nehta

P2P Document Delivery

Technical Service Specification

Version 1.1 — 14 March 2012

Final

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

Document Information

Version	Date	Comments
0.01	2011-11-24	Draft for review.
0.02	2011-11-24	Draft for review.
1.0	2011-11-29	Released to vendors
1.1	2012-03-14	Re-released with amendments listed in appendix A

Table of Contents

This page is intentionally left blank.

Preface

Document Purpose

This document is a Technical Service Specification (TSS) for the secure point-to-point delivery of clinical documents. It provides coverage of the Implementable Specification layer as defined in the National eHealth Framework (NeHF).

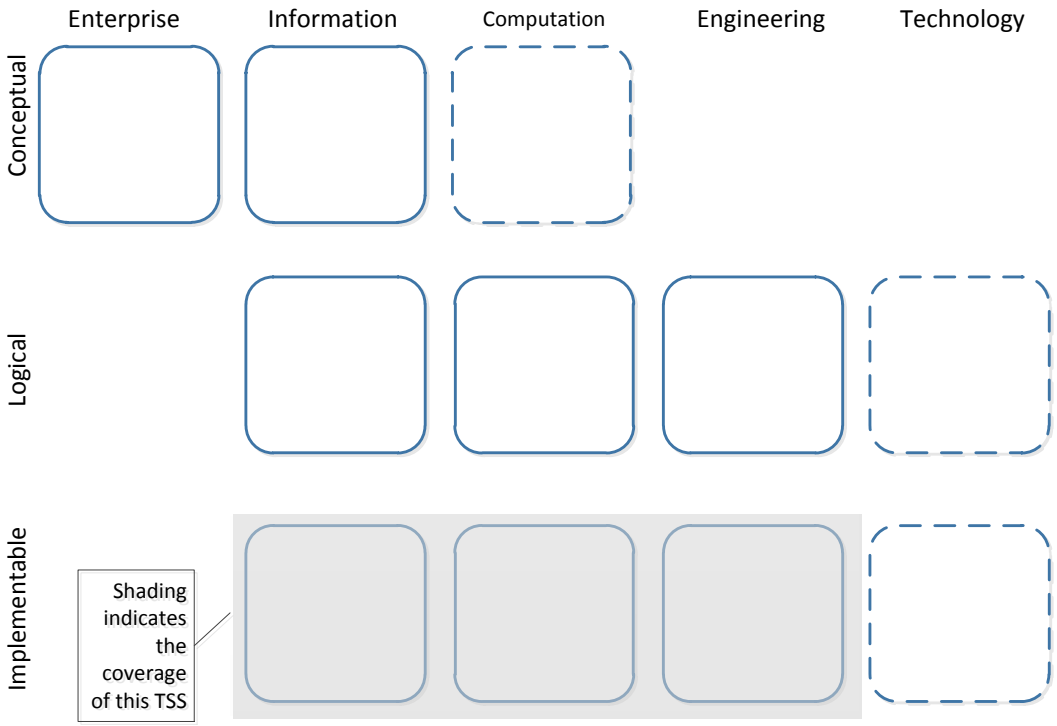

Figure 1: Relationship to National eHealth Framework

The purpose of this P2P Document Delivery TSS is to specify compliance points for systems that are used to securely send clinical documents between service instances that are operated by (or on behalf of) healthcare provider organisations. This capability meets the common document delivery requirements of clinical processes that rely on clinical documents being sent across organisational boundaries (e.g. discharge and referral processes).

This P2P Document Delivery TSS is an "implementable" specification; it is a specific realisation of the P2P Document Delivery Logical Service Specification that is based on the following:

- Secure Message Delivery in accordance with ATS 5822—2010
- Endpoint Location Services in accordance with *ELS Service Technical Service Specification* [ELSTSS].
- HI Provider Directory service in accordance with *Healthcare Identifiers (HI) Service System Interface Specification (SIS), Healthcare Provider Directory Search for Organisation Provider Directory Entry*, TECH.SIS.HI.18 [HISIS18].
- CDA Packaging in accordance with CDA Package Specification [CDAPACK]

Note that the intention is that NASH will provide the implementation of the PKI that is referenced in [ATS5822], [ELSTSS] and [CDAPACK]. Until NASH is available the PKI that is used shall be unspecified.

Intended Audience

This document is intended primarily for those who are responsible for the specification and implementation of products that are concerned – at least in part – with the secure delivery of clinical documents between healthcare provider organisations. This audience therefore includes (but is not limited to):

- The Australian Healthcare standards development community
- Jurisdictions and Medicare Australia
- Organisations that supply software products and services to the healthcare industry

This document makes use of the UML2.3 standard [UML2.3]. Familiarity with UML and service oriented architecture concepts and patterns are assumed.

Definitions, Acronyms and Abbreviations

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

References and Related Documents

For lists of referenced documents, see the References section at the end of the document, on page 19.

1 Introduction

1.1 Support for clinical workflows

Provider-to-Provider (P2P) Document Delivery is the capability for a document package (a "root" clinical document plus its associated attachments) to be sent from one system to the system that is operated by (or on behalf of) a *Document Receiver* that is identified by the *Document Issuer*.

This capability is in contrast to the use of a repository (for example the PCEHR repository) to support the sharing of a clinical document amongst a group of users where the members of that group are not pre-determined by the *Document Issuer*.

The P2P Document Delivery capability is intended to support the common requirements of a range of different clinical workflows that depend on the transfer of clinical documents (including Discharge Summary, eReferral and Specialist Letters) across organisational boundaries.

1.2 Relationship to P2P Document Delivery LSS

A platform independent specification of the technical services necessary to support the P2P Document Delivery capability is presented in the P2P Document Delivery Logical Service Specification (LSS)[1].

The P2P Document Delivery LSS does not mandate particular technologies as the basis for implementation and as such is not implementable.

This technical service specification builds upon the P2P Document Delivery LSS by identifying specific technologies for elements of the LSS.

The TSS is sufficient for the implementation of interoperable Clinical Information Systems (CISs) that fulfil the systems roles of "Issuing CIS" and "Externally Issued Documents Repository" that are defined in the P2P Document Delivery LSS (shown in Figure 2 below).

[1] See [P2P-LSS].

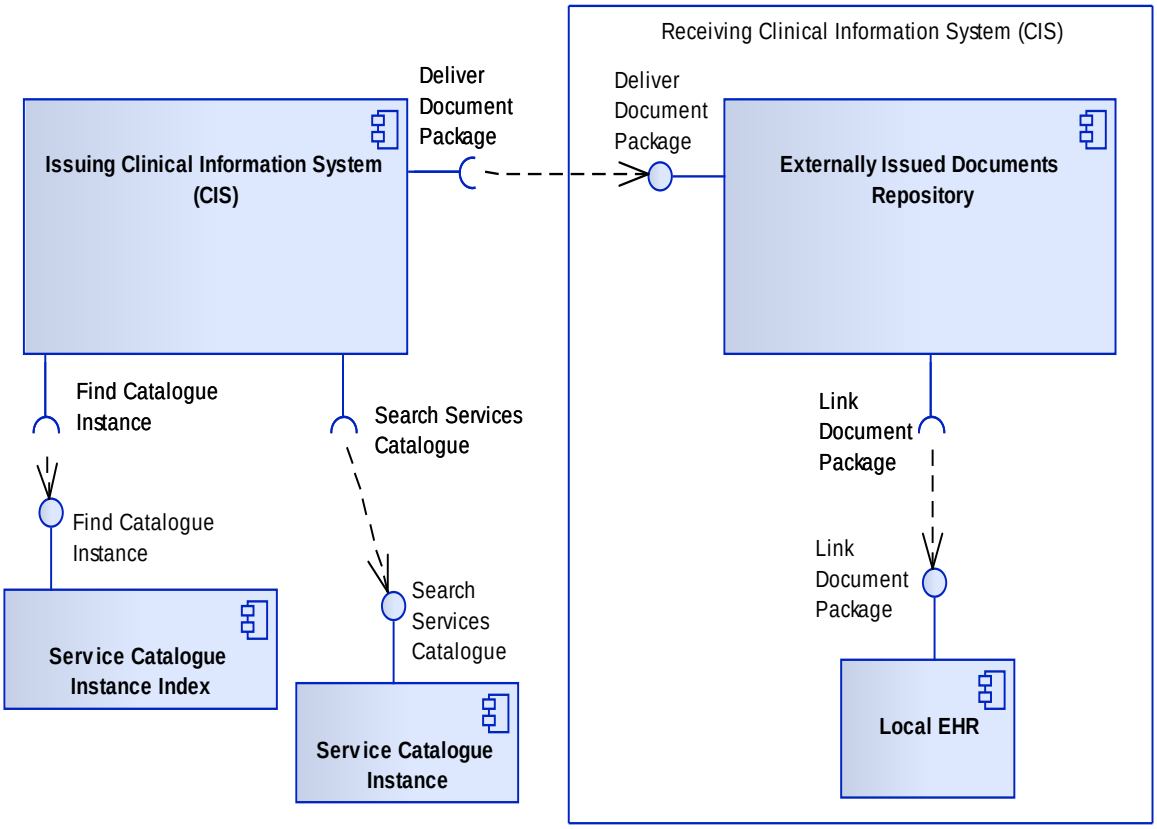

Figure 2: Logical P2P Document Delivery Architecture

ELS and the HI Provider Directory support the implementation of the Service Catalogue Instance and Service Catalogue Instance Index respectively.

The implementation of the Local EHR is not constrained by this TSS – i.e. systems that fulfil these roles must comply with the functional system requirements of the P2P Document Delivery LSS, and with any other specifications that apply to these systems independently of their usages to support P2P Document Delivery.

1.3 Overview of the standards and technology platform

The technology platform for this technical service specification is comprised of:

- The transfer of service request and service response messages between Issuing CISs and Receiving CISs using the Secure Message Delivery specification [ATS5822].
- The packaging of clinical documents together with their attachments and digital signatures, in accordance with the CDA Packaging specification [CDAPACK].
- The use of ELS (in accordance with [ELSTSS]) and the HI Provider Directory (in accordance with [HISIS18]) to provide the implementation of the Service Catalogue Instance and Service Catalogue Instance Index respectively.
- The use of HPI-Os to identify the Document Issuer and Document Receiver (i.e. the organisation on whose behalf the Issuing CIS and Receiving CIS are operated).

2 Computational Viewpoint

The computational viewpoint is concerned with describing the functional decomposition of the system into computational objects which interact at their interfaces, including descriptions of services that objects offer and other objects consume, i.e. service contracts in general terms. These objects describe the key functionality of the system to be built, while assuming that necessary infrastructure support and services are specified elsewhere, using engineering and technology viewpoint concepts described below.

This section of the document contains conformance statements that specify the services in terms of the messages exchanged, the processing required of a service invoker prior to invoking a service, the dependency between the response messages generated and the request message and the prior state of the service provider, the resulting effect (if any) on the state of the service provider and the required processing of response message by the service invoker.

2.1 Externally Issued Documents Repository

The following conformance points apply to systems that fulfil the system role of Externally Issued Documents Repository; they are additional to conformance points contained in the P2P Document Delivery LSS that also apply to the Externally Issued Documents Repository system role.

2.1.1 Deliver Document Package logical service interface

2.1.1.1 Secure Message Delivery

P2P T1 An Externally Issued Documents Repository SHALL implement the Receiver role of the E-Health Secure Message Delivery (SMD) specification [ATS5822] for the receipt of service requests for the `Deliver Document Package` logical service interface.

2.1.1.2 Service Categories

The following conformance points define service categories published by the Externally Issued Documents Repository system.

Service categories for P2P Document Delivery are of the following form:

`http://ns.electronichealth.net.au/<documentType>/sc/deliver/<payloadType>/2012`

where:

- <payloadType> defines the format of the contents of the SMD Signed Payload that the Externally Issued Documents Repository is capable of receiving (see section 3.1). This specification defines behaviour for the case where <payloadType> is "`xdmZip`".
- <documentType> is the type of document that the Externally Issued Documents Repository is capable of receiving.

A service category of this form is referenced as [P2P Service Category].

P2P T2 When publishing an SMD Receiver endpoint in a service directory for receipt of service requests for the `Deliver Document Package` logical service interface, an Externally Issued Documents Repository SHALL use the service category [P2P Service Category] where the <payloadType> is "`xdmZip`".

2.1.1.3 `deliver` operation

P2P T3a On receipt of a sealed message where the service category is of the form [P2P Service Category] and where the <payloadType> is "`xdmZip`", an Externally Issued Documents Repository SHALL decode the [PAYLOAD-CDA-PACK] consistent with Section 6 of [CDAPACK].

P2P T3b Upon decoding a [PAYLOAD-CDA-PACK], an Externally Issued Document Repository SHALL process it in accordance with section 2.2.3.2 of the P2P Document Delivery LSS where the `documentType` logical operation parameter is obtained by parsing the service category and the `package` logical operation parameter is obtained by processing the message payload as [PAYLOAD-CDA-PACK] Signed CDA Package.

P2P T4 If no fault conditions occur then the Externally Issued Documents Repository SHALL set the responseClass of the final TransportResponse to Success.

2.2 Issuing CIS

2.2.1 Deliver Document Package logical service interface

2.2.1.1 Secure Message Delivery

P2P T5 An Issuing CIS SHALL implement the Sender role of the E-Health Secure Message Delivery specification [ATS5822] for the sending of service requests for the `Deliver Document Package` logical service interface.

2.2.1.2 Service Categories

The following conformance points define service categories published by the Issuing CIS.

P2P T6 When searching for Receiver endpoints that can receive requests for the `Deliver Document Package` logical service interface, an Issuing CIS SHALL use the service category of the form [P2P Service Category] where <documentType> is the type of document that the Issuing CIS is sending and <payloadType> is "`xdmZip`".

2.2.1.3 `deliver` operation

P2P T7 An Issuing CIS SHALL conform to section 2.4 of the P2P Document Delivery LSS in preparing a `Deliver Document Package` logical service interface service request.

P2P T8a An Issuing CIS SHALL construct a [PAYLOAD-CDA-PACK] containing the document the Issuing CIS is sending.

P2P T8b If the Issuing CIS is sending to an `deliver` endpoint using a service category of the form [P2P Service Category] where <payloadType> is "`xdmZip`" then the Issuing CIS SHALL encode the [PAYLOAD-CDA-PACK] in XDM-ZIP representation conformant with Section 6 of [CDAPACK].

P2P T8c The Issuing CIS shall send the encoded [PAYLOAD-CDA-PACK] in accordance to the Sender Role of [ATS5822].

P2P T9 In response to the receipt of a final `TransportResponse` that has a `responseClass` value equal to `Success`, an Issuing CIS SHALL process the response in accordance with section 2.4 of the P2P Document

Delivery LSS for the case where a `DeliveryAck` has been received with the value of the `isSuccessful` attribute equal to `TRUE`.

P2P T10 In response to the receipt of a final `TransportResponse` that has a `responseClass` value equal to `Error`, then an Issuing CIS SHALL process the response in accordance with section 2.4 of the P2P Document Delivery LSS for the case where a `DeliveryAck` has been received with the value of the `isSuccessful` attribute equal to `FALSE`.

P2P T11 If a final `TransportResponse` has not been received within a timeout period specified in the relevant deployment policy, an Issuing CIS SHALL process the lack of response in accordance with section 2.4 of the P2P Document Delivery LSS for the case where a `DeliveryAck` has been received with the value of the `isSuccessful` attribute equal to `FALSE`, and a `failureReason` that indicates no `DeliveryAck` was received.

3 Informational Viewpoint

3.1 Deliver Document Package logical service

3.1.1 `deliver` logical operation

3.1.1.1 Service Request message

The service request messages for the `Deliver Document Package::deliver` logical operation are implemented as *CDA packages,* represented in the xdmZip format and carried as the message payload of the SMD `SealedMessage`. A request message in this form is referenced as a [PAYLOAD-CDA-PACK].

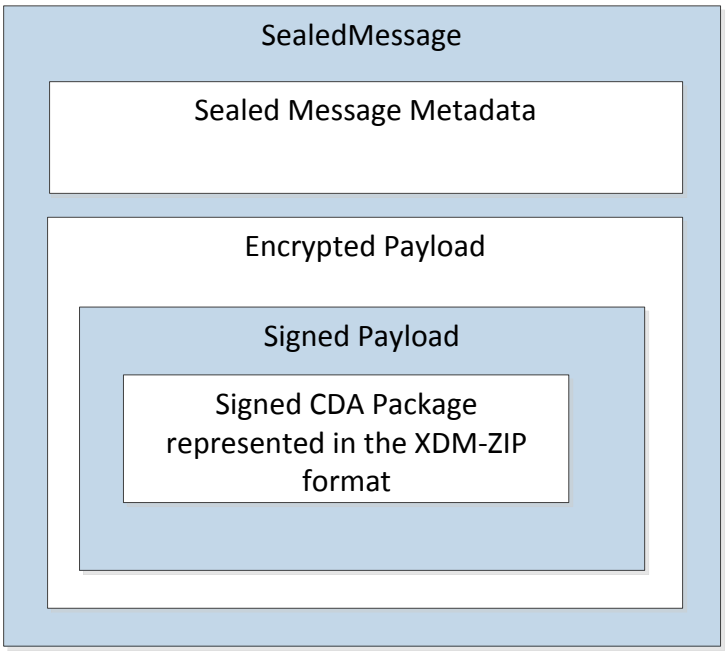

Figure 3: Deliver Document Package::deliver request

The logical input parameters are mapped as follows:

Logical input parameter	TS realization
`documentType`	A component of the service category structured identifier of the form defined in [P2P Service Category] defined in section 2.1.1.2
`package`	Sealed message payload containing the Signed CDA package represented in the xdmZip format – i.e. a [PAYLOAD-CDA-PACK]

P2P T12 A [PAYLOAD-CDA_PACK] SHALL be a profile of a Signed CDA Package as specified in [CDAPACK] that is represented in the xdmZip format.

P2P T13 An Issuing CIS SHALL NOT include the optional Repository Metadata part of the Signed CDA package.

P2P T14 A [PAYLOAD-CDA_PACK] SHALL contain an eSignature part which identifies the healthcare provider individual who is also identified in the CDA XML root part as the Document Author and is created using a certificate that asserts the identity of the healthcare provider organisation that is also identified as the value of the senderOrganisation element of the MessageMetadata element of the SealedMessage that contains the [PAYLOAD-CDA-PACK].

3.1.1.2 Service Response message

The service response messages for the `Deliver Document Package::deliver` logical operation are implemented as the final `TransportResponse`.

DeliveryAck.isSucessful	Final `TransportResponse.deliveryResponse.responseClass`
DeliveryAck.failureReason	Final `TransportResponse.deliveryResponse.responseCode` `TransportResponse.deliveryResponse.message`

4 Engineering Viewpoint

4.1 Introduction

This section contains conformance points that relate to the use of infrastructure services to implement the system roles.

4.2 Security and Access Controls

Issuing CISs and Externally Issued Documents Repositories are responsible for both the evaluation and enforcement of security policies that ensure that the personal information of subjects of care is transferred between these roles securely.

The security controls comprise:

- Issuing CISs are required to implement security controls that ensure that system users are duly authorised and authenticated before these users can authorise the release of a clinical document for delivery to a different organisation.
- Receiving CISs are required to implement security controls that ensure that system users are duly authorised and authenticated before these users can view clinical document received from a different organisation.
- The privacy of the personal health information, while it is in transit between an Issuing CIS and a Receiving CIS, is ensured using the controls defined in [ATS5822] – these can be summarised as:
  - Both communicating systems mutually authenticate each other
  - Personal health information is encrypted by the Issuing CIS using the public key of the Receiving CIS; secure messaging intermediaries therefore cannot access this information.
  - PKI Certificates are validated and managed securely

4.3 Identifiers

4.3.1 Issuing CIS

P2P T15 An Issuing CIS SHALL identify the *Document Issuer* using an HPI-O.

P2P T16 An Issuing CIS SHALL identify the *Document Receiver* using an HPI-O.

P2P T17 An Issuing CIS SHOULD identify the *Subject of Care* using an IHI.

P2P T18 An Issuing CIS SHOULD identify the *Author* using an HPI-I.

P2P T19 An Issuing CIS SHOULD identify the *Recipient* using an HPI-I.

4.3.2 Externally Issued Documents Repository

P2P T20 An Externally Managed Documents Repository SHALL identify the *Document Issuer* using an HPI-O.

P2P T21 An Externally Managed Documents Repository SHALL identify the *Document Receiver* using an HPI-O.

P2P T22 An Externally Managed Documents Repository SHOULD identity the *Subject of Care* using an IHI.

P2P T23 An Externally Managed Documents Repository SHOULD identify the *Author* using an HPI-I.

P2P T24 An Externally Managed Documents Repository SHOULD identify the *Recipient* using an HPI-I.

4.3.3 Local EHR

P2P T25 A Local EHR SHALL identify the *Document Issuer* using an HPI-O.

P2P T26 A Local EHR SHALL identify the *Document Receiver* using an HPI-O.

P2P T27 A Local EHR SHOULD identify the *Subject of Care* using an IHI.

P2P T28 A Local EHR SHOULD identify the *Author* using an HPI-I.

4.4 Directory services

4.4.1 Issuing CIS

P2P T29 An Issuing CIS SHALL invoke the Healthcare Provider Directory, Search for Organisation Provider Directory Entry, in accordance with Department of Human Services specifications, as the implementation of the `Find Catalogue Instance` logical service interface.

P2P T30 An Issuing CIS SHALL invoke the ELS Lookup service interface in accordance the NEHTA Endpoint Location Service, Technical Service Specification, as the implementation of the `Search Services Catalogue` logical service interface.

4.4.2 Receiving CIS

A *Document Receiver* (i.e. an organisation response for a given Externally Managed Documents Repository) is required to interact with the HI service provider to ensure their HPI-O is available in the HPD and that their HPD entry contains the location of their ELS provider.

Definitions

This section explains the specialised terminology used in this document.

Shortened Terms

This table lists abbreviations and acronyms in alphabetical order.

Term	Description
CDA	Clinical Document Architecture
CIS	Clinical Information System
ELS	Endpoint Locator Service
EHR	Electronic Health Record
HL7	Health Level 7
HPD	Healthcare Provider Directory
IETF	Internet Engineering Task Force
LSS	Logical Solution Specification
NeHF	National eHealth Framework
P2P	Provider to Provider
SMD	Secure Message Delivery
TSS	Technical Solution Specification
XML	Extensible Markup Language
URI	Uniform Resource Identifier

Glossary

This table lists specialised terminology in alphabetical order.

Term	Description
Service interface	The definition of the functionality of a service
Service implementation	A product (i.e. software) that conforms to a service interface
Service instance	A specific deployment of a service implementation

References

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.

[REF]	Document Name	Publisher
[ATS5822]	Australian Technical Specification – E-Health Secure Message Delivery	Standards Australia 2010
[CDAPACK]	CDA Package 1.0	NEHTA 2011
[ELSTSS]	Endpoint Location Service Technical Service Specification, version 1.3, 15 November 2010	NEHTA 2010
[HISIS18]	Healthcare Identifiers (HI) Service System Interface Specification (SIS), Healthcare Provider Directory Search for Organisation Provider Directory Entry, TECH.SIS.HI.18	Dept. Human Services (Medicare Australia) 2010
[P2PLSS]	P2P Document Delivery Logical Service Specification, v1.0	NEHTA 2011

Related Reading

The documents listed below may provide further information about the issues discussed in this document.

[REF]	Document Name	Publisher
[IF2007]	Interoperability Framework v2.0	NEHTA 2007
[UMLODP]	ITU-T Rec. X.906 | ISO/IEC 19793: Information technology - Open distributed processing - Use of UML for ODP system specifications	ITU-T
[UML2.3]	OMG Unified Modeling Language (OMG UML), Superstructure, Version 2.3	OMG 2010

Appendix A: Log of Changes

This appendix lists the major changes and fixes applied to this document resulting from public feedback and internal testing.

Changes Version 1.0 November 2011 to Version 1.1 14 March 2012

ID	Document Reference		Change Type	Change Detail	Change instigated by	Rational for Change	Date Changed
	Section	Section Name					
1	Page iii	Document Information	Changed Document Information section	Removed Contributor column form Change History Modified comment for version 1.0 Removed Authorisation History Removed Document Authorisation	NEHTA	Alignment with NEHTA document information standards	02/03/2012
2	Page iii	Document Information	Added row to table	Added version 1.1	NEHTA	New version	02/03/2012
3	2.1.1.2	Service categories	Changed word	Changed "used" to "published"	NEHTA	Clarification	02/03/2012
4	2.1.1.2	Service categories	Added quotes	Changed first dot point to add missing quotes to indicate that xdmZip a string literal value	NEHTA	Defect rectification	02/03/2012
5	2.1.1.2	Service categories	Added quotes	Changed P2P T2 to add missing quotes to indicate that xdmZip a string literal value	NEHTA	Defect rectification	02/03/2012
6	2.1.1.3	Deliver	Added quotes	Changed P2P T3 to add	NEHTA	Defect rectification	02/03/2012

ID	Document Reference		Change Type	Change Detail	Change instigated by	Rational for Change	Date Changed
		operation		missing quotes to indicate that xdmZip a string literal value			
7	2.1.1.3	Deliver operation	Split conformance point	Split P2P T3 in two to resolve ambiguity	NEHTA	Clarification	02/03/2012
8	2.2.1.2	Service categories	Changed word	Changed "used" to "published"	NEHTA	Clarification	02/03/2012
9	2.2.1.2	Service categories	Added quotes	Changed P2P T6 to add missing quotes to indicate that xdmZip a string literal value	NEHTA	Defect rectification	02/03/2012
10	2.2.1.2	Service categories	Changed word	Changed "systems" to "Receiver endpoints" to reconcile language with 2.1.1.2.	NEHTA	Clarification	02/03/2012
11	2.2.1.3	Deliver operation	Added quotes	Changed P2P T8 to add missing quotes to indicate that xdmZip a string literal value	NEHTA	Defect rectification	02/03/2012
12	2.2.1.3	Deliver operation	Split conformance point	Split P2P T8 into three to resolve ambiguity	NEHTA	Clarification	02/03/2012
13	2.2.1.3	Deliver operation	Added conformance point	P2P T14 added to specify behaviour in unhandled error condition	NEHTA	Defect rectification	02/03/2012
14	3.1.1.1	Service Request message	Added definition	Introduced [PAYLOAD-CDA-PACK]	NEHTA	Defect rectification	02/03/2012
15	3.1.1.1	Service Request message	Changed conformance point	Changed conformance point P2p T11to define [PAYLOAD-CDA-PACK] for use in other conformance points	NEHTA	Clarification – simplify the expression of conformance points	02/03/2012
16	3.1.1.1	Service Request message	New conformance point	Added conformance point P2P T12a	NEHTA	This is a common conformance point	02/03/2012

ID	Document Reference		Change Type	Change Detail	Change instigated by	Rational for Change	Date Changed
						that was formerly re-stated in each document type specific TSS	
17	3.1.1.2	Service Response message	Changed word	Changed `TransportResonse to TransportResponse`	NEHTA	Defect rectification	02/03/2012
18	4.3.1	Issuing CIS	Changed conformance point	Changed "Document Receiver" to "Recipient" in P2P T17	NEHTA	Defect rectification	02/03/2012
19	4.3.2	Externally Issued Documents Repository	Changed conformance point	Changed "Document Receiver" to "Recipient" in P2P T12	NEHTA	Defect rectification	02/03/2012