



Service Instance Locator

Requirements

Version 1.1 — 1 December 2008

Release

National E-Health Transition Authority Ltd

Level 25

56 Pitt Street

Sydney, NSW, 2000

Australia.

<http://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 © 2008, 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.

Table of contents

Table of contents	iii
Document information	iv
Change history	iv
1 Introduction	1
1.1 Background	1
1.2 Purpose	1
1.3 Scope	1
1.4 Definitions, acronyms, abbreviations	1
1.5 Overview	1
2 Service Instance Locator	2
2.1 Summary of Purpose	2
2.2 Requirements	2
2.2.1 Informational Perspective	2
2.2.2 Business Perspective	4
2.2.3 Technical Perspective	5
Appendix A: References	7

Document information

Change history

Version	Date	Comments
1.0 draft	2008-09-01	Draft for review
1.1	2008-12-01	Release

1 Introduction

1.1 Background

NEHTA national E-Health Infrastructure has identified the need for a Service Instance Locator (SIL). SIL is a directory allowing service instances (i.e. deployed service implementations) to be located.

1.2 Purpose

This document lists requirements for the Service Instance Locator.

1.3 Scope

This document deals with the requirements on the Service Instance Locator. It does not deal with the applications that use it or the business drivers for them.

This document is intended for:

- Business analysts; and
- Enterprise and solution architects.

1.4 Definitions, acronyms, abbreviations

HPI	Healthcare Provider Identifier
HPII	Healthcare Provider Identifier for Individuals
HPIO	Healthcare Provider Identifier for Organisations
NEHI	National E-Health Infrastructure
NEHTA	National E-Health Transition Authority
NASH	National Authentication Service for Health
Service Provider	An organisation that hosts a technical service, primarily a Web service, on behalf of a HPIO. It may be a healthcare provider organisation or a third party proxy organisation.
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
WSDL	Web Services Description Language

1.5 Overview

Requirements are divided into sections based on the perspectives of the Interoperability Framework [NIF2007].

2 Service Instance Locator

2.1 Summary of Purpose

Service Instance Locator (SIL) is a kind of directory for technical (electronic) services offered by a healthcare organisation. It allows any client in the e-health community to discover a service interface and bind at run time.

SIL enables message (e.g. clinical document) exchange from a producer to an intended recipient, even if the producer has no prior knowledge of how the recipient handles such a transfer. For example, a hospital may need to send a patient discharge summary to a clinic where the patient would be receiving further treatment. The clinic would have a record in its SIL containing enough information for the hospital to make the discharge summary available.

SIL is implemented as a Web service. A SIL lookup operation returns a set of structures containing Web service endpoints to actually facilitate document transfer.

Different modes are defined to perform the task, such as deliver (upload) and retrieve (download). In some cases a Web service may be hosted externally, i.e. by a third party, so a notification may be have to be sent before the document itself. Consequently, the structure returned by SIL lookup contains information on how to use the transfer services.

Each healthcare provider organisation should have one associated SIL. However, it is possible for multiple healthcare providers to share a SIL instance. If desired, one SIL instance could function as standalone central service or as a large regional service. Alternatively, an instance could be part of a fully distributed SIL environment, associated with one or just a few healthcare organisations. Any of these SIL deployment models can be accommodated from technical standpoint.

There is no need to use SIL services if two parties already understand how to exchange documents. If a document provider had previously looked up a recipient's SIL, there is no need to perform another lookup for another transfer. Once a SIL record has been downloaded, it may be reused indefinitely, or until permanent failure. As a convenience to clients, there is a SIL operation allowing for validity checking of previously obtained records.

2.2 Requirements

2.2.1 Informational Perspective

Informational requirements relate to the data that is stored and returned by a SIL instance (implementation). Design of SIL interfaces are most affected by these requirements.

IR.01	SIL MUST include a lookup operation to discover service endpoints.	The primary reason for the existence of SIL. Without a standard mechanism to locate document transfer services, ad-hoc procedures would be devised. These would likely lead to restrictions and inconsistencies.
IR.02	Each HPIO MUST be associated with only one SIL instance.	Ensures that a SIL lookup service offered by any healthcare organisation is available to all healthcare providers. There is a 1:n relationship of SIL:HPIO.
IR.03	SIL lookup MUST include support for all document exchange interaction patterns	Allows for the various supported interaction modes to accomplish

	as referenced by [CPIS2008].	document exchange.
IR.04	Interaction patterns MUST be searchable based on service category.	Allows for searches to be narrowed based on the kind of clinical document to be transferred, e.g. discharge summaries, pathology reports.
IR.05	SIL lookup information MUST match service endpoints with service roles described by interaction patterns.	Relates IR.01 to IR.03. It states that there must be a way to match a service with the correct interaction role. This is especially a consideration when the interaction pattern supports more than one role, e.g. deliver and notify.
IR.06	SIL lookup information MUST include service provider identification.	To ensure that that service provider information is known. Service provider may be different to the healthcare provider, e.g. because the service is hosted on behalf of the healthcare provider. Currently a standard identification mechanism for non-healthcare service providers is yet to be defined. However, it is deemed necessary that SIL contains information to identify them somehow.
IR.07	SIL lookup information MUST include service provider interface.	To ensure that clients can use a discovered service. In the short term, WSDL interface references will be the norm. In the longer term, non-Web service interfaces may be feasible.
IR.08	SIL lookup information MUST include information to support secure message exchange through a Web service as per [CPIS2008].	There must at least be a placeholder for certificates to use with the associated service. In the absence of a NASH service there is no standard way for clients to obtain the certificate to use to encrypt a session key. A SIL can provide for this capability in the short term.
IR.09	SIL lookup information MUST include at least one reference to an X.509 certificate for the purpose of securing communications through an associated service.	Relates to IR.06. It states that the certificate to use with the associated service (whose public key component will be used to encrypt a session key: see [XSP2008]) must be present. It may be that a service provider is associated with more than one certificate, e.g. one for each DNS host name. In that case, the appropriate certificate reference would be required from the SIL.
IR.10	SIL MUST have an operation to determine if a given interaction pattern and associated service(s) is valid.	Relates to business requirements BR.11 and BR.12. Essentially, these support the ability to cache information returned by a SIL. When a service failure occurs there must be an operation to determine whether the relevant endpoint is still supported. If it is not, the client will have to perform a SIL lookup to discover the current endpoint (assuming the interaction is still supported). If the endpoint is valid, the problem will most likely be resolved in the near future and another invocation should then succeed.

2.2.2 Business Perspective

Business requirements relate to how the system can or will be used in deployment scenarios. They are mostly functional caveats with which design of the interface and realised instances must be compatible.

BR.01	Any SIL MUST be searchable by any healthcare provider in the e-health community.	Business analogue of IR.01, the primary reason for SIL.
BR.02	A SIL implementation MUST be capable of being associated with multiple HPIOs.	States that there can be multiple HPIOs associated with a single SIL, i.e. the relationship between SIL and HPI is one to many. See also IR.02.
BR.03	SIL MUST encompass a standard lookup interface.	Provides for consistency of search operations. It allows conformant client code to be reused.
BR.04	SIL MUST encompass a standard update interface to add document exchange interactions and associated service endpoints.	BR.04 and BR.05 provide for consistency of those update operations that allow healthcare providers to modify their own records. They are particularly important when the SIL implementation is hosted by a third party.
BR.05	SIL MUST encompass a standard update interface to remove document exchange interactions and associated service endpoints.	
BR.06	A HPIO entity associated with a SIL MUST be able to create records pertaining to its supported document exchange interactions.	BR.06 and BR.08 state that a SIL implementation must allow a healthcare provider to update the services it hosts or which are hosted on its behalf. To accomplish that, healthcare providers can use standard interfaces required by BR.04 and BR.05.
BR.07	SIL MUST be able to return alternative services for the same HPIO and document category.	
BR.08	A HPIO entity associated with a SIL MUST be able to remove records pertaining to its supported document exchange interactions.	Allows for more than one implementation of the same kind of service, i.e. same interaction pattern and document category. If a healthcare provider outsources a service and later decides to outsource to a different implementer or host the service in-house, there may be a transition period where both services are supported. Also, two third party organisations may compete for service invocations. One organisation may be preferred by client <i>A</i> and the other by client <i>B</i> . SIL design should not force providers into restrictive business practices.
BR.09	Existing implementations with SIL-like functionality MUST be able to co-exist with SIL.	Allows for the continuation of current organisational practice. Although IR.02 allows for a HPI to be associated with only one SIL, current service directories are not actually standard SILs. Information maintained by such services regarding

		HPI offered services must be reflected in the appropriate SIL. To accomplish this, it is anticipated that standard update facilities required by BR.04 and BR.05 can be used.
BR.10	SIL implementations MUST be able to be hosted on behalf of healthcare providers by third-party organisations.	Many healthcare providers will lack the technical resources to host the SIL with which they are associated. This requirement exists to specifically accept the out-sourcing of SIL implementations.
BR.11	SIL Clients SHOULD be able to cache information returned from a lookup operation.	It is assumed that clients will locally store information returned by a SIL lookup, to be reused when another document is to be transferred. This amounts to caching of remote references. There is no requirement for explicit timestamps since these values are necessarily fuzzy and lead to increased maintenance. When the information obtained by some prior SIL lookup can no longer be relied on, a failure will occur. Assuming the failure is because the service is no longer active (see IR.10) another SIL lookup is necessary.
BR.12	It MUST NOT be necessary to lookup a SIL prior to every attempt at document transfer.	Corollary of BR.11. If values can be cached it should not be necessary to always reaffirm those values. In any case, as with most directory-like services, the information is expected to be relatively static.
BR.13	SIL MUST support references to UHI/NASH certificates.	Requires that the design of SIL interfaces is sufficiently flexible to adopt references to future certificates issued by supported CAs.

2.2.2.1 Deployment Model

As can be inferred from the requirements above, in particular BR.02, it will be possible to deploy a SIL as a centralised service maintaining endpoints for every HPIO. At the other extreme it is also possible to deploy one SIL for every HPIO.

It is probable that a central SIL will be employed in the early stages following SIL specification. In the longer term, it is anticipated that SIL instances will be deployed by third party organisations on behalf of healthcare providers. Both central and distributed models are permitted by the requirements.

2.2.3 Technical Perspective

Technical requirements include technology choices and performance metrics and security requirements.

TR.01	SIL MUST be implemented as Web services as per [WSP2008].	In keeping with the NEHTA ethos. SIL services can be invoked cross platform and programming language.
TR.02	SIL implementations MUST NOT be dependent on the	It must be possible for SIL implementations to be developed before the NASH service is available. The

NASH specification.	primary problem will be that trust relationships cannot be standardised. Until the NASH is realised, it is anticipated that healthcare providers may use Medicare Australia PKI or perhaps temporary certificate issued by NEHTA.
TR.03 SIL implementations MUST NOT be dependent on the UHI specification.	It must be possible to construct SIL instances while work on the UHI continues. It is anticipated that the HPIO record will contain an attribute to resolve the SIL endpoint. Until this service is a reality, SIL endpoints will have to be "well-known", obtained via a special purpose, master SIL, published on a Web site, etc.
TR.04 SIL request and response messages MUST be signed and encrypted using WS-Security as specified by [WSP2008].	Incoming and outgoing messages are signed and encrypted for the purposes of authentication, message integrity and confidentiality.

2.2.3.1 Performance Metrics

At the time of writing no performance metrics have been identified.

Appendix A: References

- [CPIS2008] NEHTA, *Concepts and Patterns for Implementing Services, V2.0*, 1 December 2008.
- [NIF2007] NEHTA, *Interoperability Framework v2.0*, 17 August 2007.
- [SA2008] NEHTA, *SIL Architecture v1.1*, 1 December 2008.
- [WSP2008] NEHTA, *Web Services Profile v3.0*, 1 December 2008.
- [XSPP2008] NEHTA, *XML Secured Payload Profile v1.0*, 1 December 2008.