namespace:

`http://ns.nehta.gov.au/Pth/Wsd/SealedPathologyResultReportSupplier/3.0-draft-20090630`

This namespace is subsequently identified using the namespace prefix `sds:`.

The service interface for implementations that comply with the TLS Security Profile is identified by:

`http://ns.nehta.gov.au/Pth/Intf/SealedPathologyResultReportSupplier/TLS/3.0-draft-20090630`

PRR.91 Intermediaries **MUST** use this interface identifier when publishing sealed pathology result report consumer service instances implementing the TLS security profile in an ELS.

7.1.3 Overview

This service interface is illustrated in Figure 7.

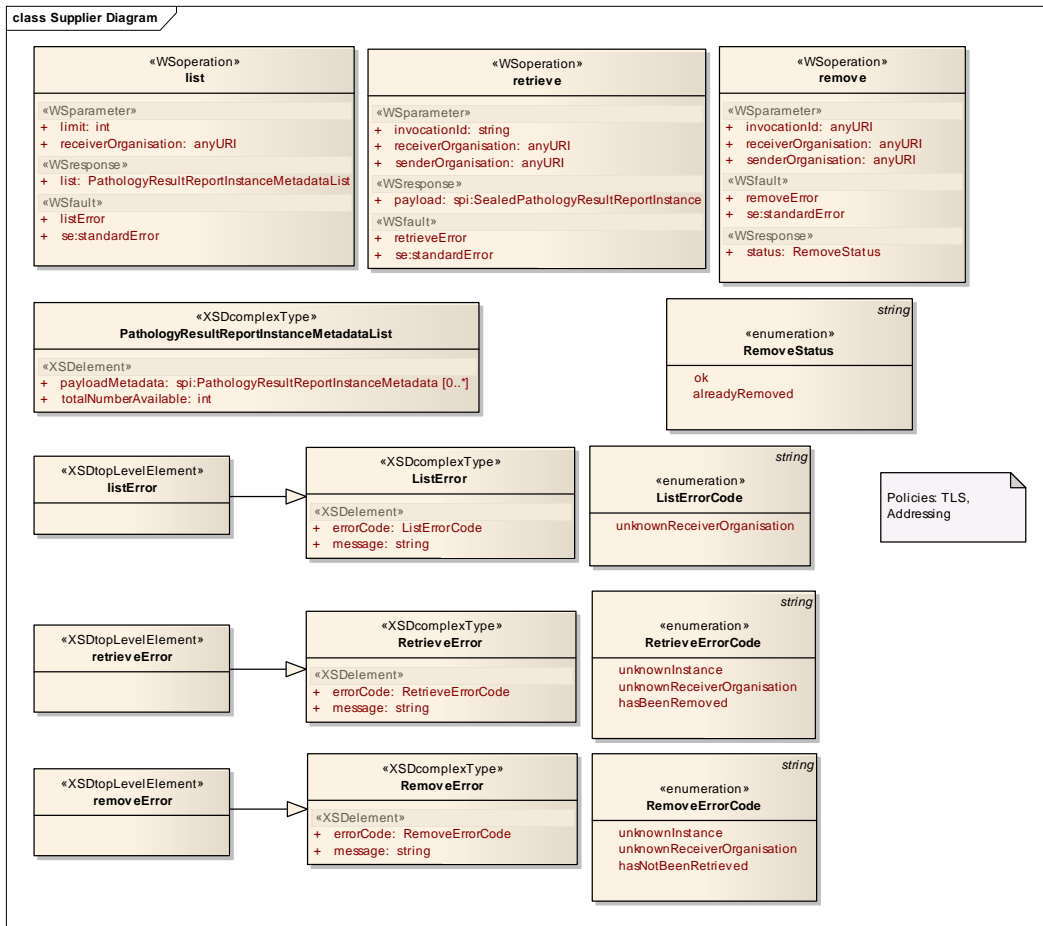


Figure 7: Components of the Sealed Pathology Result Report Supplier service interface

7.2 Operations

This service interface defines three operations:

- `list`;
- `retrieve`; and
- `remove`.

A Receiver would invoke `list` to obtain a list of documents that are available for it to retrieve. For each pathology result report in the list, the Receiver can invoke `retrieve` to retrieve it, and invoke `remove` to indicate that a retrieved pathology result report has been safely stored by the Receiver and can be removed from storage at the Intermediary.

For all operations, the service invoker is a Receiver and the service provider is an Intermediary. Conformance points in the following subsections are in addition to the conformance points for Receiver and Intermediary specified in sections 3 and 4 respectively.

7.2.1 Common Behaviours

The following conformance points apply to all invocations on the interface.

- PRR.92 The service invoker MUST identify itself in all requests by setting the `sds:receiverOrganisation` element using one of the identifier types specified by PRR.7 in section 1.5.
- PRR.93 The service provider SHOULD reject or ignore requests where the `sds:receiverOrganisation` element does not match the organisation associated with the security certificate used by the service invoker.

- PRR.94 If the organisation identified in the `receiverOrganisation` element of a request does not identify a client of the service provider, the service provider SHOULD respond to a request with a fault having the `errorCode` set to `unknownReceiverOrganisation`. The service provider SHOULD include a human-readable string describing the problem in the `message` element of the fault.

7.2.2 list

7.2.2.1 Purpose

This operation is used to return a list of pathology result reports that are available for retrieval. Pathology result reports received by the Intermediary will be listed by this operation until they are explicitly removed by the Receiver.

7.2.2.2 Request

- PRR.95 The service invoker MUST send a `list` request.
- PRR.96 The service invoker SHOULD set the `sds:limit` element to zero or a positive integer to indicate the maximum number of items to return in the `sds:list` element of the response. The service invoker MAY set the `sds:limit` element to a negative number to indicate that any number of items can be returned.

7.2.2.3 Response

The response contains the total number of available pathology result report instances and a list containing the sealed pathology result report metadata for some or all of them. Each pathology result report is identified for retrieval purposes by the combination of a `sdi:invocationIdentifier` and a `sdi:senderOrganisation`.

- PRR.97 The service provider MUST return a `list` response if successful.
- PRR.98 The service provider MUST return a `list` fault if not successful.

The remaining conformance points in this section apply to requests correctly authenticated according to PRR.93.

- PRR.99 The service provider MUST set the `totalNumberAvailable` element of a `list` response to indicate the total number of sealed pathology result report instances currently available for the `receiverOrganisation` identified in the request.
- PRR.100 The service provider MUST NOT include references to any sealed pathology result report instances that have previously been removed by the `receiverOrganisation` in the `list` response.
- PRR.101 The service provider MUST NOT count any sealed pathology result report instances that have previously been removed by the `receiverOrganisation` in the `list` response when setting the value of the `totalNumberAvailable` element.
- PRR.102 If the `limit` element of the request is a positive integer, the service provider MUST NOT return more than this number of references in a `list` response.
- PRR.103 If the `limit` element of the request is equal to zero, the service provider MUST NOT return any references. Note that the `totalNumberAvailable` should still be returned as per PRR.99. This allows the invoker to determine the number of references without retrieving them.

- PRR.104 If the service provider has pathology result reports available for the identified receiver and the request `limit` element is greater than zero, the service provider **MUST** return at least one reference.
- PRR.105 For each reference listed in the `list` response, the service provider must return an unmodified `sdi:SealedPathologyResultReportMetadata` element received by the service provider through an invocation on its `SealedPathologyResultReportConsumer` interface.

7.2.2.3.1 *Faults*

- PRR.106 The service provider **MUST** respond to a `list` request with a `sds:listError` or `se:standardError` fault if an error occurs in processing the `list` request.
- PRR.107 The service provider **MAY** respond to a `list` request with a fault containing a `se:standardError` element as defined by [WSP2009].

7.2.3 **retrieve**

7.2.3.1 Purpose

This operation is used by the Receiver to retrieve a pathology result report instance.

7.2.3.2 Request

- PRR.108 The service invoker **MUST** send a `retrieve` request.
- PRR.109 The service invoker **MUST** set the `senderOrganisation` and `invocationId` elements of the `retrieve` request to values from a reference returned by a preceding `list` request.

7.2.3.3 Response

The response contains a `sdi:SealedPathologyResultReport` instance, including both the metadata and the signed and encrypted payload.

- PRR.110 The service provider **MUST** return a `retrieve` response if successful.
- PRR.111 The service provider **MUST** return a `retrieve` fault if not successful.

The remaining conformance points in this section apply to requests correctly authenticated according to PRR.93.

- PRR.112 If the combination of `senderOrganisation` and `invocationId` identifies a `SealedPathologyResultReportInstance` held by the service provider for the `receiverOrganisation` and the instance has not been removed, the service provider **MUST** return the identified `SealedPathologyResultReportInstance`. Note that a service invoker might retrieve the same instance multiple times. This should not change the behaviour of the operation unless the report instance has been explicitly removed.

7.2.3.3.1 *Faults*

- PRR.113 The service provider **MUST** respond to a `retrieve` request with a `sds:retrieveError` or `se:standardError` fault if an error occurs in processing the `retrieve` request.
- PRR.114 The service provider **MAY** respond to a `retrieve` request with a fault containing a `se:standardError` element as defined by [WSP2009].

- PRR.115 If the combination of `senderOrganisation` and `invocationId` does not identify a `SealedPathologyResultReportInstance` held by the service provider for the `receiverOrganisation`, the service provider **MUST** respond to a `retrieve` request with a `retrieveError` fault having the `errorCode` set to `unknownInstance`. The service provider **SHOULD** include a human-readable string describing the problem in the `message` element of the fault.
- PRR.116 If the combination of `senderOrganisation` and `invocationId` identifies a `SealedPathologyResultReportInstance` that has previously been removed by the `receiverOrganisation`, the service provider **MAY** respond to a `retrieve` request with a `retrieveError` fault having the `errorCode` set to `hasBeenRemoved`. The service provider **SHOULD** include a human-readable string describing the problem in the `message` element of the fault.

7.2.4 remove

7.2.4.1 Purpose

This operation is used by a Receiver to indicate that the pathology result report instance has been retrieved and stably stored by the Receiver and can be removed.

7.2.4.2 Request

- PRR.117 The service invoker **MUST** send a `remove` request.
- PRR.118 The service invoker **MUST** set the `senderOrganisation` and `invocationId` elements of the `remove` request to values from a reference returned by a preceding `list` request.
- PRR.119 The service invoker **MUST NOT** send a `remove` request for a `SealedPathologyResultReport` that has not previously been received and stably stored.

7.2.4.3 Response

The response indicates whether the `remove` operation succeeded.

- PRR.120 The service provider **MUST** return a `remove` response if successful.
- PRR.121 The service provider **MUST** return a `remove` fault if not successful.

The remaining conformance points in this section apply to requests correctly authenticated according to PRR.93.

- PRR.122 If the request identifies a `SealedPathologyResultReportInstance` held by the service provider for the `receiverOrganisation` that has not previously been removed, the service provider **MUST** respond to the request with an `ok` status if the removal operation is successful.
- PRR.123 If the request identifies a `SealedPathologyResultReportInstance` that has previously been removed by the `receiverOrganisation`, the service provider **SHOULD** respond to a `remove` request with an `alreadyRemoved` status.

Note that a service provider is not required to physically remove a `SealedPathologyResultReportInstance` in response to a `remove` request. It will, however, need to record the removal action to correctly implement `list`

and `remove` behaviour. This is intentional and allows the service provider to offer other services to providers, for example, an archive service.

7.2.4.3.1 *Faults*

The conformance points in this section apply to requests correctly authenticated according to PRR.93.

- PRR.124 The service provider **MUST** respond to a `remove` request with a `sds:removeError` or `se:standardError` fault if an error occurs in processing the `remove` request.
- PRR.125 The service provider **MAY** respond to a `remove` request with a fault containing a `se:standardError` element as defined by [WSP2009].
- PRR.126 If the request does not identify a `SealedPathologyResultReportInstance` held by the service provider for the `receiverOrganisation`, the service provider **MUST** respond to a `remove` request with a `removeError` fault having the `errorCode` set to `unknownInstance`. The service provider **SHOULD** include a human-readable string describing the problem in the `message` element of the fault.
- PRR.127 If the request identifies a `SealedPathologyResultReportInstance` that has not previously been retrieved successfully by the `receiverOrganisation`, the service provider **MUST** respond to the request with a `removeError` fault having the `errorCode` set to `hasNotBeenRetrieved`. The service provider **SHOULD** include a human-readable string describing the problem in the `message` element of the fault.

8 WSDL: Sealed Acknowledgement Consumer

8.1 Introduction

8.1.1 Purpose

This service interface is implemented by Senders or their Intermediaries to receive acknowledgements for pathology result reports from Receivers.

8.1.2 Identity

This service is identified by the following service category:

`http://ns.nehta.gov.au/Pth/Sc/SealedAcknowledgementConsumer/3.0-draft-20090630`

A Sender MUST publish sealed acknowledgement consumer service instances in an ELS under this service category. Note that the publication action might be performed by an Intermediary on behalf of a Sender.

The WSDL schema for this service is defined in the following namespace:

`http://ns.nehta.gov.au/Pth/Wsd/SealedAcknowledgementConsumer/3.0-draft-20090630`

This namespace is subsequently identified using the namespace prefix `sac:`.

The service interface for implementations that comply with the TLS Security Profile is identified by:

`http://ns.nehta.gov.au/Pth/Intf/SealedAcknowledgementConsumer/TLS/3.0-draft-20090630`

PRR.128 Senders MUST use this interface identifier when publishing sealed acknowledgement consumer service instances implementing the TLS security profile in an ELS.

8.1.3 Overview

This service interface is illustrated in Figure 8.

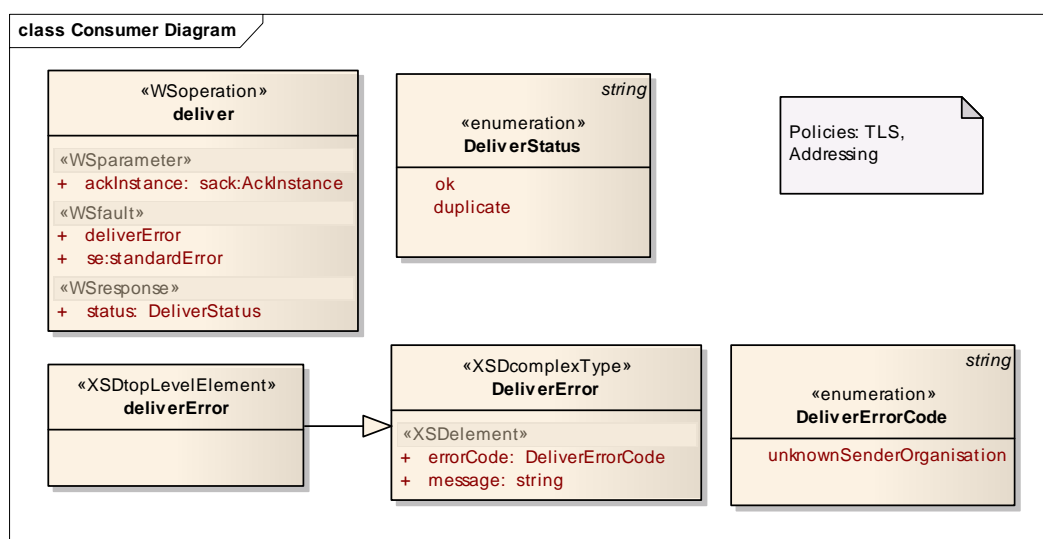


Figure 8: Components of the Sealed Acknowledgement Consumer service interface

8.2 Operations

8.2.1 deliver

8.2.1.1 Purpose

This operation is used to deliver a message containing the Sealed Acknowledgement to a Sender or the Sender's Intermediary. A Receiver invokes `deliver` to acknowledge each pathology result report received from a Sender. The following conformance points associated with the `deliver` operation are in addition to the endpoint conformance points defined in sections 2, 3 and 4.

In the following subsections, the service invoker is a Receiver, and the service provider is a Sender or Intermediary. The term 'sealed pathology result report' refers to the particular sealed pathology result report being acknowledged by this invocation.

8.2.1.2 Request

The request contains a signed then encrypted acknowledgement and metadata to assist in delivering the acknowledgement. The following conformance points apply:

- PRR.129 The service invoker **MUST** send a `sac:deliver` request.
- PRR.130 The service invoker **MUST** set the encrypted payload `sack:ep` using XSP [XSP2009] to sign then encrypt an `ackd:AckDocument` instance.
- PRR.131 If the sealed pathology result report was successfully processed, the service invoker **MUST** set the `sack:successful` flag to `true`. Otherwise, the service invoker **MUST** set the `sack:successful` flag to `false`.
- PRR.132 The service invoker **MUST** set the `sack:senderOrganisation` and `sack:receiverOrganisation` elements to qualified identifier values [QI2008] for the Sender and Receiver respectively using one of the identifier types specified by PRR.7 in section 1.5. Note that 'sender' in this context refers to the original sender of the pathology result report (not the acknowledgement) and the 'receiver' refers to the original receiver of the pathology result report.

8.2.1.3 Response

The response indicates whether the operation succeeded or not. The following conformance points apply:

- PRR.133 The service provider **MUST** return a `sac:deliver` response.
- PRR.134 The service provider **MUST NOT** return a successful response until after the sealed acknowledgement is successfully stored in non-volatile storage.
- PRR.135 The service provider **MUST NOT** store more than one sealed acknowledgement from a particular service invoker with the same `sack:invocationId` (i.e. no duplicates stored).
- PRR.136 If request has the same `sack:invocationId` as a previous request from the same service invoker and processing of the previous request was successful, then the service provider **MUST** return a status of `sac:duplicate` in the response.

8.2.1.3.1 Faults

Faults indicate that an error has occurred at the service provider.

- PRR.137 The service provider **MUST** respond with a `sdc:deliverError` or `se:standardError` fault if an error occurs in processing the `deliver` operation.
- PRR.138 The service provider **MUST** respond with a `sdc:deliverError` fault if the `sop:senderOrganisation` element of the request does not identify the service provider or a Sender that has explicitly engaged the service provider as per PRR.67 in section 4.4.2. In this case the service provider **MUST** also discard the sealed acknowledgement.

9 WSDL: Sealed Acknowledgement Supplier

9.1 Introduction

9.1.1 Purpose

This service interface is implemented by Intermediaries to make sealed acknowledgements available for Senders to retrieve.

9.1.2 Identity

This service is identified by the following service category:

`http://ns.nehta.gov.au/Pth/Sc/SealedAcknowledgementSupplier/3.0-draft-20090630`

PRR.139 An Intermediary MUST publish sealed acknowledgement supplier service instances in an ELS under this service category

The WSDL schema for this service is defined in the following namespace:

`http://ns.nehta.gov.au/Pth/Wsd1/SealedAcknowledgementSupplier/3.0-draft-20090630`

This namespace is subsequently identified using the namespace prefix `sas:`.

The service interface for implementations that comply with the TLS Security Profile is identified by:

`http://ns.nehta.gov.au/Pth/Intf/SealedAcknowledgementSupplier/TLS/3.0-draft-20090630`

PRR.140 Intermediaries MUST use this interface identifier when publishing sealed message consumer service instances implementing the TLS security profile in an ELS.

9.1.3 Overview

This service interface is illustrated in Figure 9.

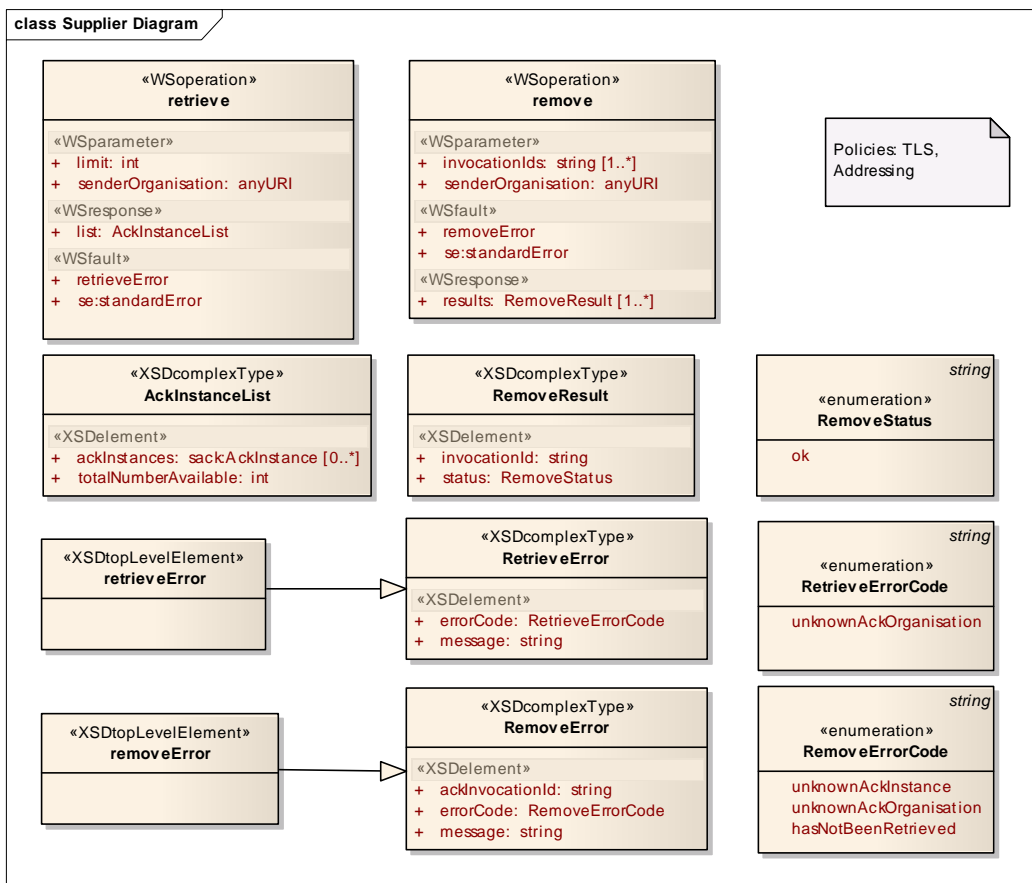


Figure 9: Components of the Sealed Report Acknowledgement supplier service interface

9.2 Operations

This service interface defines two operations:

- `retrieve`; and
- `remove`.

A Sender would invoke `retrieve` to retrieve a set of acknowledgements that are available from an Intermediary, then invoke `remove` to indicate that a set of acknowledgements has been successfully retrieved and safely stored.

For both operations, the service invoker is a Sender and the service provider is an Intermediary. Conformance points in the following subsections are in addition to the conformance points for Sender and Intermediary specified in sections 2 and 3 respectively.

9.2.1 Common Behaviours

The following conformance points apply to all invocations on the interface.

- PRR.141 The service invoker MUST identify itself in all requests by setting the `sas:ackOrganisation` element using one of the identifier types specified by PRR.7 in section 1.5.
- PRR.142 The service provider SHOULD reject or ignore requests where the `sas:ackOrganisation` element does not match the organisation associated with the security certificate used by the service invoker.
- PRR.143 If the organisation identified in the `ackOrganisation` element of a request does not identify a client of the service provider, the service provider SHOULD respond to a request with a fault having the `errorCode` set to `unknownAckOrganisation`. The service

provider SHOULD include a human-readable string describing the problem in the `message` element of the fault.

9.2.2 retrieve

9.2.2.1 Purpose

This operation is used by the Sender to retrieve a list of acknowledgements.

9.2.2.2 Request

PRR.144 The service invoker MUST send a `retrieve` request.

PRR.145 The service invoker SHOULD set the `limit` element to zero or a positive integer to indicate the maximum number of items to return in the `list` element of the response. The service invoker MAY set the `limit` element to a negative value to indicate that any number of items can be returned.

9.2.2.3 Response

The response contains a list of `sack:SealedAcknowledgementInstances`, including both the metadata and the signed and encrypted payload.

PRR.146 The service provider MUST return a `retrieve` response if successful.

PRR.147 The service provider MUST return a `retrieve` fault if not successful.

The remaining conformance points in this section apply to requests correctly authenticated according to PRR.142.

PRR.148 The service provider MUST set the `totalNumberAvailable` element of the response to indicate the total number of acknowledgement instances currently available for the `ackOrganisation` identified in the request.

PRR.149 The service provider MUST NOT count any sealed acknowledgement instances that have been removed by the `ackOrganisation` in the response when setting the value of the `totalNumberAvailable` element.

PRR.150 The service provider MUST NOT return any sealed acknowledgement instances that have been removed by the `ackOrganisation` in the response.

PRR.151 If the service provider has acknowledgements available for the identified receiver and the request `limit` element is greater than zero, the service provider MUST return at least one sealed acknowledgement instance.

PRR.152 If the `limit` element of the request is a positive integer, the service provider MUST NOT return more than this number of sealed acknowledgement instances in the response.

PRR.153 If the `limit` element of the request is equal to zero, the service provider MUST NOT return any sealed acknowledgement instances. Note that the `totalNumberAvailable` should still be returned as per PRR.148. This allows the invoker to determine the number of acknowledgements without retrieving them.

PRR.154 For each sealed acknowledgement instance in the response, the service provider must return the unmodified payload received by the service provider through an invocation on its `SealedAcknowledgementConsumer` interface.

9.2.2.3.1 *Faults*

- PRR.155 The service provider **MUST** respond to a `retrieve` request with a `sas:retrieveError` or `se:standardError` fault if an error occurs in processing the `retrieve` request.
- PRR.156 The service provider **MAY** respond to a `retrieve` request with a fault containing a `se:standardError` element as defined by [WSP2009].

9.2.3 **remove**

9.2.3.1 Purpose

This operation is used by a Sender to indicate that a set of acknowledgements have been retrieved and stably stored by the Sender.

9.2.3.2 Request

- PRR.157 The service invoker **MUST** send a `remove` request.
- PRR.158 The service invoker **MUST NOT** send a `remove` request for a `SealedAcknowledgementInstance` that has not previously been received and stably stored.

9.2.3.3 Response

The response indicates whether the operation succeeded or not using the enumerated values in the `RemoveStatus` `simpleType` (see section 9.1.3).

- PRR.159 The service provider **MUST** return a `remove` response if successful.
- PRR.160 The service provider **MUST** return a `remove` fault if not successful.

The remaining conformance points in this section apply to requests correctly authenticated according to PRR.142.

- PRR.161 If all `invocationIds` in the request identify `SealedAcknowledgementInstances` held by the service provider for the `ackOrganisation` that have not previously been removed, the service provider **MUST** respond to the request with an `ok` status if the removal operation is successful for all `invocationIds`.

9.2.3.3.1 *Faults*

The conformance points in this section apply to requests correctly authenticated according to PRR.142.

- PRR.162 The service provider **MUST** respond to a `remove` request with a `sas:removeError` or `se:standardError` fault if an error occurs in processing the `remove` request.
- PRR.163 The service provider **MAY** respond to a `remove` request with a fault containing a `se:standardError` element as defined by [WSP2009].
- PRR.164 If one or more `invocationIds` in the request do not identify a `SealedAcknowledgementInstance` held by the service provider for the `ackOrganisation`, the service provider **MUST** respond to a `remove` request with a `removeError` fault having the `errorCode` set to `unknownInstance` and list each unknown acknowledgements `invocationId` as a comma separated list of strings in the message element of the fault.
- PRR.165 If PRR.164 does not apply and one or more `invocationIds` in the the request identify a `SealedPathologyResultReportInstance` that has not previously been retrieved successfully by the

`ackOrganisation`, the service provider MUST respond to the request with a `removeError` fault having the `errorCode` set to `hasNotBeenRetrieved` and list each unretrieved acknowledgement `invocationId` as a comma separated list of strings in the message element of the fault.

Definitions

This section explains the specialised terminology used in this document.

Shortened Terms

This table lists abbreviations and acronyms in alphabetical order.

Term	Description
HPI-O	Healthcare Provider Identifier for Organisations
HPI-I	Healthcare Provider Identifier for Individuals
URI	Uniform Resource Identifier
UUID	Universally Unique Identifier
WSDL	Web Services Description Language
XML	Extensible Markup Language

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 Pathology Result Reporting Specification.

Pathology Result Reporting Specification Documents			
[REF]	Document Name	Publisher	Link
[PRR-TBP]	Pathology Result Reporting: Request-Test-Report "To Be" Process	NEHTA Pending	
[PRR-SDT]	Pathology Result Reporting: Structured Document Template	NEHTA 2009	
[PRR-IF]	Pathology Result Reporting: Interchange Format Endpoint Specifications	NEHTA 2009	
[PRR-ES]	Pathology Result Reporting: Endpoint Specifications	NEHTA 2009	
[PRR-WX]	Pathology Result Reporting: Endpoint Specifications: WSDL and XML Schema files v3.0 draft 2009-06-30.	NEHTA 2009	

References

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

Reference Documents			
[REF]	Document Name	Publisher	Link
[EAMJ2008]	Enterprise Architecture Mapping for Jurisdictions Version 2.0,	NEHTA 2008	Reference in preparation for future release.
[IDMG2007]	Identity Management Glossary of Terms v1.0	NEHTA 2007	Reference in preparation for future release.
[INTER2007]	Interoperability Framework v2.0	NEHTA 2008	 Publications)">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	 Publications)">http://www.nehta.gov.au/(Home > Publications)
[UHI-CO]	Unique Healthcare Identification – Concept of Operations	NEHTA 2007	 Publications)">http://www.nehta.gov.au/(Home > Publications)
[WSP2009]	Web Services Profile v3.1	NEHTA 2009	

[XSP2009]	XML Secured Payload Profile v1.2	NEHTA 2009	
[QI2008]	Qualified Identifiers v1.0	NEHTA 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.
[RFC2119]	RFC 2119: Keywords for use in RFCs to Indicate Requirement Levels	IETF 1997	http://ietf.org/rfc/rfc2119.txt
[RFC3986]	RFC 3986: Uniform Resource Identifier (URI): Generic Syntax	IETF 2005	http://ietf.org/rfc/rfc3986.txt
[RFC4122]	RFC 4122: A Universally Unique Identifier (UUID) URN Namespace	IETF 2005	http://ietf.org/rfc/rfc4122.txt
[RFC5280]	RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	IETF 2008	http://ietf.org/rfc/rfc5280.txt

Known Issues

This section lists known issues for this document. The identified issues will be addressed in subsequent releases.

Reference	Description
	A number of the XML schemas presented in section 5.4 are likely to be shared by multiple NEHTA specifications in future, allowing implementers to use a single implementation for all specifications. In particular, the message metadata will most likely be split into standard and specific components to allow domain-specific metadata (e.g. business process correlation identifiers).
	For consistency across implementations, it is possible that the transport acknowledgement defined in section 5.4.3 will exclude the option for application payload in future versions. An application response would be carried in a separate messaging interaction.
	If the pending "to be" analysis of the pathology business process identifies a need for an application acknowledgement, it is possible that the transport acknowledgement interfaces defined here in sections 8 and 9 will become redundant and might be removed or become optional.
	Uses cases that require an intermediary or sending agent to have access to clinical payload (e.g. for application service provider services) have been identified in other NEHTA work. The requirements for signing, encryption and verification of certificates might be modified in future to permit such access.
	The specification includes explicit timing requirements relating to delivery and acknowledgements, for example PRR.28. It is likely that these requirements will be modified or parameterised according to the results of the pending "to be" analysis.
	The specification includes explicit escalation points relating to failures, for example PRR.36. These requirements will be reviewed and possibly modified as a result of the pending "to be" analysis.
	The specification explicitly references the ELS interface for registration and retrieval of service interface details. While this function and its metadata will remain, it is possible that the mechanism for registration and retrieval of services will be decoupled from the specification, removing explicit references to ELS.
	The specification is currently limited to pathology report delivery and does not include any semantics for report amendments, cancellations or any other derived functions. While the transport mechanism and interchange format permits these functions to be identified in the HL7 payload, subsequent versions of the specification will most likely include explicit semantics for these additional functions.
	This specification has been developed in parallel with a payload agnostic secure messaging mechanism currently known as "Clinical Document Delivery". It is likely that future versions of this specification will permit pathology reporting functions to be implemented using the payload agnostic mechanism as an alternative. If this occurs, deterministic transformations will be defined to allow bridging between implementations.