

nehta

e-Referrals

Solution Design

Version 1.0 - 17 December 2010

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 © 2010, 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	Contributor	Comments
1.0 draft	2010-08-30	Kevin Lin	Release 1.0
1.0	2010-12-17	Paul Smith	Final release

Document Authorisation


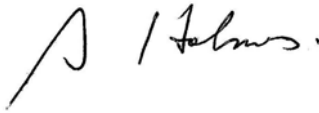
Name	Title	Signature
Paul Williams	Head of Information Services	
Sean Holmes	Program Manager, Continuity of Care	

Table of Contents

Document Information	iii
Change History	iii
Document Authorisation	iii
Table of Contents	iv
Preface	vii
Document Purpose	vii
Intended Audience.....	vii
Document Map.....	vii
Definitions, Acronyms and Abbreviations.....	viii
References and Related Documents	viii
1 Introduction	1
1.1 Overview.....	1
1.2 Referral Definition.....	1
1.3 Referral Process	2
1.4 Scope	2
1.4.1 Scope Inclusions.....	2
1.4.2 Scope Exclusions	2
1.5 Goals and Objectives.....	2
1.6 Dependencies	3
2 Solution States	4
2.1 Timeframes	4
2.2 Current	4
2.2.1 Assumptions	4
2.2.2 Constraints	4
2.2.3 High Level Solution View (Current)	5
2.2.4 Implementable Referrals Process (Current)	5
2.2.5 Referral Document Delivery Options (Current).....	6
2.3 Interim	7
2.3.1 Assumptions	7
2.3.2 Constraints	7
2.3.3 High Level Solution View (Interim)	7
2.4 Future.....	8
2.4.1 Assumptions	8
2.4.2 Referrals Process (Future)	9
2.4.3 High Level Solution View (Future).....	9
3 Business View	12
3.1 Roles and Services.....	12
3.1.1 Roles.....	12
3.1.2 Services	12
3.2 Safety and Quality in Healthcare	12
3.2.1 Implications for the Solution.....	12
3.2.2 Clinical Safety Management in e-Health.....	14
4 Information View	15
4.1 Introduction.....	15
4.2 Information Flows.....	15
4.3 Information Components	17
4.3.1 Overview	17
4.3.2 Referral	17
4.3.3 Terminology	18
4.3.4 Messages.....	19

4.3.5	Identification	19
4.3.6	Endpoint Location Service	20
4.4	Message Formats	21
4.4.1	Clinical Document Architecture (CDA)	21
4.4.2	HL7 v2.x	21
5	Technical View	22
5.1	Authentication and Security	22
5.1.1	Security Framework	22
5.1.2	Security Requirements	22
5.1.3	Secure Transmission	23
5.1.4	Certificates	23
5.2	Web Services Profiles	24
5.2.1	Web Services Specification	24
5.2.2	Transport	25
5.2.3	Protocol	25
5.2.4	Metadata	25
5.2.5	Security	25
5.3	Payload Encryption and Signing	26
5.3.1	Signed Container Profile	26
5.3.2	Encrypted Container Profile	26
5.3.3	XML Signature Profile	26
5.3.4	XML Encryption Profile	27
5.4	Referrals High Level Component Model	27
5.5	Referrals SOAP Payload Detail	28
5.5.1	HL7 CDA	28
5.5.2	Transport Level Signatures and Encryption	29
5.5.3	Plain Text Metadata	29
5.5.4	SOAP Payload	29
5.6	Message Exchange Scenarios	29
5.6.1	Referrer and Referee Host Web Services	29
5.6.2	Referrer and Referee do not host Web Services	29
5.6.3	Referrer uses a storage provider, Referee hosts Web Service	30
5.6.4	Referrer hosts Web Services, Referee uses a storage provider.	31
6	Implementation Approach	32
7	Compliance and Conformance	33
7.1	Introduction	33
7.1.1	Assessment	33
7.1.2	Declaration of conformance	33
7.1.3	Relevance for referrals	33
	Definitions	34
	Shortened Terms	34
	Glossary	34
	References	36
	Package Documents	36
	References	36
	Related Reading	37
	Appendix A: Sample e-Referrals Architecture	38
A.1	General Practitioner/Specialist Component Model	38
A.1.1	Clinical Information System (CIS)	38
A.1.2	Practice Management System (PMS)	39
A.1.3	Shared Components	40
A.1.4	Other Modules	41
A.1.5	Desktop Operating System Components	41
A.1.6	Gateway	41
A.1.7	External Components	42

A.2	Gateway Logical Components	42
A.2.1	Assembly and Dispatch	43
A.2.2	Foundation Service Gateways	46
A.2.3	Gateway Core Services	47
A.3	Foundation Services Gateway - Bootstrapping.....	48

Preface

Document Purpose

This Solution Design document serves as the technical anchor-point for the e-Referrals package, and builds upon the context-related discussion of the Business Requirements Specification. As such, it is suggested that readers familiarise themselves with both these documents before moving to the Core Information Components document.

The e-Referrals package describes the standards and guidelines to be adopted by implementers when developing interoperable referral-related solutions (refer to section 1.4 for the exact scope of the package) within the Australian healthcare community.

Intended Audience

This document is intended for all interested stakeholders including:

- Early adopter hospitals and health departments in the process of planning, implementing or upgrading an e-Referrals system;
- Software vendors developing an e-Referrals system product;
- Early adopter general practitioner and specialist desktop software vendors;
- Senior managers and policy makers, clinical experts, Health Information Managers, IT operations and support teams, system integrators;
- Stakeholders associated with the development and use of upcoming e-health initiatives relating to 'continuity of care'; and
- Technical and non-technical readers.

While a considerable portion of this document discusses technical content, efforts have been made to make it accessible to the majority of readers. Where possible, simple non-technical language has been used, jargon explained, and a comprehensive list of definitions, acronyms and abbreviations has been made available (see below).

Document Map

The following diagram represents the relationship between this document and others within the e-Referrals package.

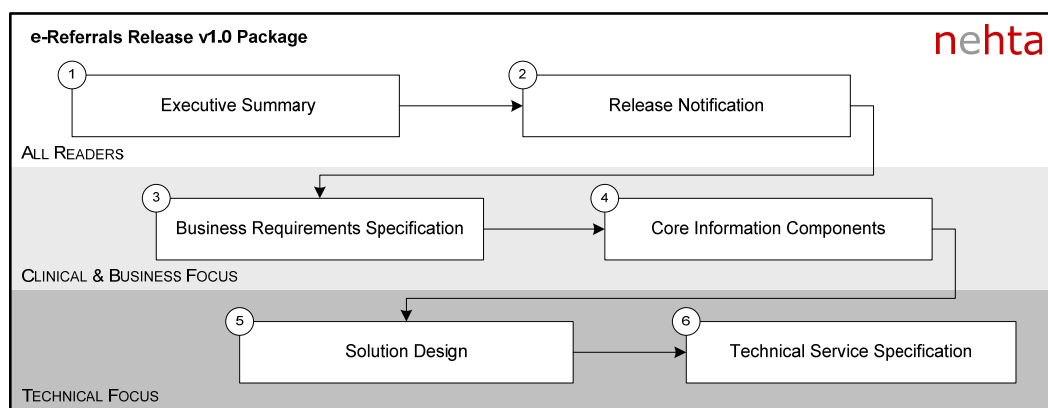


Figure 1 e-Referrals Package Document Map

The Solution Design defines Current, Interim and Future solution states supported by the Business Requirements Specification. The Core Information Components document defines the minimum set of data groups and elements that are recommended for implementation in any system involved in healthcare referral transactions within Australia.

Definitions, Acronyms and Abbreviations

For a list of abbreviations, acronyms and abbreviations, see the [Definitions section](#) on page 34.

References and Related Documents

For a list of all referenced documents, see the [References section](#) on page 36.

1 Introduction

1.1 Overview

NEHTA is leading a national approach to the implementation of an electronic clinical referral to support private, national, state and territory healthcare reforms. These reforms are aimed at improving the safety, effectiveness, timeliness, efficiency and equity of healthcare by facilitating the flow of health information between authorised parties in a secure and private manner. Critical components or tools that will be required to enable an effective e-Referrals system in Australia include:

- Unique electronic identification for each patient, professional healthcare provider and healthcare provider organisation
- Secure, effective, efficient and standardised messaging processes
- Standardised clinical information models and clinical terminology.

It is important to note that this document aims to assist readers in understanding the overall e-Referrals solutions package. The information provided here is background information and is not normative in nature. This document does not aim to specify the exact interaction model nor all the software components required to support the internal processing or generation of an e-Referrals document.

To enable interoperability, the e-Referrals Technical Service Specification and CDA implementation guide contains normative conformance points that must be satisfied by each implementation of the e-Referrals package.

1.2 Referral Definition

Referrals are an essential part of clinical care in the Australian health system, as they allow the informed sharing of resources, including clinical expertise, diagnostic testing, and technical/interpretive skills. Referrals are commonly issued by general practitioners to allow patients a period of specialist consultation, focussing upon a specific health problem.

Currently, there are varying definitions for 'a referral' within Australia, depending upon the organisation or authority sourced, and the specific perspective considered (e.g. administrative, clinical-responsibility, financial, regulatory).

Within the Australian health care environment, there are two commonly-cited definitions of a referral.

The Medicare Benefits Schedule Book (MBS) [MBSB2009] defines a referral as:

"... a request to a specialist or a consultant physician for investigation, opinion, treatment and/or management of a condition or problem of a patient or for the performance of a specific examination(s) or test(s)."

The Schedule also notes:

"The general practitioner is regarded as the primary source of referrals. Cross-referrals between physicians should usually occur in consultation with the patient's general practitioner."

The Australian Standard [AS4700.6–2006] uses the following definition:

"The communication, with the intention of initiating care transfer, from the provider making the referral to the receiver."¹

¹ "Implementation of Health Level Seven (HL7) Version 2.4, Part 6: Referral, Discharge and health record messaging" 2006, p9

The Standard also distinguishes between such transfers as being 'in part'; requests for specialist opinion or other special service, accompanied by a relevant health event summary and record extracts, or being 'in whole'; the transfer of a patient from one general practitioner to another, accompanied by relevant health record data.

NEHTA's specification development effort identifies that in the case of general practitioner-initiated referrals, the concept of a patient's usual general practitioner performing the central role of care coordinator is key. The majority of referrals relate only to an aspect of a patient's care, for a defined time, and for a particular purpose, typically beyond the area of the referrer's expertise.

1.3 Referral Process

The referral process has been defined within the e-Referrals Business Requirements Specification document. Please refer to [ER-BRS2010] for more information.

1.4 Scope

1.4.1 Scope Inclusions

The scope of the e-Referrals package includes electronic referral processes, between general practitioners and specialists. That is, it involves the creation, delivery, receipt and confirmation of patient referral documents in electronic form.

1.4.2 Scope Exclusions

The scope of this package excludes the following:

- The 'decision to refer' process
- The 'booking/scheduling' process at either the general practice or the specialist clinic.

1.5 Goals and Objectives

One of the goals of NEHTA's national referral specification is to drive the adoption of open standards and specifications that collectively:

- Support secure, private, and robust interoperability to enable exchange of more timely, accurate and reliable referral information, thereby improving the delivery of patient care for both consumers and clinicians
- Facilitate improved communication of patient information between general practitioners and specialists to support the continuum of care for patients
- Supply healthcare providers with timely access to patient information in a way that supports the care management process
- Improve clinical and administrative efficiency.

The primary objectives include:

- The adoption of Web service architectures designed to streamline existing business functions involving electronic information exchange using existing identifiers
- The early adoption of clinical content specifications, prior to the full implementation of national infrastructure services, including the ability to:

- Gather and store referral information locally to facilitate future electronic information exchanges based on a defined content template
- Send standard terminology in conjunction with content templates and interchange formats
- Receive, validate and process terminology in conjunction with content templates and interchange formats, automatically integrating this information into the receiving system where appropriate
- A migration to National Infrastructure Services such as the National Authentication Service for Health (NASH), Endpoint Location Service (ELS) and National Health Identifiers (IHI, HPI-I, HPI-O) as part of the infrastructure services approach.

1.6 Dependencies

The table below outlines the dependencies for an interoperable national e-Referrals solution.

Item	Description
1.	<p>The e-Referrals initiative is reliant on the following national e-Health foundation initiatives to provide an agreed, consistent technical solution to enable the exchange of referral information:</p> <ul style="list-style-type: none"> • Healthcare Identifiers Service (HI Service) - for identifiers • NASH - for authentication services <p>Note: Interim solutions may be required until these foundation services are available.</p>
2.	<p>The development and availability of nationally agreed terminology reference sets² for each data element in the referral message specification. In addition:</p> <ul style="list-style-type: none"> • The logical reference model employed and its relationship to the Structured Document Template (SDT) and terminology • The relationship between the referral terminology, the feeder systems, and terminology mappings • Terminology common to multiple packages and how this is structured (e.g. headers and shared data groups) • The migration path to post-coordination, including guidance on the representation of qualifiers, and the use of structure or pre-coordination • Exchange format mapping • Implementation guides for terminology and the SDT.
3.	<p>The definition of Web services and connectivity specifications from the Secure Messaging initiative.</p>
4.	<p>Specific referral projects and initiatives. NEHTA's role is to work with vendors, hospitals and health departments to ensure that jurisdiction solutions are aware of and comply with the national specifications for the exchange of referral information.</p>
5.	<p>The referral solution monitors the national e-Health strategy to ensure that it maintains alignment.</p>

Table 1 Solution Dependencies

² Ref/def might be appreciated by readers.

2 Solution States

2.1 Timeframes

This package makes use of the following terms to indicate the temporal context of specific descriptions or discussions.

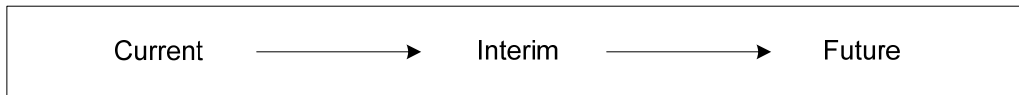


Figure 2 Current, Interim and Future States

'Current' refers to the health sector setting at the time of publication, and indicates the implementation measures that can begin immediately, typically related to infrastructure specifications.

'Interim' refers to upcoming specifications and implementation measures which will be available in the near-future, via the release of subsequent package documents or components.

'Future' refers to the goal state, based upon implementations of e-health specifications and standards.

Opportunity for synergies between e-health solutions, and added value, increases with later states.

2.2 Current

The following section describes the types of referral-related systems implementers can build immediately based on the current specifications of the e-Referrals Release 1.0 package.

2.2.1 Assumptions

Package discussion assumes the availability of the following document, at the date of publication:

- e-Referrals Technical Service Specification [ER-TSS2010].

2.2.2 Constraints

Package discussion is constrained by the following, at the date of publication:

- The Referrals Core Structured Document Template v1.0 [ER-SDT2010] is planned for release.
- SNOMED CT-AU reference sets are released six monthly and development schedule for referral items are not yet finalised..
- The Referrals Core HL7 CDA Implementation Guide v1.0 is planned for release.
- In-development components, comprising:
 - NASH services
 - National identifiers for Providers (HPI-I) , Organisations (HPI-O) and Individuals (IHI)
 - HI Service, facilitating communication and information exchange between providers, and retrieving IHI numbers
 - Endpoint Location Service (ELS) information and/or services.

2.2.3 High Level Solution View (Current)

The following figure depicts the scope of the Current solution state based upon the constraints and assumptions of the initial referrals process.



Figure 3 High Level Solution View (Current Solution State)

The original (initiating) referral message will be sent to the appropriate endpoint (which may be a third party messaging vendor, referrals repository or the referee directly). Upon successful delivery, the referrer will then receive a delivery acknowledgment to indicate that the message has been successfully received by the destination endpoint. No assumption is made as to whether the referral has been read and/or opened by the receiver at this point. The delivery acknowledgement is not to be considered an 'Accept' response.

2.2.4 Implementable Referrals Process (Current)

Within the assumptions and constraints of the Current state, implementers will be able to build solutions using NEHTA specifications and national standards for the following three steps (refer to Section 1.3) within the overarching referrals business process, and contribute to the national e-Referrals solution infrastructure.

2.2.4.1 Determine Recipients

- Locate the healthcare organisation that offers the required service (with suitable availability) using either the local system's address book or a provider directory(s).
- Determine the preferred means of communication from information stored within the address book or provider directory. This may include a reference to the providers ELS if one exists.

2.2.4.2 Assembly and Dispatch

- Auto-populate the Referrals SDT with information from the general practitioner system.
- Include referring provider and individual identifying information within the referral to aid in the matching process at the receiver's end, subject to compliance with relevant privacy legislation.
- Manually add clinical details and review any automatically populated information.
- If the selected recipient has an associated ELS, invoke it to determine the appropriate document format and endpoint address. If the provider does not have an associated ELS, this information will have been provided by the address book and/or provider directory.
- Construct the document in the correct exchange format such as HL7 v2.x. The mapping profile from the Referrals Core Information Components v1.0 to an HL7 v2.x format will need to be published by

the participants within the exchange. Ideally, existing standards should be used where appropriate.³

- Obtain the required Public Key Infrastructure (PKI) certificate to be used to digitally sign the clinical payload. This is a certificate that is bound to the identity of the healthcare organisation which the individual referrer represents. As NASH services will not yet be available, alternate certificates will need to be used such as HeSA (Medicare) certificates for this purpose.
- Digitally sign the referral. The referral being signed must contain the full name and the HPI-I of the individual referrer. The digital signature must only be applied after the individual referrer has viewed the referral and has explicitly approved it for signing. In order to ensure that digital signatures thereby applied reliably identify the individual referrer, the referring organisation must comply with the RACGP Standards for general practices 4th edition as they relate to Information Security (i.e. criterion 4.2.2).
- Prepare the referral (in accordance with [ATS 5822—2010]) for transmission using the Secure Message Delivery (SMD) interfaces. SMD also uses digital signatures; in this case so that the recipient can verify that the document has not been tampered with, and SMD uses encryption so that the confidentiality of the contents is protected while the referral is in transit, before being delivered to the referee.
- Send the referral.

2.2.4.3 Receipt and Assimilation

- Confirm the receipt of referral. This confirmation should indicate that the referral message has successfully persisted at the remote endpoint. This does not necessarily indicate that the referral has successfully been passed/validated and/or uploaded within the endpoint application, however.
- Determine if the subject of care is a new or existing patient. This will be done by performing name matching by the supplied personal and/or organisational demographic information contained within the source document. (As noted previously, national identifiers are not yet available.)
- Incorporate data from the referral into the clinical information system.
- The referral message should be persisted in its entirety by the receiving system. The referee is required to be able to subsequently make the referral available to the relevant authority for audit purposes. As part of this audit process, the authority shall be able to verify the digital signature applied by the referring system and determine the identity of the individual referrer.

2.2.5 Referral Document Delivery Options (Current)

Options include (but are not limited to):

- Secure messaging vendors. This option uses a third party to handle the secure delivery of the referral message to the ultimate recipient.
- Point-to-Point communication using the Referrals Technical Service Specification [ER-TSS2010].

³ Such as the Australian standard AS4700.6 'Implementation of Health Level Seven (HL7) Version 2.4—Referral, discharge and health record messaging' and the corresponding handbook; HB 235-2007, 'Implementers guideline for HL7 referral, discharge and health record messaging', both available via <http://infostore.saiglobal.com/store/> at date of publication.

- Externally-hosted referral repositories. Access to these repositories may be via a Web portal interface with e-mail based notifications to inform the referee that new referrals are ready for processing.
- Combinations of the above listed options. For example, an externally hosted referral repository (or external central gateway) may also use the Referrals Technical Service Specification to implement NEHTA secure messaging.

2.3 Interim

The primary differences between the Current and Interim states are the addition of terminology bindings and an HL7 CDA implementation guide.

2.3.1 Assumptions

The following assumptions apply when considering the Interim state:

- The scope of the Interim state is constrained to that of the package, as specified in Section 1.4.
- NEHTA will have released:
 - Referrals Core Structured Document Template v1.0 [ER-SDT2010]
 - SNOMED CT-AU reference sets to support data groups present in the Referral SDT
 - Referrals Core HL7 CDA Implementation Guide v1.0
 - e-Referrals: Technical Service Specification v1.0.

2.3.2 Constraints

The following constraints apply when considering the Interim state:

- NASH services are not yet available.

2.3.3 High Level Solution View (Interim)

The following figure depicts the solution based upon the envisaged Interim state of the e-health landscape. Note that conceptually, the Interim solution state view is the same as the current state with the exception of the assumptions and constraints listed above.



Figure 4 High Level Solution View (Interim Solution State)

The structure of the information being sent within the referral document conforms to the Referrals Core Structured Document Template v1.0 [ER-SDT2010] and is transformed into an HL7 CDA document using the Referrals Core HL7 CDA Implementation Guide v1.0, planned for release in 2010.

The referrals document will contain standard terminology (SNOMED CT-AU) within the structured document as defined by the Referrals Core Terminology Bindings v1.0.

As national identifiers are available, the referral document will be populated with information identifying the individual and provider (current identifier apply), to aid in the matching process performed by the receiver e.g. provider numbers.

As NASH services are not yet available, alternate digital PKI certificates (such as HeSA Medicare certificates) will need to be used for digital signing and secure messaging purposes.

If ELS information is unavailable during the 'determine recipients' activity, then the preferred method of communication and means to do so will need to be derived from alternate sources, which may include the local address book or provider directory.

2.4 Future

The following assumptions are based upon a theoretical Future state within the e-health landscape, and specifically the e-Referrals domain. Although NEHTA has performed significant research in this area, assumptions made will need to be validated by rigorous external consultation and are subject to change.

2.4.1 Assumptions

The following assumptions apply when considering the Future state:

- The scope of the Future state is constrained to the scope of the package, as specified in Section 1.4.
- NEHTA will have released:
 - Referrals Core Structured Document Template v1.0 [ER-SDT2010]
 - SNOMED CT-AU reference sets to support data groups present in the Referral SDT
 - Referrals Core HL7 CDA Implementation Guide v1.0
 - e-Referrals Technical Service Specification [ER-TSS2010]
 - Structured Document Templates for specific specialities and points of care and will build upon the Referrals Core Structured Document Template v1.0
 - Relevant information regarding a template service, allowing for the generic population and transformation of clinical information for a wide range of template structures and document formats
 - An updated Technical Service Specification for the package covering additional message types to support the extended referrals workflow process. This specification will extend the Referrals Technical Service Specification [ER-TSS2010]
 - Updated HL7 CDA implementation guide to support the additional referrals templates, building upon the Referrals Core HL7 CDA Implementation Guide v1.0
- Additional message types (such as Accept, Decline and Cancel) supporting the overarching referrals workflow will be available and supported by the referrals service interface specification
- NASH services will be available
- National identifiers for Providers (HPI-I) , Organisations (HPI-O) and Individuals (IHI) will be available
- HI services will be available
- ELS information and/or services will be available.

2.4.2 Referrals Process (Future)

The following figure depicts the scope of the Future state of the referrals process, applying e-health enhancements to the end-to-end process.

These enhancements include:

- Notifications
- Updates and reports flowing back and forth between the referrer and the referee.

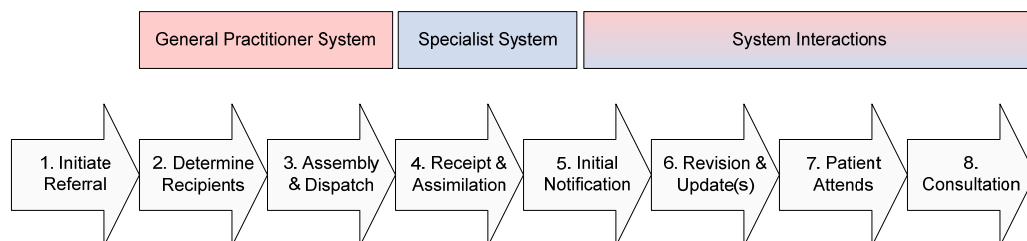


Figure 5 Referrals Process (Future Solution State)

2.4.3 High Level Solution View (Future)

The following figure depicts the solution based upon the envisaged Future state of the e-health landscape. (For the sake of clarity, delivery acknowledgements have not been shown.)

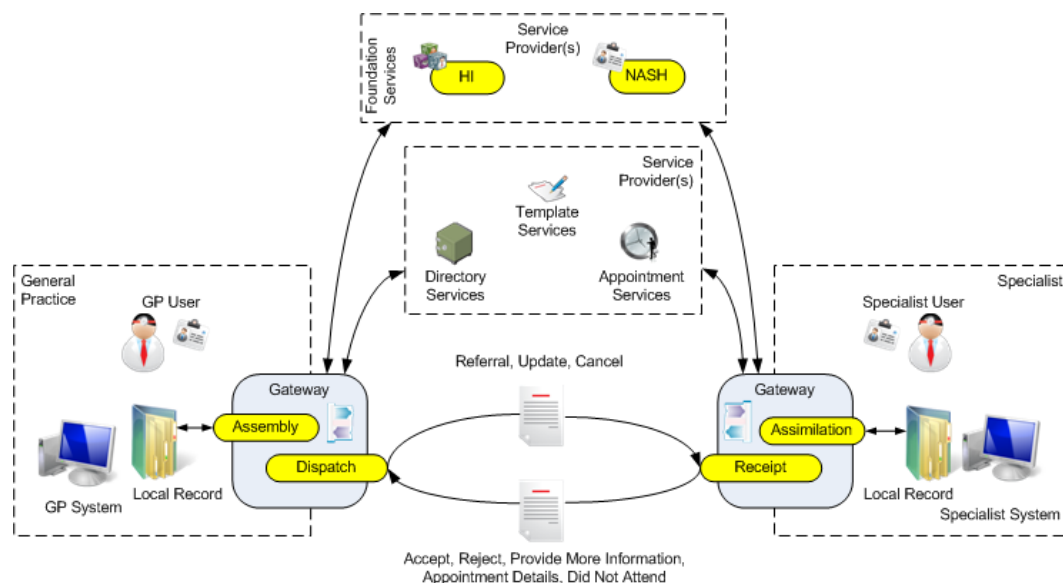


Figure 6 High Level Solution View (Future Solution State)

2.4.3.1 Electronic Workflow Support

The referrer is able to generate the initial referral, updates and cancellation messages. The referee is able to accept, decline or ask for additional information from the referrer. In addition to these message types, the referee is able to routinely provide appointment update details on an ad-hoc basis and is able to provide a 'Did Not Attend' notification if the patient does not present to the referee by the scheduled appointment date.

2.4.3.2 Directory Services

Directory services will be available to the referrer and will provide 'yellow pages'-style search facilities. These may use federated searching capabilities to allow a search inquiry to include multiple external directories. The search

results will contain national identifiers for provider individuals (HPI-I) and provider organisations (HPI-O) and may also include endpoint location information (ELS) for secure messaging purposes. Digital certificates may also be obtained from these services.

2.4.3.3 Appointment Services

Appointment, scheduling and booking services may provide consolidated centralised booking facilities to improve the administrative appointment waiting list process between providers who use the service. The service would allow for direct application integration (ideally using published standards and/or specifications) and/or have a centralised portal-based approach for accessing the information from a Web browser. Using the latter approach would also allow the patient access to his or her own appointment information, and may include booking reminders via SMS and/or e-mail.

2.4.3.4 Template Services

Template services may be used so that information from the referrer’s electronic medical record (EMR) can automatically populate as much structured data as possible into the most appropriate template available for the selected service provider. These services may also be used to transform the structured data within the referral (once completed and verified by the referring provider) into a format which can be consumed by the referee’s information system. These transformations could occur locally or be performed by the service itself. In addition to these facilities, it is envisaged that such a service would allow for updates to existing templates and the creation of new templates to be made with little or no need to reconfigure the sending or receiving applications (provided that both parties are subscribed to the service).

2.4.3.5 National Infrastructure Services

Both the referrer and referee will make use of national infrastructure services such as the NASH and HI Service. However, it should be noted that such interactions may be done indirectly by using other services such as external provider directories (which use the HI Service, in turn).

2.4.3.6 Referral Documents

The following figure is an indicative view of a sample referral, as used within the Future state. The left side of the diagram depicts the required national information assets, specifications and standards. The right side shows the e-Referrals document.

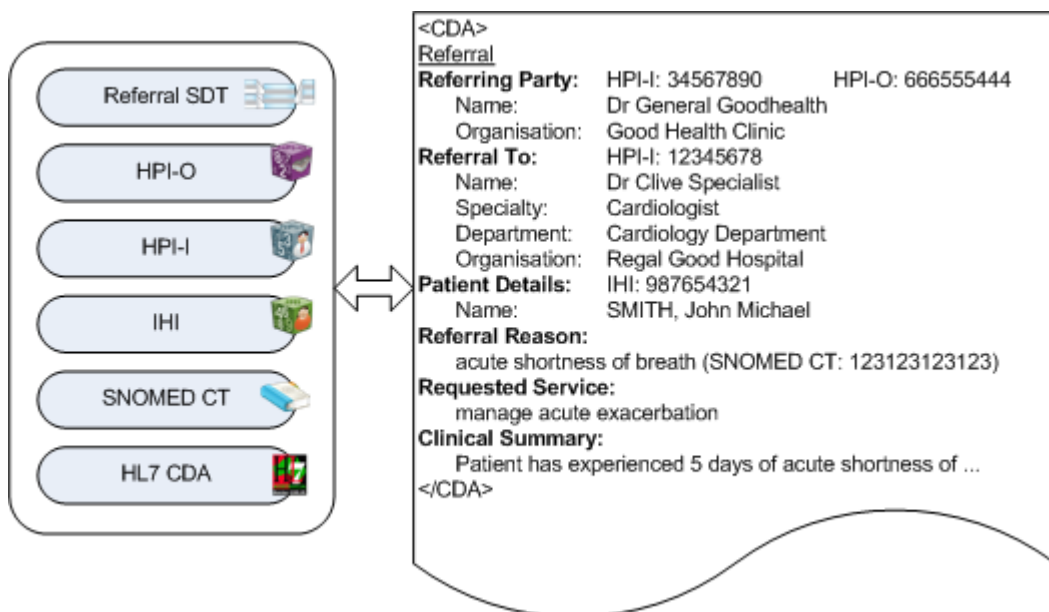


Figure 7 Referral Document (Future Solution State)

The structure of the information being sent within the referral document conforms to the NEHTA e-Referrals structured document template (SDT) and is transformed into an HL7 CDA document using the Referrals Core HL7 CDA Implementation Guide v1.0, planned for release in 2010.

The referrals document will contain national identifiers for the referrer and referee (HPI-I), the referrer and referee organisation (HPI-O) and the patient (IHI). Standard terminology (SNOMED CT-AU) will also be used within the structured document.

National identifiers and PKI certificates (used for unique identification and digital security) are used during the assembly and dispatch processes (and also during the receipt and assimilation processes), sourced by using national infrastructure services.

3 Business View

3.1 Roles and Services

This section lists the logical roles and services involved in the generation, distribution and receipt of the e-Referrals. Further detail on the listed roles and services can be obtained from the e-Referrals Business Requirements Specification [ER-BRS2010].

3.1.1 Roles

- Patient
- Referee
- Referrer

3.1.2 Services

- Clinical Information Systems
- (Electronic) Distribution Services
- Authentication Service
- Provider Directory Services
- Healthcare Identifiers Service

3.2 Safety and Quality in Healthcare

3.2.1 Implications for the Solution

The national e-Referrals package upholds the requirements of the Charter, as detailed in the following table.

Item	General Safety & Quality Requirements	Implications for Solution
1.	The information in the referral concerns the right patient.	Individual health identifiers (IHI) will enhance existing best practice for correct patient identification (name, date of birth, demographic matching) at the point of referral creation and receipt.
2.	The referral is delivered to the right recipients.	Health identifiers will assist in ensuring an e-Referral is delivered to the correct recipients, and that the patient/carer is subsequently given a copy. Other data will be used (e.g. date of birth), consistent with existing best practice.
3.	Delivery by the right method in the right format.	Directly into an interoperable provider desktop via a secure and robust national connectivity service, in a format supporting reuse of structured data.
4.	The referral is completed at the time of the consultation, facilitating timely care and	Ideally, the referral is completed and transmitted

Item	General Safety & Quality Requirements	Implications for Solution
	cross service continuity of care.	<p>immediately from the referring healthcare professional to the referred healthcare organisation, and a copy is given to the patient.</p> <p>The referral contains the patient's own information and the patient can view the information being shared with the referred healthcare organisation which can include nurses and administration staff.</p>
5.	The referral has the right information included.	<p>Clinical content is of high quality, being accurate, complete and succinct.</p> <p>The content is readable, standard terminology and reference sets are used where possible. NEHTA endorses the use of SNOMED CT and AMT.</p>
6.	The referral has its information presented in the right way.	<p>Standardised presentation, allowing interoperability.</p> <p>Critical elements are appropriately highlighted and sequenced.</p> <p>The presentation of information is accessible, and avoids reader overload.</p> <p>Where possible, abnormal flags from diagnostic investigations (e.g. pathology result) are preserved.</p>

Table 2 Policy Requirements and Implications

3.2.2 Clinical Safety Management in e-Health

A clinical safety assessment has been completed for the e-Referrals package.

The outcome of the assessment identified three (3) main areas of potential Clinical Safety risk:

- Delays in care, due to the non-delivery or misdelivery of the e-Referrals message
- Inadequate prioritisation of care due to the lack of a prioritisation status within the e-Referrals design.
- Sensitive information and access restrictions that could potentially prevent legitimate access to e-Referrals.

Each of these risks have been mitigated by a combination of internal, external, human factor and assumed clinical controls to a level that is considered as low as reasonably practicable.

As such, none of the aforementioned clinical safety risks would prevent the release of the e-Referrals 1.0 specifications.

4 Information View

4.1 Introduction

An Information Architecture describes how to exchange information successfully and what information should be exchanged.

In their discussion on the value of information exchange and interoperability in the health sector, Walker et al.⁴ define four levels of healthcare information sharing, as below.

Information-sharing	Definition
Level 1	Non-electronic data exchange using postal mail, telephone, etc.
Level 2	Machine-transportable data limited to non-electronic manipulation. Examples include fax, scanned documents, portable data format (PDF).
Level 3	Machine-organised data that requires manual translation between incompatible vocabularies, proprietary data formats, or unstructured content.
Level 4	Machine-interpretable data transmission utilising structured messages from standardised and coded vocabularies.

Table 3 Levels of healthcare information sharing

In an e-Referrals environment, the goal is to exchange information such that the systems at each end of the exchange can consistently and reliably interpret and represent the intended meaning. This is known as semantic interoperability. Full semantic interoperability is not a reality yet, however every step that is taken to move towards this goal is an important one for e-health.

The most common first step involves a Level 2 exchange of documents that are only human readable (e.g. text document, PDF file). This allows for secure transfer of information from human-to-human, but not from machine-to-machine.

The next step is to use a messaging format that allows for structured representation of the referral data elements, such that a computer system can take the data elements and import them directly into its own database, preserving the context that the data is bound to. This Level 3 exchange allows functional interoperability across machine-to-machine boundaries, where the structures of the data are recognised; however, the underlying meaning (i.e. semantics) of the data may not be interpretable.

In the final step, a Level 4 exchange allows semantic access to the clinical meaning of the information exchange. Although human-to-human semantic exchange is well-established, creating consistent and unambiguous representations between two or more machines is much more challenging. Already, there exist a number of standards and specifications designed to enable this type of interoperability, but they are not yet widely used.

4.2 Information Flows

The following figure gives an overview of the information flows that may occur when a referral is electronically sent to a referee.

⁴ <http://content.healthaffairs.org/cgi/content/full/hlthaff.w5.10/DC1> (accessed 17/12/09)

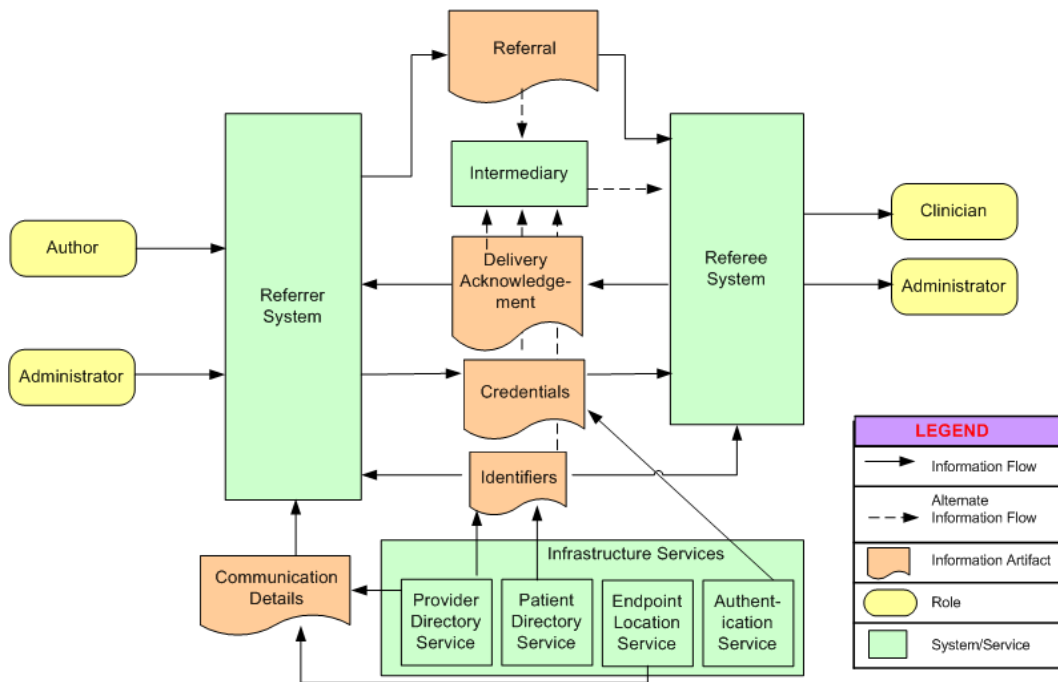


Figure 8 Referral Information Flows

It depicts the main information artefacts, systems/services and participant roles involved in the electronic distribution of referrals.

The information artefacts involved include:

- The Referral
- Delivery Acknowledgement
- Credentials
- Identifiers
- Communication Details

The systems/services involved include:

- Referrer System
- Intermediary
- Referee System
- Infrastructure Services, including:
 - Provider Directory Service
 - Healthcare Identifiers Service
 - Endpoint Location Service
 - Authentication Service, including PKI infrastructure e.g. NASH

The participant roles involved include:

- Author (Referrer)
- Administrator (Referrer)
- Clinician (Referee)
- Administrator (Referee)

Note: Although the subject of care is a central participant in the referral process (e.g. providing consent for the referral to be distributed), enabling them to directly interface with the referral system is currently out of scope for this version of the e-Referrals package.

4.3 Information Components

4.3.1 Overview

The key information components used in an e-Referrals solution are shown in the high-level class diagram, below.

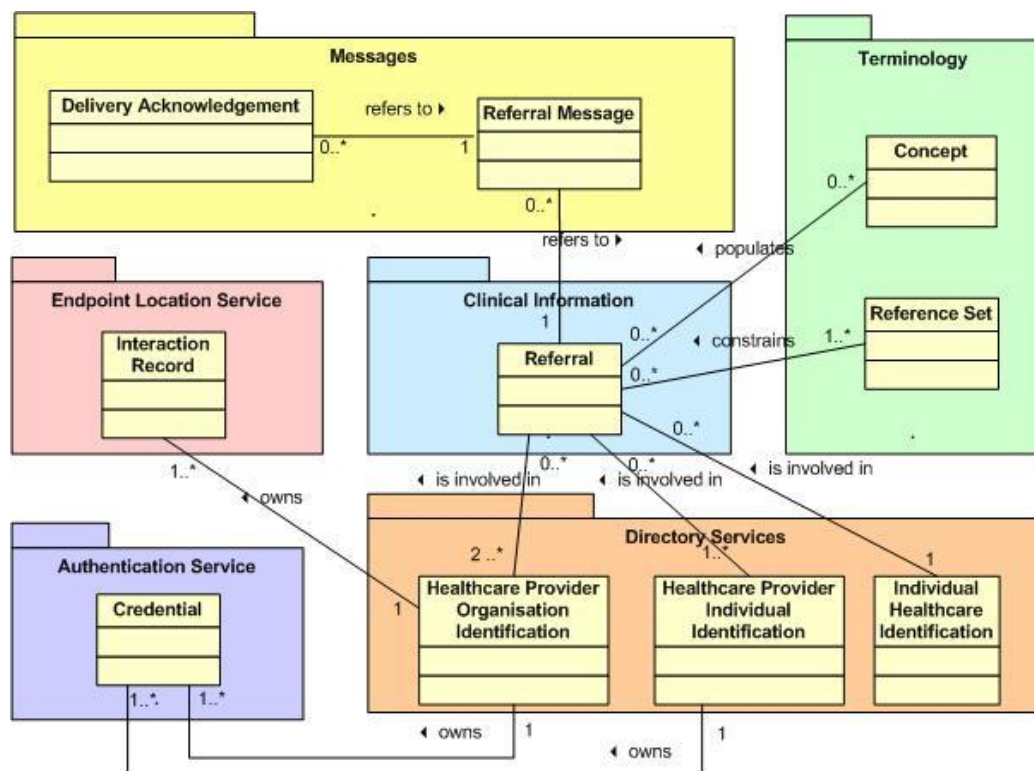


Figure 9 Information Component Overview

This diagram groups the key information components into logical categories (represented as separate UML packages), and shows the relationships between these components. The key information components include:

- The Referral (Clinical Information)
- Concepts and Reference Sets (Terminology)
- The Referral and Delivery Acknowledgement Messages
- Healthcare Provider Identifier Individual (HPI-I), Healthcare Provider Identifier Organisation (HPI-O) and Individual Healthcare Identification (IHI) (HI Services)
- Interaction Record (Endpoint Location Service)
- Credentials (Authentication Service including PKI e.g. NASH).

These information components will be discussed in more detail in the following subsections.

4.3.2 Referral

A referral is generated to share information between healthcare providers to optimise collaborative patient care, and satisfy business requirements relating to reimbursements.

In order to move closer to Level 4 semantic information sharing, e-Referrals must use a common clinical terminology to describe information, such as diagnoses, procedures, and medications.

4.3.3 Terminology

4.3.3.1 Background

One prerequisite to the safe exchange of clinical information between healthcare providers is the establishment of a common, coded clinical language (clinical terminology). The concepts and descriptions (or terms) used in clinical communications that describe diagnoses, procedures, therapies, medications, and other clinical meanings must be accurately and consistently interpreted by all participating health IT systems and the clinicians that interact with them.

4.3.3.2 SNOMED CT

SNOMED CT is a broad, clinical reference terminology suitable for documentation and reporting.

SNOMED CT has been recommended by NEHTA and endorsed by state, territory and Commonwealth governments of Australia as the basis for a national clinical terminology standard to be used across the nation's strategic health information solutions. SNOMED CT is now available at no charge for use in Australia, under NEHTA's licensing arrangements with the International Health Terminology Standards Development Organisation (IHTSDO). Visit <http://nehta.org.au/aht> to obtain access.

Additionally, NEHTA aims to refine, improve, extend and focus SNOMED CT to meet the localised needs of Australian healthcare. The Australian-specific extensions to SNOMED CT are anticipated to cover an increasing number of terminology domains over time. However, initial priorities have been defined to cover areas such as medications, adverse reactions, pathology, problems/diagnoses and clinical interventions. Ongoing priorities will be defined through stakeholder consultation and NEHTA's assessment of benefits and capacity to support ongoing releases. The Australian release of SNOMED CT including Australian content will be known as 'SNOMED Clinical Terms – Australian Extension', abbreviated to SNOMED CT-AU.

With this in mind, SNOMED CT-AU will be used, wherever suitable, to define coded terms used within a referral sent by a referrer to a referee. The adoption of SNOMED CT-AU as the standard ensures a consistent language is available to record, store, retrieve and aggregate clinical data.

4.3.3.3 Terminology Binding

The forthcoming Referrals Core Structured Document Template v1.0 [ER-SDT2010] will describe and constrain the contents of a referral sent by a referrer to a referee. This specification also identifies those data elements which either can, or should, use terminology values to populate them. Data elements of this kind (or their codeable components) are identified by the data type 'CodeableText' or 'CodedText'.

Each of these 'codeable' data elements has a value domain, which will be bound (or restricted) to specific terminology value sets, called 'reference sets'. These define the possible set of concepts that may be used to populate the associated data element.

The following figure shows the common structure of all Event Summaries (e.g. Referral), and the relationship of its component with those of terminology. In particular, it shows the relationship between the data elements and the concepts which populate them, and the relationship between the value domains and the reference sets which constrain their valid values.

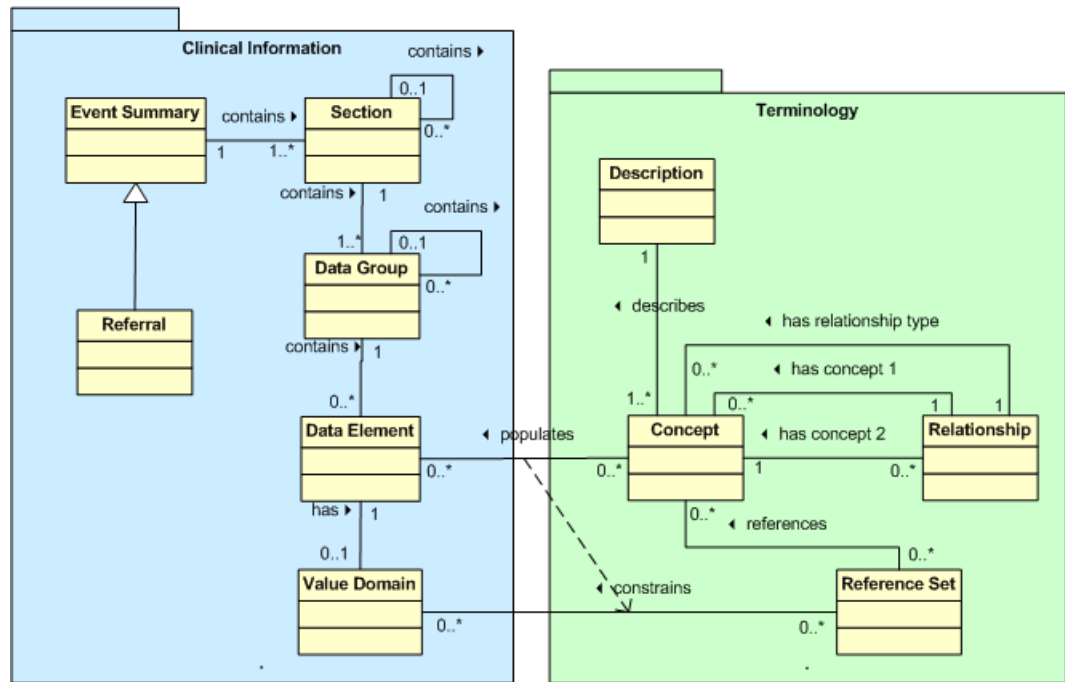


Figure 10 Referral Terminology Binding

4.3.4 Messages

The following figure shows the messages which are relevant to the distribution of referrals.

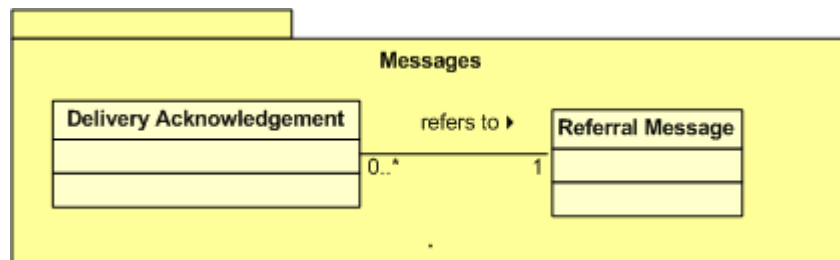


Figure 11 Referral Messages

The referral message is used by the referrer to create the initial referral request.

The delivery acknowledgement message is used to flag that the referee’s system has received and persisted the referral message. No assumption has been made as to whether the referral document (within the referral message) has been read and/or opened. The delivery acknowledgement contains no clinical content and does not indicate an 'accept' response.

4.3.5 Identification

4.3.5.1 Overview

Healthcare relies on the ability to uniquely and accurately identify individuals and organisations, both to relate current patient status to previous care, and to support the communication between healthcare providers. This is true whether or not a manual or computer-based information environment exists. Within the healthcare service delivery community, the process of positively identifying healthcare consumers involves matching data supplied by those individuals against data held by healthcare providers.

To this end, three types of identification are required, for:

- Individual healthcare consumers
- Individual healthcare providers
- Healthcare provider organisations.

To support this identification process, NEHTA is participating with Medicare Australia to design and build Australia's first national healthcare identification service. The resulting Healthcare Identifiers Service (HI Service) will provide the requisite identification service for the healthcare professionals and organisations directly involved in the provisioning of healthcare services. For more information on this national HI service, please refer to Section **Error! Reference source not found.** 'National Infrastructure and Enablers'.

Initially, however, it is assumed that jurisdictional and local system identifiers (including Medical Record Numbers and Unique Patient Identifiers) and the national Healthcare Identifiers (HIs) will coexist. In the longer term, IHIs and HPIs are expected to replace these local identifiers, providing a more interoperable approach to identification.

4.3.5.2 Identifiers in Referral Documents

A referral document includes the following entities which need to be identified accurately:

- Patient
- Referring practitioner
- Referring organisation
- Referred practitioner
- Referred organisation
- General practitioner usually attending the subject of care.

The above entities can be categorised into three types: medical practitioners, healthcare clinics and the patient. Currently, those entities are identified through a common combination of data e.g. name and address. When the national Health Identifier becomes available, it provides the capability to separately identify entities in each of the above mentioned categories:

- Individual Healthcare Identifier (IHI) - healthcare individual
- Healthcare Provider Identifier (HPI-O) - healthcare clinic
- Healthcare Provider Identifier (HPI-I) - healthcare provider

4.3.6 Endpoint Location Service

An Endpoint Location Service (ELS) is a simple directory of technical services for message exchange. An ELS allows a system in the e-health community to locate electronic services offered by a healthcare provider organisation for particular service categories. These categories broadly correspond to business services and may include the clinical message type and/or terminology employed.

An ELS contains one or more interaction records, each of which is associated with exactly one Healthcare Provider Organisation. Each interaction record contains an associated service and reference to one or more required certificates.

Data in an ELS is structured as follows:

- Healthcare Organisation
- Service Category
- Service Interface

- Service Endpoint
- Provider Identifier
- Set of Certificates to be used for service invocation.

For more information about interaction records and the ELS please refer to the Technical Report Endpoint Location Service [TR 5823—2010].

4.4 Message Formats

NEHTA describes the referral content structure independently of any individual exchange format, thereby providing flexibility to map the information model to various message and document formats.

This degree of decoupling allows implementers the flexibility to choose from a library of common exchange format mapping specifications to suit their requirements, while still conforming to the NEHTA content structure.

In the short term, recipient general practitioner/specialist desktop applications will require the ability to extract key structured data elements (such as healthcare individual identifiers or patient demographics) in order to associate the referral with a particular patient's Electronic Medical Record (EMR) in the general practitioner/specialist desktop database.

In the future, practitioners may choose to select individual elements or sections of a referral (e.g. Medications) and have these populate particular parts of their local patient record.

Suitable referral message formats should:

- Incorporate the data elements described in the structured document template [ER-SDT2010] without loss of data
- Be recognised as an e-health messaging standard suitable for use within the referral context
- Offer both structured and unstructured information representation
- Be relatively easy to integrate into software packages.

4.4.1 Clinical Document Architecture (CDA)

HL7 CDA is NEHTA's preferred exchange format for referral documents. It provides structured representation of information using XML and can be rendered in HTML viewers (such as Web browsers) when used with an appropriate style sheet.

4.4.2 HL7 v2.x

The current interim Australian standard (published by Standards Australia) for exchanging referral, discharge and health record messaging (AS4700.6:2007) is HL7 v2.5.

Australia already has an existing base of healthcare organisations that use the HL7 messaging protocol to exchange information between different computer application systems.

5 Technical View

This section describes the technologies to be used when developing nationally-interoperable referral software components, and their key technical characteristics, based on the Business Requirements Specification [ER-BRS2010].

5.1 Authentication and Security

5.1.1 Security Framework

There are four key elements involved in establishing a security framework.

5.1.1.1 Authentication

Establishing or confirming that someone (or something) is authentic, that is, the claims made by or about the thing are true. This might involve confirming the identity of a person who is attempting to access a computer application, or assuring that the person or entity sending the referral was as represented.

In the case of a referral, there is usually a need for strong authentication. General practitioners and specialists often make clinical decisions based on the contents of such documents, and will therefore require assurance that a referral originated from an appropriate source.

5.1.1.2 Authorisation

Authorisation is concerned with the process of restricting access to specific resources, and making them selectively available to parties permitted to use them.

5.1.1.3 Data Security and Encryption

Ensuring that information is accessible only to those authorised to have access. In a referral context, this is mainly concerned with making sure that only authorised persons can view the content of the referral.

This can be achieved by encrypting the content of the referral as it is transported, such that third parties who may intercept the message cannot read it.

Once the referral message is received and decrypted at the recipient's practice, it is expected that general practitioner/specialist desktop applications will implement access controls that restrict the viewing of the referral to the authorised personnel only (e.g. clinicians and authorised administrators).

5.1.1.4 Non-repudiation

Ensuring that a party in a transaction cannot refute the validity of their signature on a document or the sending of a message. Although this concept can be applied to any communication, the most common application is in the verification and trust of handwritten signatures.

The most common method of asserting the digital origin of data is through digital certificates. Data signed by such a certificate can - with reasonable certainty - be trusted to have come from a party who possesses the private key corresponding to the signing certificate.

5.1.2 Security Requirements

The security of information is a key requirement of referral activity, therefore all electronic communication should be encrypted. Virtual Private Networks (VPN) and Transport Layer Security (TLS) go some way to achieving this,

however the most widely used and recognised approach involves the use of Public Key Infrastructure (PKI), which also allows for signing and can ensure that only the intended recipient can view the contents of a referral.

General practitioner/specialist desktop applications, like most information systems, generally authenticate the identity of the user by prompting for a user name and password. This authentication practice is well understood and accepted by most computer users.

Once authenticated, the application imposes access controls limiting the functions the user may perform based on that user's role (commonly referred to as Role Based Access Control). An example would be a general practitioner desktop application which limits the creation and viewing of referral content to individuals authorised to access a patient's medical record.

5.1.2.1 Intermediaries

One of the requirements for referrals is that the message contents are signed and encrypted by the sender in a way that can only be decrypted by the intended, ultimate recipient. If third party messaging providers are involved in the e-Referrals transaction model, referral documents can be routed without risk to the confidentiality of the referral content.

5.1.3 Secure Transmission

Transmitting data in any standardised format makes it theoretically easier for unintended recipients to access sensitive information. As referrals contain such information, message encryption is essential in order to assure confidentiality.

To date, the most common forms of internet encryption have used a transport level encryption scheme such as TLS, which encrypts and decrypts transmissions transparently to the application sending or receiving the message. With an adequate key length, TLS protects messages from interception during transport to and from the Web service. However, it does not provide complete end-to-end protection of a referral when intermediaries are involved, and does not provide the level of authentication required to positively identify message senders. It is also an incomplete solution for Web services as they are designed to operate independently of the transport layer.

By contrast, a higher level of message security for Web services is provided by support for the WS-Security standard, described in the Australia Technical Specification: E-Health Web Services Profiles [ATS 5820—2010].

Within this standard, there are a number of methods to authenticate the identity of message senders. The most commonly accepted practice for securely exchanging information is based on Public Key Infrastructure (PKI) and involves signing the Simple Object Access Protocol (SOAP) payload using the sender's private key and then encrypting it using the recipient's public key.

Interoperable PKI implementations must ensure communicating parties:

- Are issued with public and private keys originating from a mutually recognised chain of trust
- Can obtain the recipient's public key via a robust process that ensures the identity of the recipient and the authenticity of their digital certificate.

5.1.4 Certificates

Most primary healthcare organisations in Australia have been issued with a Medicare Australia location certificate, and the widespread adoption of these certificates makes it an attractive option for discharge summary solutions.

However, Medicare Australia location certificates are not generally usable for Web services security. As a result, a new Web service certificate profile has been specified and an Operational CA (OCA) is being built for the NEHTA UHI program by Medicare Australia. This will provide suitable certificates for securing Web services. These new Web service certificates also have the organisations HPI-O included within them.

5.1.4.1 National Authentication Service (NASH)

The National Authentication Service (NASH) will ultimately provide the PKI infrastructure necessary to support the HI. It establishes a framework for provisioning of digital certificates, a new Certificate Authority (CA) within the Medicare Australia chain of trust.

Certificates will be issued with the registration of every HPI-O with the Health Identifier (HI) Service. This certificate will be used for the purposes of authentication and securing transactions.

5.2 Web Services Profiles

Web service technologies are industry standards that provide secure, reliable message delivery. NEHTA recommends Web services as the mechanism for communication in Australia's E-Health environment.

Web service standards by themselves are insufficient to ensure that different systems can be integrated to exchange information. The reason for this is that these standards are very flexible, allowing them to be implemented in potentially-incompatible ways.

Nevertheless, with consensus and preparation, Web service profiles can be developed to provide clear definitions to enable interoperable solutions.

Consequently, Standards Australia Committee IT-014, Health Informatics has developed the Australia Technical Specification: E-Health Web Services Profiles [ATS 5820—2010]. This specification defines a common set of mechanisms to enable interoperability in the Australia E-Health environment.

The specification defines the following:

- Web Services Specification
- Transport
- Protocol
- Metadata
- Security

Please refer to E-Health Web Services Profiles [ATS 5820—2010] for a comprehensive list of conformance points in relation to Web services.

Please refer to e-Referrals Technical Service Specification [ER-TSS2010] for the Web services required to support the transfer of discharge summaries.

5.2.1 Web Services Specification

The Web Service Specification describes the service contract such as behaviour, data structures and messaging policies. To be compliant with the Australia Technical Specification, Web services must be specified in Web Services Description Language (WSDL) version 1.1.

The Web Services Description Language (WSDL) is a machine-readable form for describing the function of a Web service and the way it is invoked. The description can be used as part of the formal documentation of the service, and it can also be used as input for development tools and programs.

5.2.2 Transport

The transport section of Web services standards defines the communication protocols used to exchange data between Web services end points. To be compliant with The Australian Technical Standard: E-Health Web Services Profiles, Hypertext Transfer Protocol (HTTP) version 1.1 needs to be adopted.

HTTP v1.1 was specified in the technical specification for its support of Web services that uses an interactive paradigm. It is important to note that HTTP1.1 supports non-interactive style Web services as well. While it is acknowledged that the majority of messaging currently conducted in health is non-interactive, it is expected that interactive applications/services will become more prevalent in the future.

5.2.3 Protocol

SOAP is a protocol for exchanging messages with a Web service using XML. This protocol provides a framework to represent service functions, the high-level structure of input data, and the result content of a function. The specific descriptions of a particular service function and associated content are represented separately. SOAP is the fundamental Web service.

The E-Health Web Services Technical Specification requires all Web service specifications to use SOAP 1.2 as the Web services protocol. SOAP 1.2 is a W3C recommendation. Although widely used, SOAP version 1.1 is only a de facto standard and is not a W3C recommendation.

5.2.4 Metadata

WS-Addressing 1.0 is specified by the E-Health Web Services Profile Technical Specification to carry the addressing data in a SOAP message. The specification also requires the use of WS-Addressing Action, WS-Addressing MessageID and WS-Addressing in SOAP requests/responses/faults.

WS-Addressing defines the mechanism for identifying messages and endpoints. The information is used to process messages. WS-Addressing is a W3C recommendation and is a common mechanism for addressing in Web services.

5.2.5 Security

The Australia Technical Specification: E-Health Web Services Profiles provides two profiles for securing Web services: the TLS security profile and the WS-Security profile.

Transport Layer Security (TLS) is a protocol for establishing a secured channel for communications. It is used to encrypt the data for confidentiality. It is also used to authenticate one or both parties.

TLS is a widely accepted and implemented protocol but TLS on its own does not provide end to end security. End to end security is provided by encapsulating sensitive information within a Secured Payload that can exist outside of the secured communication channel of TLS.

The Web Services Security specification (WS-Security) specifies features which support the secure exchange of SOAP message. It provides mechanisms for preserving the confidentiality and integrity of messages through the use of encryption and digital signatures.

Unlike TLS which secures the connection, WS-Security has the added capability to secure portions of a message through the application of XML encryption.

WS-Security provides flexible support for PKI and other forms of encryption by specifying general methods allowing security tokens of different types to

be attached to messages. Various tokens can be attached to the message substantiating the senders claim to a particular identity which can then be examined by the Web service to confirm the source of the communication.

5.3 Payload Encryption and Signing

Confidentiality is a key requirement of the referral activity, and as such, all electronic communication should be encrypted. Virtual Private Networks (VPN) and Transport Layer Security (TLS) go some way to achieving this (secure connection). However they do not provide a mechanism to ensure the security of the payload.

The most widely used and recognised approach to securing payload involves use of Public Key Infrastructure (PKI). This allows for signing and encryption. Consequently only the intended recipient can view the discharge summary and have confidence in message integrity.

The National Authentication Service for Health (NASH) will ultimately provide the PKI infrastructure for the healthcare sector. It establishes a framework for provisioning of highly trusted, digital credentials (e.g. certificates).

Digital credentials may be requested with the registration of every HPI-O or HPI-I. These credentials may be used for the purposes of authentication and securing e-health transactions.

For more information about NASH, please refer to the NEHTA Blueprint [NBP2010].

Standards Australia Committee IT-014, Health Informatics has developed the Australia Technical Specification: E-Health XML Secured Payload Profiles [ATS 5821—2010]. This specification defines mechanisms for representing signed and encrypted XML data. The specification defines the following:

- Signed Container Profile
- Encrypted Container Profile
- XML Signature Profile
- XML Encryption Profile

Please refer Australia Technical Specification: E-Health XML Secured Payload Profiles [ATS 5821—2010] for a comprehensive list of conformance points in relation to payload encryption and signing.

5.3.1 Signed Container Profile

The signed container profile represents an XML payload that is digitally signed using the XML signature profile. It provides the additional mechanism to include an XML element to represent the payload and one or more signatures on that payload. This enables the recipient of an E-Health message to confirm the integrity of the message.

5.3.2 Encrypted Container Profile

The Encrypted Container Profile represents XML payload that is cryptographically encrypted using the XML Encryption Profile. It provides the additional mechanism to include an XML element to represent the encrypted XML as well as one or more encrypted keys. This enables the use of one or more private keys to decrypt the payload and ensuring the confidentiality of the message.

5.3.3 XML Signature Profile

The XML signature profile detailed in the E-Health XML Secured Payload Profiles specification defines signature (ds:signature) and not the

representation of the signed payload. XML signatures utilises asymmetric encryption method where a public key and a private key is involved.

A signature is used to validate the sender of the message. A signature is the digest value resulted from the application of the receiver's public key to a transformed XML fragment. Upon receiving the message, the recipient will apply its private key to the transformed XML fragment. Identity of the sender is verified if the checksums are the same.

5.3.4 XML Encryption Profile

The XML encryption profile detailed in the E-Health XML Secured Payload Profiles Technical Specification defines the encrypted data (xenc:EncryptedData) and the encrypted key (xenc:EncryptedKey).

Payload encryption is required to adopt the symmetric encryption method to achieve higher levels of efficiency. A session key is used to encrypt the payload. The session key is transferred to the receiver utilising asymmetric encryption i.e. receiver's public key is used to encrypt the symmetric key and the receiver will decrypt the session key using its private key.

5.4 Referrals High Level Component Model

The following figure illustrates the primary solution components for a referral being sent from a general practitioner to a specialist.

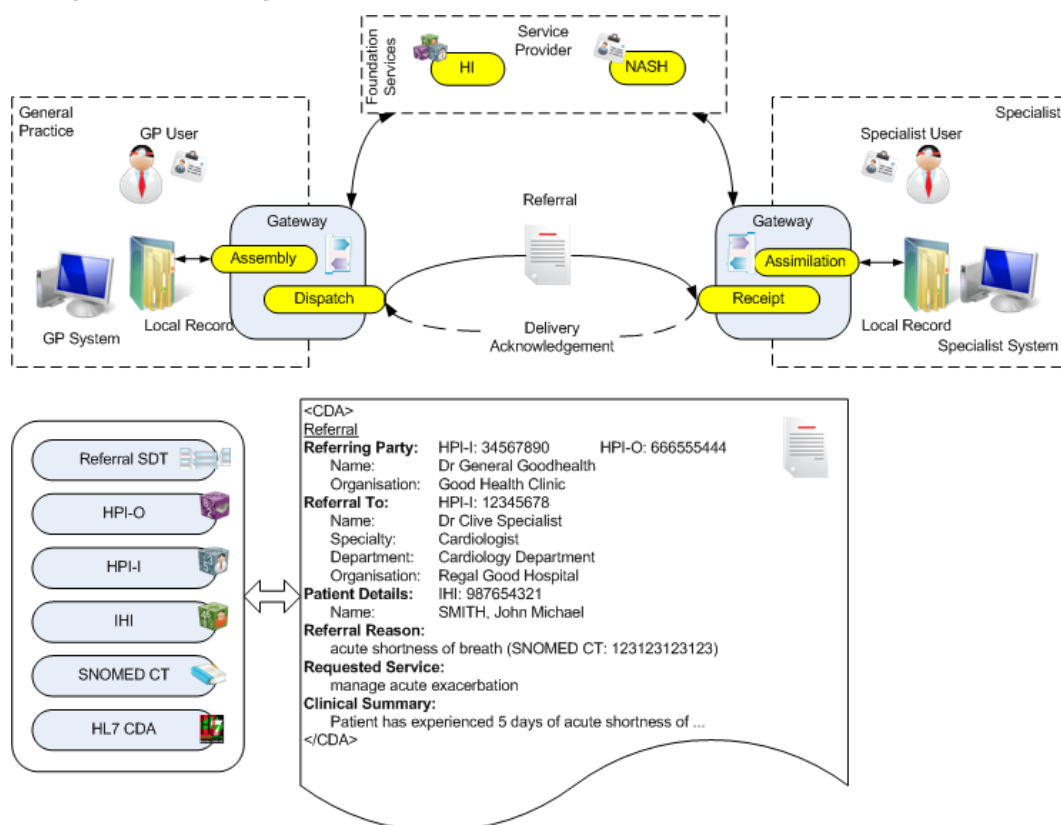


Figure 12 Referrals High Level Component Model

The referral document will contain the minimum clinical information required to optimise collaborative patient care between the general practitioner and the specialist. The majority of this information is expected to be automatically populated by the general practitioner system using data from local records contained within the clinical information systems' electronic medical record (EMR). The referral may also contain additional information manually entered by the general practitioner during the referral document creation process. The structure of the information being sent conforms to the

NEHTA referrals structured document template and is transformed into an HL7 CDA document using the forthcoming NEHTA HL7 CDA implementation guide⁵.

The referrals document will also contain national identifiers for the referrer and referee (HPI-I), the referrer and referee organisation (HPI-O) and the healthcare individual (IHI). Standard terminology (SNOMED CT-AU) will also be used within the structured document⁶.

Assembly, Dispatch, Receipt and Assimilation will be handled by gateway services. These gateway services may be incorporated within the host application(s) or may be a separate component(s), however it is envisaged that the gateway may be used for additional national e-health solutions (e.g. discharge summaries) and utilise a common set of services required to implement best practice services⁷ for B2B integration.

National identifiers and PKI certificates which are used for unique identification and digital security may be sourced by using national infrastructure services. These processes may be optimised (or made redundant) with the use of appropriate caching technologies and/or methods.

5.5 Referrals SOAP Payload Detail

The following section describes the content of the referral's SOAP payload which is sent between end points.

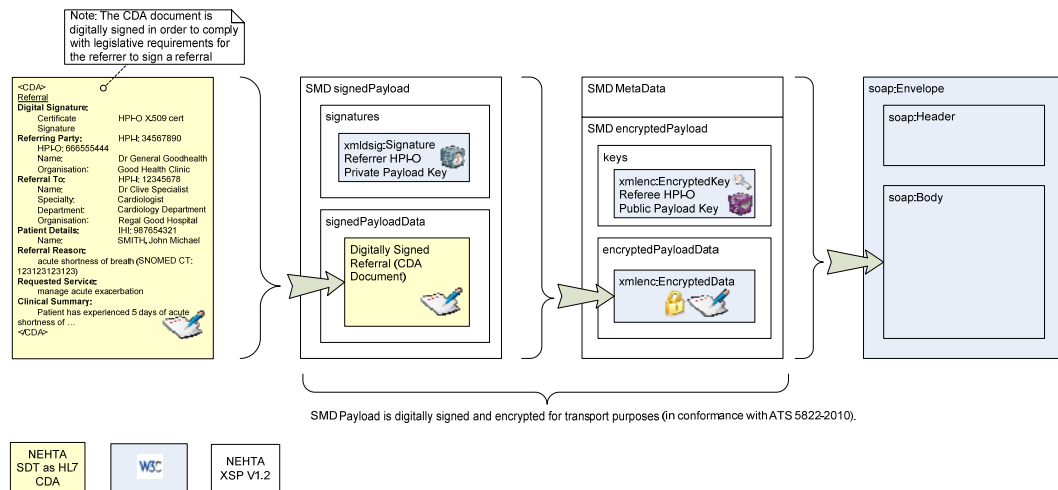


Figure 13 Referrals SOAP Payload Detail

5.5.1 HL7 CDA

The referral will contain structured information as specified within the Referrals Core Structured Document Template v1.0 [ER-SDT2010]. This information will then be formatted using the Referrals Core HL7 CDA Implementation Guide v1.0. The CDA document includes a digital signature which serves the same purpose as the referrer's handwritten signature would for a paper referral. This digital signature is generated using the HPI-O private signing key of the organisation that the individual referrer represents; it serves the purpose of identifying the individual referrer because the signed CDA document also includes the referrer's authenticated name and HPI-I.

⁵ This profile is currently being developed by NEHTA and is expected to be released during 2010.

⁶ As defined within the NEHTA Referrals Core Structured Document Template [ER-SDT2010].

⁷ Such services may include (but are not limited to) Event Logging, Exception Handling, Business Activity Monitoring, and Auditing.

5.5.2 Transport Level Signatures and Encryption

The payload will be digitally signed using the private payload signing key of the healthcare organisation represented by the referrer (or their agent). The signed payload will then be encrypted using the referees' HPI-O public payload encryption key. This will ensure that the contents of the payload cannot be changed and that any intermediaries used for payload delivery are not able to access the content of the encrypted data elements.

Signing and Encryption must occur as per the Australia Technical Specification: E-Health XML Secured Payload Profiles [ATS 5821—2010]

5.5.3 Plain Text Metadata

Plain text metadata will be present within the SOAP body of the message. This text will contain no clinical information and will be used for message routing and orchestration purposes. This is to enable business process managers to act upon the referral messages within the appropriate workflow instance (i.e. such that an 'accept' message can be associated with the corresponding referral instance).

The metadata will be secured by channel level encryption (i.e. TLS) and is not in plain text beyond the sender and the receiver. Please refer to Australia Technical Specification: E-Health Secure Message Delivery [ATS 5822—2010].

5.5.4 SOAP Payload

The SOAP body will contain the referral which in turn has been digitally signed and encrypted for secure messaging purposes. The SOAP body will also contain plain text metadata used for message routing and correlation.

5.6 Message Exchange Scenarios

The following section describes a series of message exchange scenarios using asynchronous document delivery. The transfer of the referral document and the subsequent reception of the transport acknowledgement are two separate transactions.

5.6.1 Referrer and Referee Host Web Services

The following figure depicts a scenario where both the referrer and the referee are hosting an always on ATS 5822—2010 compliant Web services. These services are invoked directly upon the appropriate endpoint for message exchange.

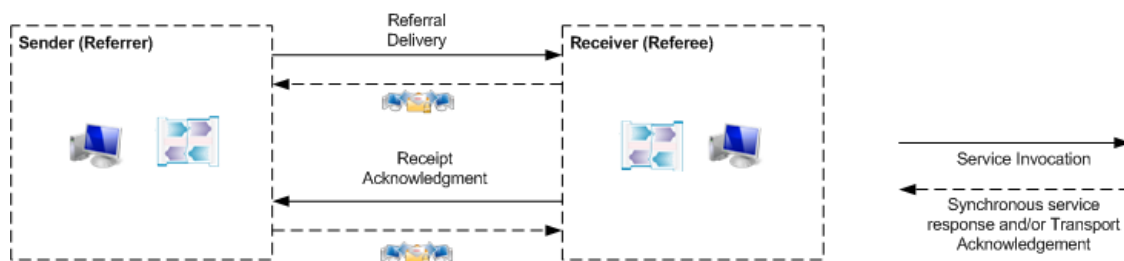


Figure 14 Referrer and Referee host Web Services

5.6.2 Referrer and Referee do not host Web Services

5.6.2.1 Both referrer and referee share a common storage provider

The following figure depicts a scenario where both the referrer and referee are not capable of hosting an always on ATS 5822—2010 compliant Web services

and use the same storage provider. (Although both parties are using the same storage provider, this fact will not necessarily be known by either party). Document delivery and retrieval is achieved by invoking Web services hosted by the storage provider.

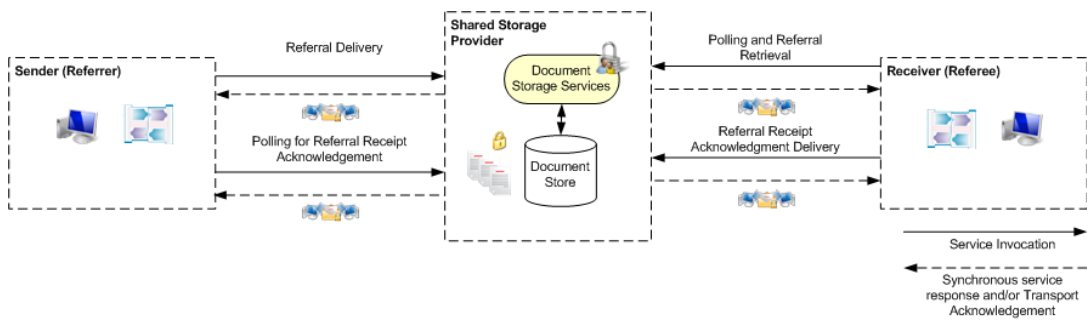


Figure 15 Referrer and Referee Share Storage Provider

5.6.2.2 Referrer and referee use different storage providers

The following figure depicts a scenario where the referrer and referee are not capable of hosting an always on ATS 5822—2010 compliant Web services and use different storage providers. (The fact that both parties are using different storage providers will not necessarily be known by either party). As with the previous scenario, document delivery is achieved by invoking Web services hosted by the appropriate storage provider. However, document retrieval is achieved by the referee invoking the Web services hosted its storage provider.

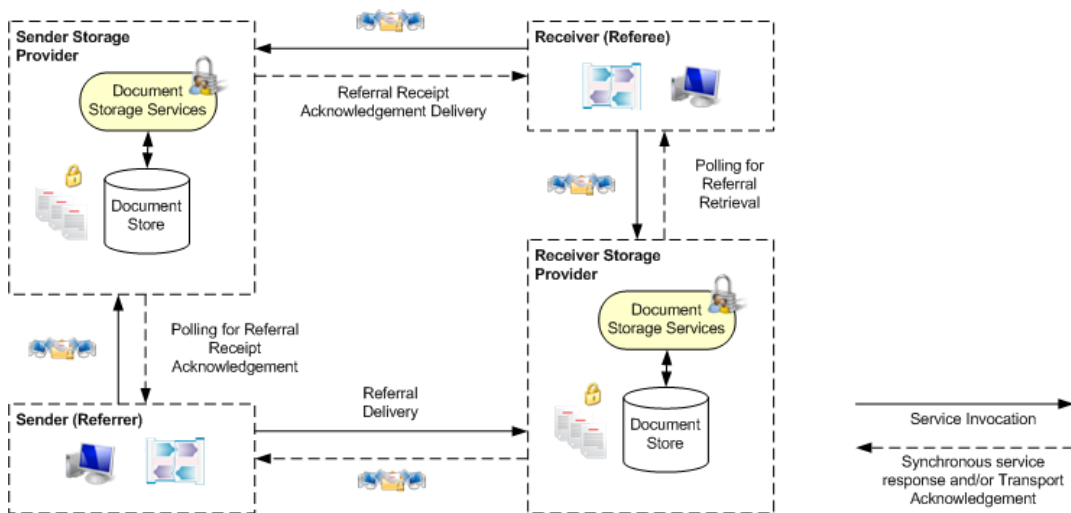


Figure 16 Referrer and Referee use different Storage Providers

5.6.3 Referrer uses a storage provider, Referee hosts Web Service

The following figure depicts a scenario where the referrer is not capable of hosting an always on ATS 5822—2010 compliant Web services (and is therefore using a storage provider) but the referee is capable of hosting such services, and is choosing to do so. The referrer will send referral messages directly to the referee by invoking Web services hosted by the referee. The referee will send referral receipt acknowledgement messages for the referrer to the referrer’s nominated storage provider. The referrer will need to poll its storage provider periodically to retrieve documents.

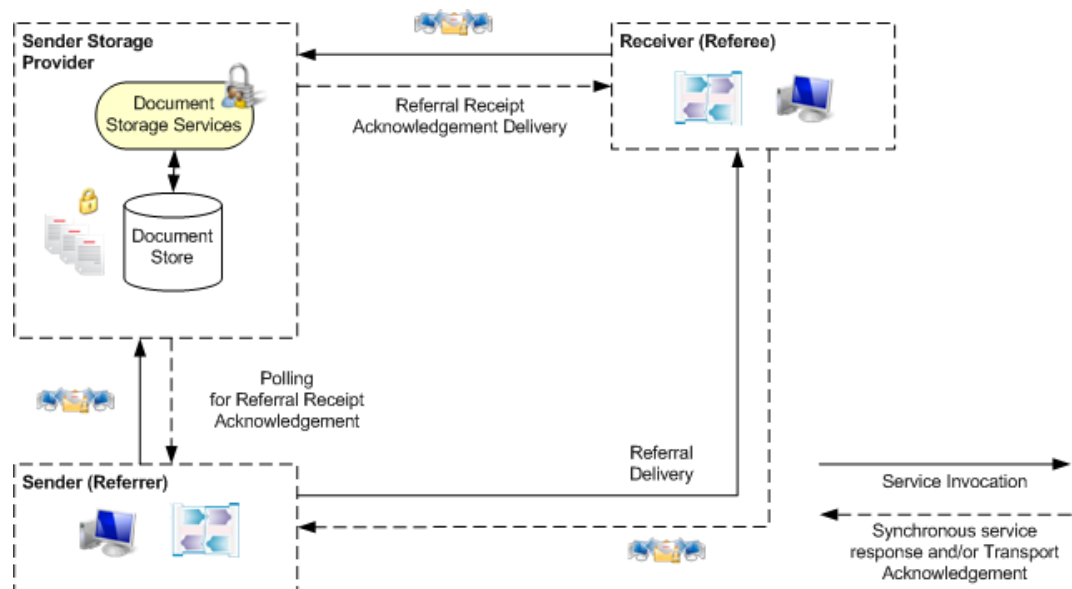


Figure 17 Referrer uses Storage Provider, Referee hosts Web Service

5.6.4 Referrer hosts Web Services, Referee uses a storage provider.

The following figure depicts a scenario where the referee is not capable of hosting an always on ATS 5822—2010 compliant Web services (and is therefore using a storage provider) but the referrer is capable of hosting such services, and is choosing to do so. The referrer will send referral messages for the referee to the referee’s nominated storage provider. The referee will need to invoke its storage provider periodically to retrieve their referral documents. The referee will send referral receipt acknowledgement messages directly to the referrer by invoking Web services hosted by the referrer.

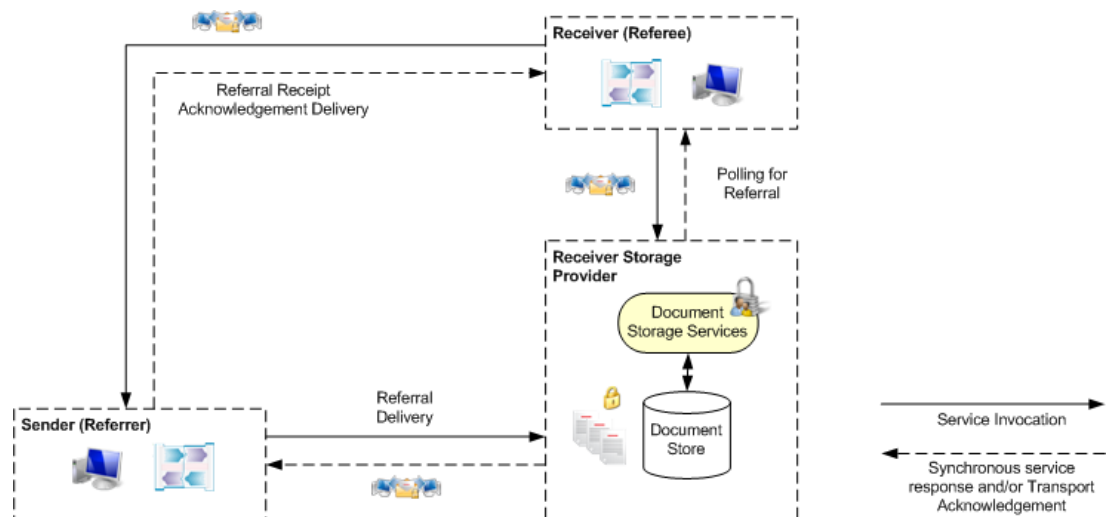


Figure 18 Referrer hosts Web Service, Referee uses Storage Provider

6 Implementation Approach

NEHTA's work program is focused on the development of a nationally-interoperable framework for e-health and facilitated adoption of national specifications, which support the framework by establishing collaborative relationships with early adopter partners and associated vendor and service providers.

With a number of jurisdictions and healthcare providers currently working towards the introduction of state-wide e-Referrals systems, NEHTA is providing guidance and advice on implementation of a national standards based approach.

Given that national referral system projects are at varying stages, ranging from planning to implementation, NEHTA is using an iterative implementation strategy to allow for the uptake of NEHTA specifications in a managed and structured manner over a period of time.

The implementation strategy being employed to facilitate this collaborative approach comprises eight phases. These phases are illustrated in the following figure.

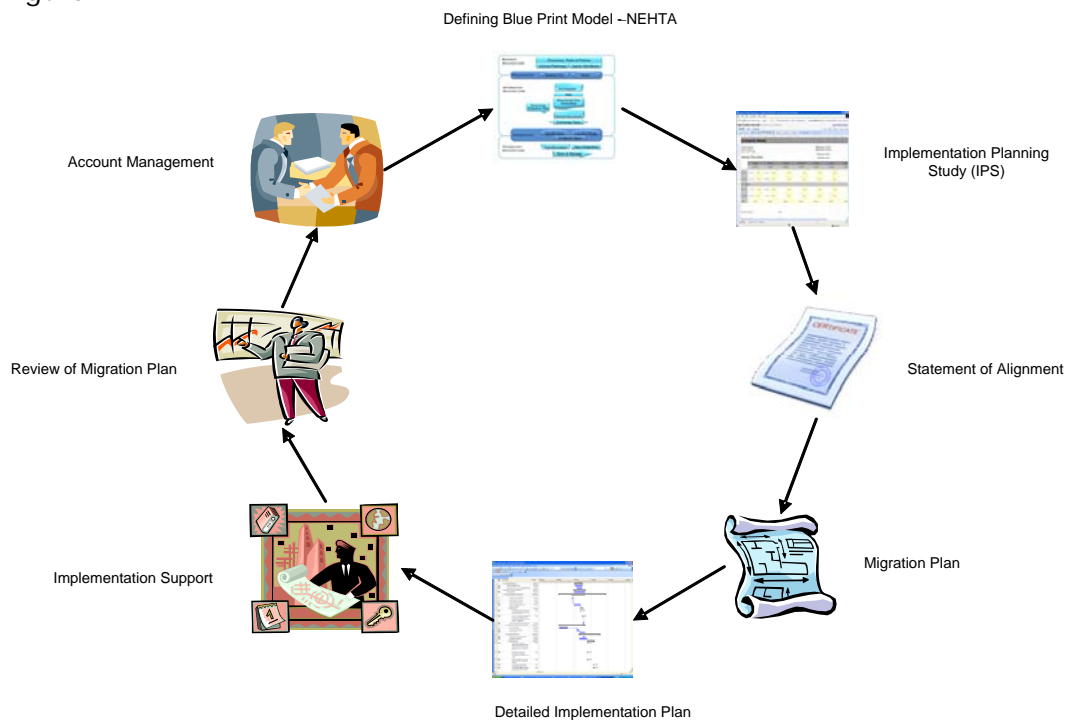


Figure 19 Implementation Strategy Phases

Implementers are invited to contact NEHTA for more detailed discussions regarding implementation strategy, tactics and benefits.

7 Compliance and Conformance

7.1 Introduction

Compliance and conformance assessments are used to demonstrate that specified requirements relating to a product, process or software are fulfilled.

Compliance assessments are applied to organisations to provide assurance of how well their adopted business processes adhere to regulations, policies, standards and specifications.

Conformance assessments are applied to software systems and provide users with some assurance or confidence that the software behaves as expected, performs functions in a known manner, and/or has an interface or format that adheres to a standard.

For each specification, NEHTA will document compliance and conformance criteria and a scheme for assessing the compliance and conformance of services and software systems with each specification. The criteria and assessment scheme will be determined by consultation with stakeholders and will be based on an analysis of the risks of non-conformance and on the feasibility and costs of conformance testing.

7.1.1 Assessment

NEHTA's view is that assessment of conformance should be performed by independent third-party test laboratories or by self assessment. It is important that there is an industry test capability to support the conformance criteria defined in NEHTA specifications. NEHTA will investigate and support the development of an e-health industry test capability to ensure that sufficient capability exists to test software systems against NEHTA specifications. Where insufficient test capability exists in industry then NEHTA will develop a strategy to build this capability with industry.

7.1.2 Declaration of conformance

The main objective of conformance testing is to obtain or issue a declaration of conformance for a software system. A declaration of conformance is not a guarantee of conformance but minimises the risk of non-conformance to an acceptable level.

It is through a declaration of conformance that vendors are able to advertise that their software product(s) have successfully navigated the testing regime. Consequently, procurers are able to locate and identify products that have successfully achieved conformance and use this information to inform their procurement processes and decisions.

7.1.3 Relevance for referrals

NEHTA will consult with stakeholders to develop compliance and conformance criteria for the referrals specification. An assessment scheme will be determined and an industry testing capability will be established to independently test software systems for conformance.

Definitions

This section explains the specialised terminology used in this document.

Shortened Terms

This table lists abbreviations and acronyms in alphabetical order.

Term	Description
CC	Core Connectivity
CI	Clinical Information
CT	Clinical Terminology
EHR	Electronic Health Record
ELS	Endpoint Location Service
HI Service	Healthcare Identifiers Service
ICT	Information and Communication Technology
NASH	National Authentication Service for Health
SDT	Structured Document Template
SNOMED CT	Systemised Nomenclature of Medicine, Clinical Terminology
SNOMED CT-AU	Systemised Nomenclature of Medicine, Clinical Terminology - Australian Extension

Glossary

This table lists specialised terminology in alphabetical order.

Term	Description
Demographic Record	These are the complete details of the IHI Record. This record contains more information about an individual than a summary record, which is disclosed during the search process. (Subject to any special conditions defined).
Department of Health and Ageing	The Department's role is to achieve the Australian Government's priorities (outcomes) for health and ageing. This is done by developing evidence-based policies, managing programs and undertaking research and regulation activities.
Digital Identity	The electronic representation of an individual or provider's actual identity that includes a unique healthcare identifier, associated identifying attributes, permissions, and a supporting token or login (token or login being credentials).
Electronic Health (e-health)	The process of using ICT (information and communication technology) to enable better healthcare outcomes. A longitudinal collection of personal health information concerning a single individual, entered or accepted by healthcare providers, and stored electronically. The information is organised primarily to support continuing efficient quality healthcare and is stored and transmitted securely.
Electronic Health Record (HER)	The Electronic Health Record (EHR) contains information which is retrospective, concurrent and prospective.
Endpoint	Where a Web service connects to the network. Source: http://www.looselycoupled.com/glossary/endpoint
General Practice	General practice is the provision of primary continuing comprehensive whole-patient medical care to individuals, families and their communities.(RACGP)

Term	Description
General Practitioner	A practicing physician who does not specialize in any particular field of medicine (Webster's New World College Dictionary)
General Practitioner System (Health Information System)	Repository of information regarding the health of a subject of care in computer processable form, stored and transmitted securely, and accessible by multiple authorised users. It has a commonly agreed logical information model which is independent of EHR (electronic health record) systems. Its primary purpose is the support of continuing, efficient and quality integrated healthcare and it contains information which is retrospective, concurrent and prospective.
Healthcare Event	This is an instance of providing healthcare to an individual.
Healthcare Identifiers Service (HI Service)	The service which assigns and maintains healthcare identifiers.
Healthcare Provider Identifier Individual (HPI-I)	The unique identifier number that is assigned to a Healthcare Provider Individual.
Healthcare Provider Identifier Organisation (HPI-O)	The unique identifier number that is assigned to a Healthcare Provider Organisation.
Healthcare Provider Organisation	Organisation involved in the direct provision of health activities. This may include departments, sites or location within a Provider Organisation (e.g. hospital radiology department).
Interoperability	The ability of software and hardware on multiple machines from multiple vendors to communicate. Source: The Free On-line Dictionary of Computing. Denis Howe. 21 Apr. 2008. From: Dictionary.com - http://dictionary.reference.com/browse/Interoperability
Medicare Australia	Is the Australian government organisation that administers Medicare, the Pharmaceutical Benefits Scheme (PBS) and a range of other Commonwealth programs.
Medicare Australia Provider Directory System.	The system that records information about healthcare providers whose services directly or indirectly generate a claim for Medicare benefits. It holds the information concerning the identity of the provider, eligibility under Medicare arrangements, and the information necessary for the processing and payment of Medicare claims.
NASH	National Authentication Service for Health
Patient (Healthcare Individual)	These are the individuals who are, or could be, the subjects of care in the context of a healthcare event.
Patient Administration System	A system used by Healthcare Providers to support scheduling, financial and clinical management within a healthcare organisation.
Patient Record	Information relating to a patient, comprising not only earlier and actual diseases but also hereditary disposition, habits, family relations, work and social status.
Provider Directory	This is a provider domain, read only listing of provider information used for facilitating healthcare. It is a white pages of Healthcare Providers, Provider Organisations and provider relationships on a voluntary basis. It does not list Healthcare Individuals and is not available to them.
Specialist	A health practitioner who specialises in and practices one branch of medicine.
Specialist System	IT resources used by specialists to manage patient data and send clinical information to other care providers.

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.

Package Documents

The documents listed below are part of the suite delivered in the E-Referrals Package.

e-Referrals Package Documents			
[REF]	Document Name	Publisher	Link
[ER-ES2010]	e-Referrals Release 1.0 - Executive Summary v1.0	NEHTA 2010	http://www.nehta.gov.au/e-communications-in-practice/ereferral Open menu: e-Referrals Package
[ER-RN2010]	e-Referrals Release 1.0 -Release Notification v1.0		
[ER-BRS2010]	e-Referrals Release 1.0 -Business Requirements Specification v1.0		
[ER-SD2010]	e-Referrals: Solution Design v1.0		
[ER-CIC2010]	e-Referrals Release 1.0 - Core Information Components v1.0		
[ER-TSS2010]	e-Referrals: Technical Service Specification v1.0		

References

The documents listed below are non-package documents that have been cited in this document.

Reference Documents			
[REF]	Document Name	Publisher	Link
[AS4700.6-2006]	Australian Standard 4700.6-2006 "Implementation of Health Level Seven (HL7) Version 2.4, Part 6: Referral, Discharge and health record messaging"	Standards Australia 2006	http://infostore.saiglobal.com/store2/Details.aspx?ProductID=317581
[GNPP2001]	Guidelines to the National Privacy Principles	Office of the Federal Privacy Cmsnr 2001	http://www.privacy.gov.au/materials/types/download/8774/6582
[HIS-COO2010]	HI Service Concept of Operations Version 2.0— 8 June 2010, Release – Final	NEHTA 2010	http://www.nehta.gov.au/connecting-australia/healthcare-identifiers Open menu: Concept of Operations
[NBP2010]	NEHTA Blueprint	NEHTA 2010	http://www.nehta.gov.au/about-us/nehta-blueprint
[TR 5823—2010]	Technical Report: Endpoint Location Service	Standard Australia Committee IT-014 Health	http://www.e-healthstandards.org.au/Home/Publications.aspx

Reference Documents			
		Informatics	
[MBSB2009]	Medicare Benefits Schedule Book, November 2009	Australian Govt. Dept. of Health & Ageing 2009	http://www.health.gov.au/internet/mbsonline/publishing.nsf/Content/Medicare-Benefits-Schedule-MBS-1
[ATS 5820—2010]	Australia Technical Specification – E-Health Web Services Profiles	Standard Australia Committee IT-014 Health Informatics	http://www.e-healthstandards.org.au/Home/Publications.aspx
[ATS 5821—2010]	Australia Technical Specification – E-Health XML Secured Payload Profiles	Standard Australia Committee IT-014 Health Informatics	http://www.e-healthstandards.org.au/Home/Publications.aspx
[ATS 5822—2010]	Australia Technical Specification – E-Health Secure Message Delivery	Standard Australia Committee IT-014 Health Informatics	http://www.e-healthstandards.org.au/Home/Publications.aspx

Related Reading

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

Related Documents			
[REF]	Document Name	Publisher	Link
[ELSA2009]	Endpoint Location Service Architecture v1.2	NEHTA 2009	http://nehta.gov.au/connecting-australia/secure-messaging
[ER-SDT2010]	Referrals Core Structured Document Template v1.0	NEHTA	Scheduled for release 2010.

Appendix A: Sample e-Referrals Architecture

The following section describes an example implementation of the e-Referrals package. It identifies the major software components, their characteristics, and the interactions between them.

The system architecture outlined here supports the use cases and requirements set out for this package. It is not, however, intended to be a complete 'blueprint' for building referral solutions; rather, the intent is to focus on key aspects affecting interoperability. It must be noted that individual implementation may involve more or less system components than is described here.

Each subsequent section will then decompose specific components and describe these in more detail. It should be noted that the components shown within the following sections are logical. How these components are realised in a physical implementation will vary from vendor to vendor.

A.1 General Practitioner/Specialist Component Model

The following figure shows a nominal view of logical software components used by the practitioner (general practitioner and/or specialist) within the practice.

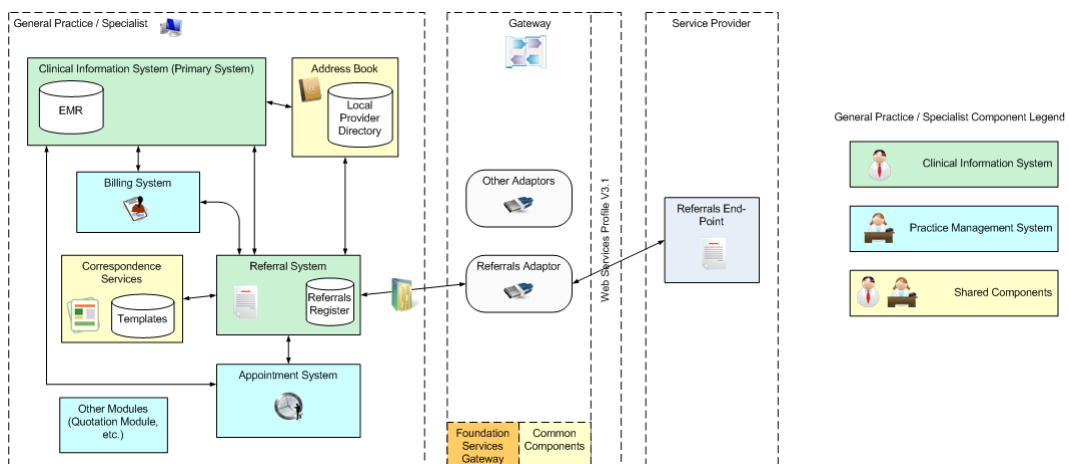


Figure 20 General Practitioner/Specialist Component Model

The logical components of particular interest within the referrals solution are detailed below.

A.1.1 Clinical Information System (CIS)

The CIS is the component which maintains clinical information about healthcare individuals, and will also have interfaces to various other components within the application, such as the referral system and the address book.

- Key Function:
 - Maintains electronic medical records for healthcare individuals of the practice.

The CIS will integrate directly with the Referral System. The integration will support the pre-populating of the referral from structured data contained in the EMR for the healthcare individual being referred.

The referral information contained within the referral document will be stored within the patient EMR. Healthcare individual and provider demographic details may be sourced from the address book.

A.1.1.1 Electronic Medical Record (EMR)

The EMR will contain structured clinical information, patient record and other documents (scanned or otherwise such as radiological images, radiology reports and pathology results).

The information contained within the EMR will pre-populate the referral with the relevant clinical information.

A.1.1.2 Referral System

The referral system is a component which manages the complete end-to-end referral business process including human-driven workflow process steps. This includes the initial creation of a referral from the referring practitioner to the creation of the final outcome report and assimilation within the referring practitioner's EMR.

- Key Functions:
 - Maintain referral workflow state
 - Provide alerts and/or exceptions for referral business conditions which require special attention or action by the appropriate person (e.g. general practitioner or practice manager)
 - Referral administration and workflow tracking
 - Interface directly with the appointment system
 - Referral reporting and auditing.

A.1.1.3 Referrals Register

The referrals register is the storage facility for referral documents. This will include metadata for managing referral state transitions as the referral progresses through the various stages of the referral business workflow. The referrals register will be used by the referrals system to generate alerts and exceptions, and allows the general practitioner and/or the practice manager to check on the progress of any outstanding referrals.

- Key Function:
 - Referrals metadata storage facility.

A.1.2 Practice Management System (PMS)

The PMS is made up of logical components used for administrative (i.e. non-clinical) purposes for the day-to-day operation of a practice.

A.1.2.1 Billing System

The billing system is used to manage all healthcare individual billing and accounting functions of the practice. It is integrated directly with the CIS and the referral system. The system will include a comprehensive set of reports for analysis and tracking.

- Key Functions:
 - Maintains payer and provider accounting details
 - Generates accounting/billing reports.

A.1.2.2 Appointment System

The appointment system is used for appointment tracking and scheduling. Practitioners and practice managers can get a total view of the workday⁸ and efficiently manage their working schedule.

- Key Functions:
 - Multi-practitioner scheduling
 - Centralised and consolidated practice-wide appointment tracking
 - Appointment searching facilities
 - Missed appointments and rescheduling.

A.1.3 Shared Components

A.1.3.1 Address Book

The address book is used to store address and general contact information about healthcare individuals. The address book may also store national identifiers previously provided by the HI Service. These identifiers may be sourced via a batch process, an asynchronous background process, or on demand as required.

- Key Function:
 - Provides contact and demographic information for healthcare individuals.

A.1.3.2 Local Provider Directory

The local provider directory offers a local 'yellow pages' type searching facility to locate providers for one or more specific services. The provider directory may also store national identifiers previously sourced from the HI Service. The directory may also store previously-cached Endpoint Location Service (ELS) information for invoking referral Web services.

- Key Function:
 - Search capabilities for providers based on services offered.

A.1.3.3 Correspondence Services

Correspondence services are used to create referral and other clinical documents to be used for external correspondence with the patient and other providers. These services may integrate with external applications such as word processors (e.g. MS-Word, Open Office) or support direct document editing facilities. Clinical correspondence may use structured data extracted from the patients EMR within the CIS in conjunction with templates to produce clinical reports and/or letters.

- Key Function:
 - Template-based document creation.

A.1.3.4 Templates

The correspondence services will use a set of templates to provide automated tokenised text replacement facilities to extract structured data and demographic details from patient EMRs to produce the appropriate document. Different templates may be used for the referral, depending upon the target speciality of the referred provider. This process may be automated to varying degrees, such that the provider information sourced from the local provider directory may contain metadata which may be used to drive business rules to

⁸ The system may support a calendar style user interface where different views may be selected such as Day, Week and/or Month.

determine which templates (default or otherwise) are available for referral creation.

- Key Function:
 - Template repository

A.1.4 Other Modules

Other modules may exist within the practice system, such as a quotation module for specialists, but are currently outside the scope of this package.

A.1.5 Desktop Operating System Components

The practice software will operate on a computer operating system and utilise a number of additional applications and/or components which all work together to form the complete practice software solution.

- Noteworthy components:
 - Office Productivity Applications (such as MS-Office or Open Office)
 - Computer File System (as supported by the relevant operating system, such as NTFS or HPFS)
 - Certificate Storage (X.509 certificate and other credentials, keys and passwords)
 - Cryptographic Services (a set of API's which allow for the programmatic implementation of digital security)
 - Application Frameworks (generic programming frameworks on which applications are built such as .NET and Java)
 - Database (back-office database facilities and services, such as those offered by SQL Server etc.).

A.1.6 Gateway

Assembly, Dispatch, Receipt and Assimilation will be handled by gateway services. The gateway will be used for all external integration needs within the practice IT system. It will be developed in such a way as to allow for additional extensions to be subsequently integrated in the form of adaptors. In addition, it will use a common set of libraries and infrastructure components to allow for this extensible architecture.

- Key Functions:
 - Dispatch and Receipt of messages to and from externally facing entities
 - Assembly and Assimilation of messages in and out of the core application(s)
 - Standard integration facilities such as (but not limited to) Event Logging, Exception Handling and Auditing
 - Offer an extensible architecture to allow for maximum re-use, flexibility and adaptability
 - Caching of appropriate information (such as national endpoint addresses) to improve system performance
 - Include integration with national infrastructure services.

A.1.6.1 Referrals Adaptor

The referrals adaptor is used to transform the local referrals information into HL7 CDA, ready for transmission to an external party. This will include the use of the appropriate terminology reference sets. The adaptor will also provide

proprietary interfacing between the practice IT system (specifically the referral system previously mentioned) and the gateway itself. The gateway will provide standardised interfacing between the practice and the outside world.

A.1.6.2 Other Adaptors

Other adaptors may be used within the gateway to support other clinical solutions such as discharge summaries and/or pathology results. The gateway architecture is designed in such a way as to minimise the amount of development effort required to build these additional adaptors, given that the common libraries and components used within the gateway handle standard implementation requirements to meet NEHTA interoperability specifications⁹.

A.1.6.3 Foundation Services Gateway

This sub-gateway is used for direct interfacing with national infrastructure services such as NASH, Base-ELS (for bootstrapping) and HI Services (IHI and HPI).

A.1.6.4 Common Components

Common components and libraries are used throughout the implementation of the gateway to allow for maximum re-use. The gateway can be extended with other adaptors (such as those for discharge summary and/or pathology). Common components may include (but are not limited to) identifier mapping, obtaining PKI certificates, digital security¹⁰ and secure messaging.¹¹

A.1.6.5 Web Services Profile

The gateway uses Australia Technical Specification: E-Health Web Services Profiles [ATS 5820—2010] for all external secure messaging interactions with the outward-facing community. The Referrals Technical Service Specification [ER-TSS2010] will specify the use of the Australia Technical Specification: E-Health Secure Message Delivery [ATS 5822—2010].

A.1.7 External Components

7.1.3.1.1 Referrals Endpoint

A referrals endpoint is any other NEHTA-compliant referrals-capable recipient. This may include third party messaging vendors, provided that these vendors support the required specifications (such as [ATS 5820—2010]). The endpoint location will be sourced from the appropriate ELS record (locally cached or otherwise).

A.2 Gateway Logical Components

The following section describes the core components and processes which may be part of the gateway within the general practitioner/specialist IT system.

Note: Conceptually, these functions would also be required within a hospital context.

⁹ Such as the Web Services Profile V3.1 [WSP2009], XML Secure Payload Profile V1.2 [XSP2009] and invoking national infrastructure services such as the NASH and the HI.

¹⁰ NEHTA XML Secured Payload Profile v1.2 [XSP2009]

¹¹ NEHTA WSP V3.1 [WSP2009]

A.2.1 Assembly and Dispatch

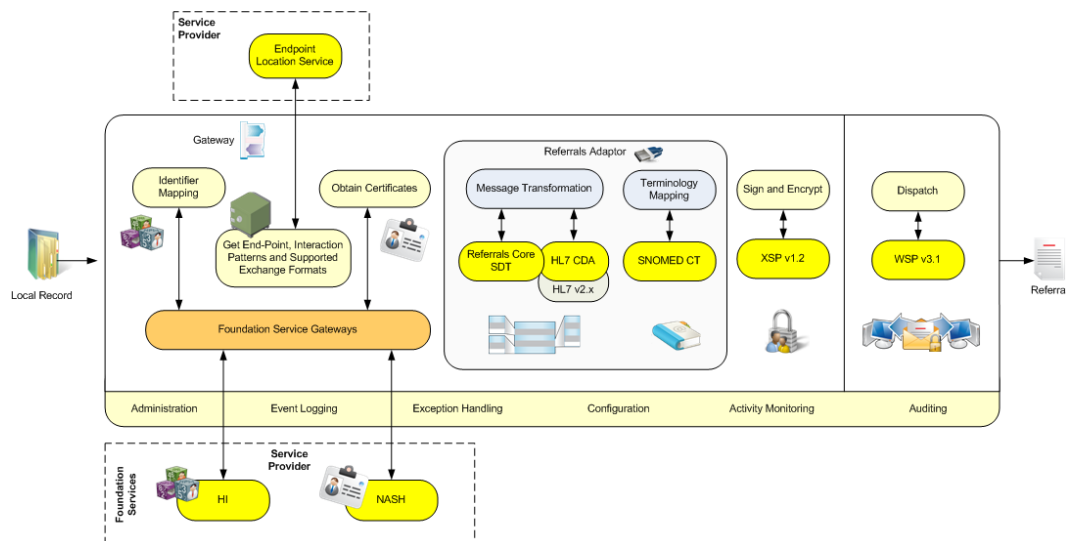


Figure 21 Gateway Assembly and Dispatch

A.2.1.1 Identifier Mapping

The identifier mapping component is used to translate local CIS identifiers for organisations and people¹² into national identifiers such as HPI-O, HPI-I and IHI. This step may not be required if the local CIS incorporates these identifiers within the core application. The national identifiers may already be available through the local address book and may have been downloaded and/or linked using an asynchronous batch update or background population process.

Where the national identifiers are not available locally, the foundation services gateway may be used to look-up the identifiers required. This is achieved by supplying local system attributes (such as person name, organisation name, etc.). The foundation services gateway would then invoke the appropriate Web services from the HI service.

Note: Any ambiguous matches (e.g. searching for a unique person and retrieving many results) would need to be resolved manually by the end-user before the message could be sent to the next endpoint.

The HI services (specifically HPI-O) will also return the endpoint location for the required organisation’s ELS service. This ELS service will be used to obtain the ELS record for electronic interaction with the referee. This information may be cached locally.

A.2.1.2 ELS Record Lookup

The Endpoint Location Service (ELS) contains entries of electronic services provided by the healthcare organisation and the endpoints for the invocation of those services. The ELS may also indicate which interaction pattern needs to be used, which referral template and mapping profile is required for payload creation and finally the required PKI certificate references required for digital security and messaging. Note that the information returned from the ELS lookup may be cached locally so that future interactions with the same provider organisation can be used directly without the need for the ELS lookup. A passive style ‘fail and retry’ model is used in this case to refresh entries within the local cache if the current ELS information results in failed interactions. The ELS service endpoint of the organisation would have already been provided by an HPI-O lookup to the HI Service. The referee’s ELS endpoint address is then used by the referrer (by invoking the referee’s ELS) to determine the referrers’ endpoint location, and their service capabilities for

¹² In the future, this may also include Clinical and/or Human Services as well.

the purposes of sending the e-Referral. This may have occurred as part of the identifier mapping process but may have been downloaded 'out-of-band' via some other asynchronous background process. However, it must be noted that ELS is an independent specification. An organisation not part of the HI service (i.e. does not have a HPI-O) can advertise its ELS through other channels/provider directories.

A.2.1.3 Obtain Certificates

This component is used to retrieve the X.509 Public Key Infrastructure (PKI) certificates from the foundation service gateway component (which in turn invokes the NASH service as required). This component may also be used to validate certificates by checking the CRL and/or using OCSP. Certificates may be retrieved by passing a certificate reference and/or a national identifier (such as an HPI-O). Once PKI certificates have been downloaded, these may be cached locally (using operating system services such as the Windows Certificate Cache or otherwise). PKI certificates may also be cached within externally hosted provider directories.

A.2.1.4 Referrals Adaptor

The referrals adaptor is a package-specific component whose primary function is transforming the local referral record set into the appropriate NEHTA-compliant format. This will include the use of terminology reference sets also defined as part of the SDT release and digital signatures for clinical purposes. The architecture of the gateway is such that package specific components (or other components) can be 'plugged into' the gateway so as to re-use all of the gateway standard libraries and/or infrastructure services in a consistent way. The referrals adaptor acts as an interface bridge between the referrals system and the gateway.

A.2.1.5 Message Transformation

The function of the message transformation component within the assembly context is to take the local CIS referral record set (rendered in the proprietary format used within the core system¹³) and transform this information into the appropriate NEHTA-compliant referral format. The data and format will be specified within the e-Referrals SDT and HL7 CDA implementation guide, planned for a future release by NEHTA. Technologies such as XSLT or other mapping libraries/tools may be used where appropriate.

A.2.1.6 Terminology Mapping

This function is the process of mapping reference set values from the local CIS to the NEHTA specified terminology values (SNOMED CT-AU) for the e-Referrals SDT. This will be specified within the NEHTA terminology reference set profile.

Note: Terminology mapping may not be necessary if the local CIS incorporates SNOMED CT-AU reference set values within the application.

A.2.1.7 Sign and Encrypt

This component is used to digitally sign and encrypt content within message payloads. The signing and encryption methods used must conform to the Australia Technical Specification: E-Health XML Secured Payload Profiles [ATS 5821—2010]. Cryptographic API's will be used to perform the required encryption. The referrals adaptor will invoke the functions offered by this component to digitally sign the referral using the referring organisations private payload signing key. The signed payload will then be encrypted by using the referee organisation's public payload encryption key.

¹³ The CIS needs to support at least the minimum mandatory fields, specified within the NEHTA Referrals SDT as structured data.

A.2.1.8 Dispatch

The dispatch component is used to invoke Web services at the required endpoint. These interactions must conform to the Australia Technical Specification: E-Health Web Services Profiles [ATS 5820—2010]. The Referrals Technical Service Specification will specify the use of the Australia Technical Specification: E-Health Secure Message Delivery [ATS 5822—2010]. The content used within the Web service calls will include NEHTA-compliant referrals.

A.2.1.9 Receipt and Assimilation

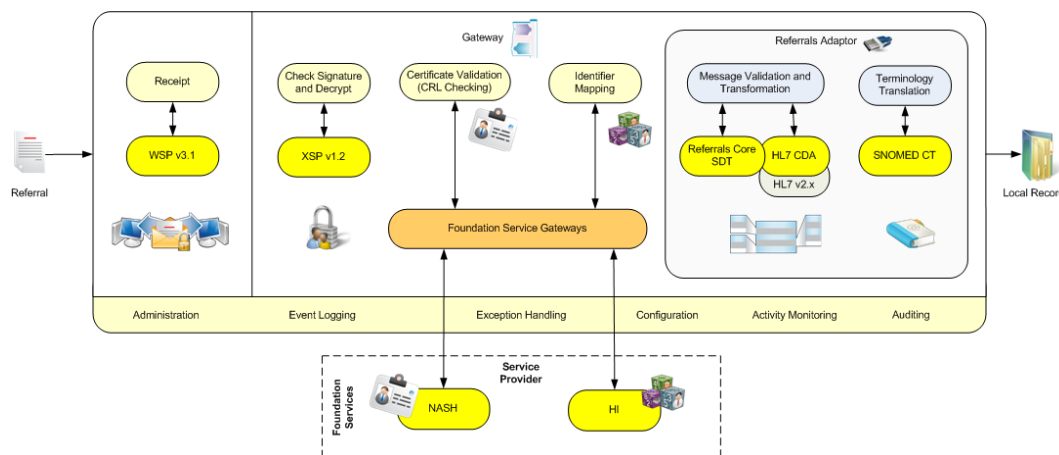


Figure 22 Gateway Receipt and Assimilation

A.2.1.10 Receipt

The receipt component is used to receive inbound Web service calls. These interactions must conform to the Australia Technical Specification: E-Health Web Services Profiles [ATS 5820—2010] and the Referrals Technical Service Specification.

A.2.1.11 Check Signature and Decrypt

This component is used to decrypt the secured content within the message and/or payload. Once decrypted, any digital signature within the payload should also be processed (i.e. the signers' identity and authenticity can be asserted by the receiver using the appropriate PKI technologies). The digital signature and encryption methods used must conform to the Australia Technical Specification: E-Health XML Secured Payload Profiles [ATS 5821—2010]. Also, cryptographic API's will be used to perform the required decryption.

A.2.1.12 Certificate Validation

The certificate validation step is used to check the validity of all the certificates which have been used to sign the payload. The foundation service gateway component can be used for validation (which will in turn use the appropriate NASH service if required).

A.2.1.13 Identifier Mapping

The identifier mapping component is used to translate national identifiers (HPI-O, HPI-I and IHI) into local CIS system identifiers for individuals and organisations. This step may not be required if the local CIS incorporates these identifiers within the core application. The national identifiers may already be available through the local address book and may have been downloaded and/or linked using an asynchronous batch update or background population process.

Where the national identifiers are not available locally, the local CIS will need to perform identity matching (i.e. person and/or organisation). This is achieved by trying to match the supplied identifying attributes within the payload (such as person name, organisation name, etc.) to the correct entries found within the local address book. Note that any ambiguous matches would need to be resolved manually by the end-user before the message can be correctly processed within the referrals system.

A.2.1.14 Referrals Adaptor

The referrals adaptor is a package-specific component whose primary function is for structured data transformation, terminology translation and local system (i.e. referral system) interfacing.

A.2.1.15 Message Validation and Transformation

The function of the message transformation and validation component in the referral assimilation context is to take the NEHTA-compliant HL7 CDA document and transform this into the local CIS referral record set. The data and format will be specified within the Referrals SDT [ER-SDT2010] and Referrals HL7 CDA implementation guide, planned for subsequent release. Use of technologies such as XSLT or other mapping libraries/tools should be used where appropriate.

A.2.1.16 Terminology Translation

This function is the process of mapping (or 'terminology binding') SNOMED CT-AU reference set values from the referral document(s) to the local CIS terminology values. This will be specified within the NEHTA terminology reference set profile. Translation may not be necessary if the local CIS incorporates SNOMED CT-AU reference set values within the application.

A.2.2 Foundation Service Gateways

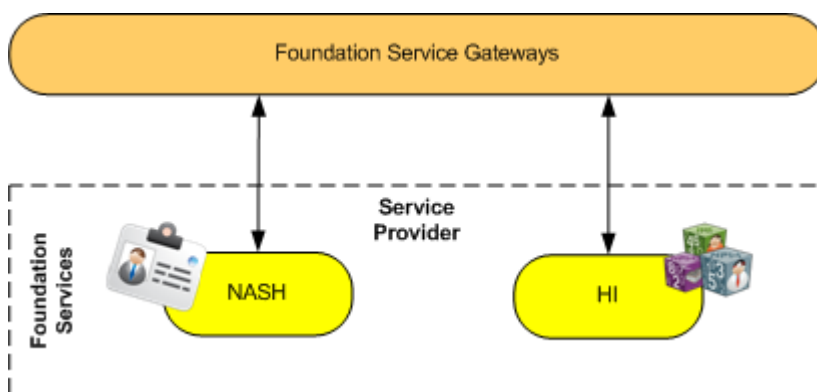


Figure 23 Foundation Service Gateways

The foundation service gateways component is used as an interface between the common gateway components and national infrastructure services. It may also provide caching facilities for PKI certificates and ELS records depending upon implementation.

A.2.2.1 Health Identifier (HI) Interface

The HI interface will provide proxy services for the HI HPI and IHI Web services. The HPI services will be used to provide HPI-O and HPI-I identifiers interactively from identifying information (e.g. name, date of birth) supplied by calling components. The HPI-O service will also return the endpoint for the provider's ELS. The IHI service will return an individual's national identifier by supplying the relevant person's name and other identifying information. The foundation service component may also provide caching facilities for previously downloaded information. Access to the national infrastructure

services will be mutually authenticated using TLS and the caller's HPI-O certificates.

A.2.2.2 National Authentication Service for Health (NASH) Interface

The NASH interface will provide proxy services to the NASH services for PKI certificate retrieval and CRL retrieval. Certificate and CRL retrieval will be via HTTP or LDAP. Access to the HTTP and LDAP directory will not require any authentication or encryption. Calling components will provide certificate references (returned from ELS record information) and/or national identifiers as parameters to the proxy functions. The certificate retrieval interface may also use caching to improve efficiency.

A.2.3 Gateway Core Services

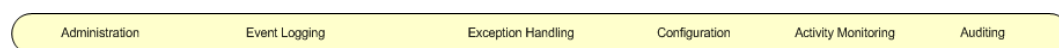


Figure 24 Gateway Core Services

The gateway component will provide a number of core services as part of the overall component infrastructure. Some of these services may be invoked from other components within the gateway (e.g. Event Logging, Exception Handling) or be used as part of normal gateway operation (e.g. Administration, Activity Monitoring, Configuration).

A.2.3.1 Administration

This service allows the gateway to be administered (remotely or locally) by the appropriate technical user. The service allows for day-to-day operations of the gateway to be performed as required (e.g. checking audit logs, monitoring current activity, trouble-shooting).

A.2.3.2 Event Logging

Event logging will be used throughout the gateway to record all significant events (e.g. message receipt and dispatch). The type of events being logged will be highly configurable and the level of event logging would vary from installation to installation. Specific event types (such as exception events) may also trigger administrative alerts.

A.2.3.3 Exception Handling

This service will provide consistent exception handling facilities. Exception handling performed in a consistent way will ensure that technical assistance can be made with improved efficiency. The exception handling service(s) may also provide automated alerts (via e-mail or otherwise) to system administrators.

A.2.3.4 Configuration

Configuration services allow the gateway to be configured and optimised for the specific installation. Functions may include configurable event logging types, message processing metrics, alert message delivery methods (e.g. SMS and/or e-mail) and gateway operational times (to allow for system maintenance and backup).

A.2.3.5 Activity Monitoring

This facility allows administrators to view (locally and/or remotely) the current health and activity of the gateway over a specific period, or in real-time. This will allow administrators the ability to 'tune' the gateway for best operational performance.

A.2.3.6 Auditing

This allows administrative staff to report on specific events which have been captured during the operation of the gateway including messages sent, received and/or viewed by staff.

A.3 Foundation Services Gateway - Bootstrapping

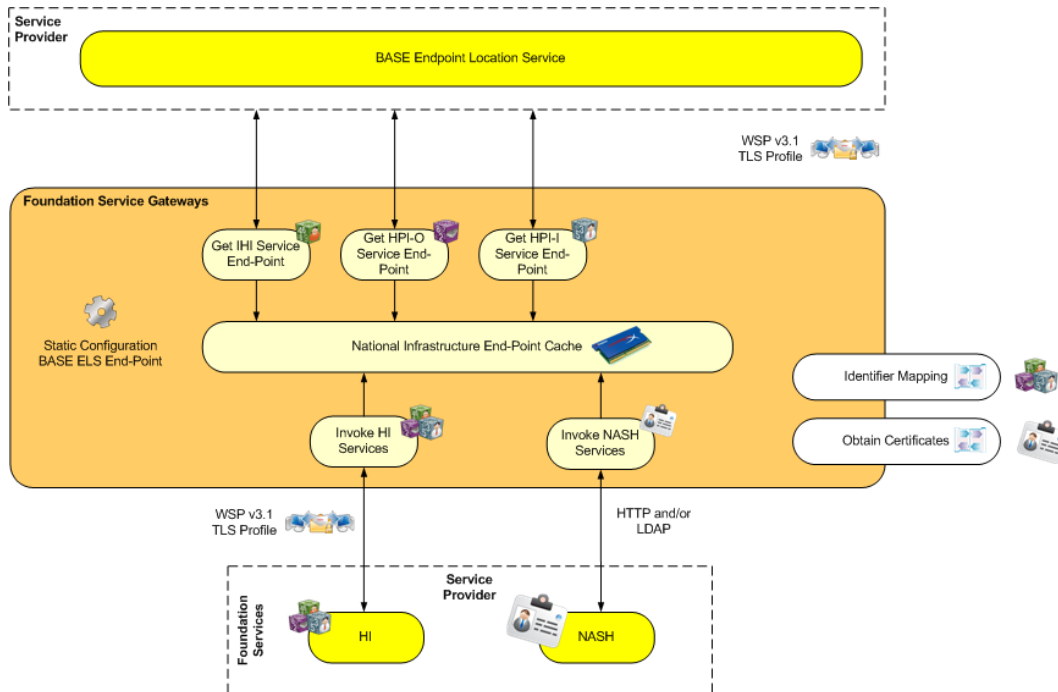


Figure 25 Foundation Service Gateways - Initialisation

The gateway will provide access to a number of core national infrastructure services such as the NASH and HI. The foundation service gateway (a sub-component of the gateway) will act as a proxy (i.e. encapsulating national infrastructure access-instances and allowing for caching, etc.) for these services. In order for this to occur, the foundation service gateway will need to be configured with the endpoint for these national infrastructure services (with the exception of NASH, as access to the NASH services will be via HTTP and/or LDAP). This will be achieved during the start-up process when the gateway is first initialised.

The foundation service gateway will contain the fixed endpoint address for the BASE ELS service. This service will be used to return the endpoint locations for all other national infrastructure services. In this regard, only the BASE ELS endpoint address needs to be 'static'. It is envisaged that this will be part of the static configuration within the foundation service gateway.

Prior to any interaction with HI services, the foundation services gateway will load the ELS records for each of the core national infrastructure services:

- IHI Service
- HPI-O Service
- HPI-I Service

Ideally, each of these endpoints will be locally cached so that the bootstrapping process only occurs when necessary (i.e. until a refresh is required due to an unknown endpoint location interaction failure with one or more of the infrastructure services).

Each of the interactions with the BASE ELS and the national infrastructure services will be handled securely using the TLS profile of the Australia

Technical Specification: E-Health Web Services Profiles [ATS 5820—2010]. For this reason, only the initiating (calling) provider organisation certificate is required for authentication.