



E-Procurement Hub Service Operational Guidelines

Supply Chain

Version 1.0 – 12/07/2007

Final

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 © 2007, 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

Executive Summary	1
1 Introduction	2
1.1 Purpose	2
1.2 Document Context	2
1.3 Intended Audience	3
1.4 Scope.....	3
1.5 Sources of Guidelines	3
1.6 Limitations.....	3
1.7 Guideline Identification.....	4
1.8 Language Used to Describe Imperatives	4
1.9 Definition of Terms	4
2 Context.....	6
3 Performance Guidelines.....	7
3.1 Transaction Rates	7
3.2 Queuing Characteristics.....	8
4 Scalability Guidelines.....	9
4.1 General	9
5 Availability Guidelines	10
5.1 Availability Characteristics	10
5.2 Hours of Operation.....	11
5.3 Failover Characteristics.....	11
5.3.1 Unplanned Failover.....	11
5.3.2 Planned Failover	12
5.4 Disaster Recovery	12
6 Security Guidelines	13
6.1 Attribution	13
6.2 Access Control.....	13
6.3 Audit.....	13
Appendix A: References.....	14

This page has been left blank intentionally.

Executive Summary

This document is part of the technical perspective of the E-Procurement Architecture and it describes the operational guidelines for E-Procurement Hub Services.

This document is intended to form a checklist of capabilities that Hub Services should provide, and may be used as a foundation for the terms and conditions presented in Service Level Agreements or other arrangements and contracts used in rolling out the NEHTA E-Procurement solution.

The guidelines in this document are based on the E-Procurement Business Requirements and take into consideration the E-Procurement Technical Architecture.

The guidelines cover the following areas:

- An overview of the *Context* of the relationship of the E-Procurement Hub Service with other parties involved in health Supply Chain;
- *Scalability guidelines*, which covers the anticipated size of the system required to support some subset of national health e-procurement;
- *Performance guidelines*, which describe the required support for transaction rates and performance response times for some subset of national health e-procurement. This version of the document assumes the existence of several complimentary E-Procurement Hubs, each with the ability to forward messages via other hubs to the appropriate end party;
- *Availability guidelines*, which define guidelines such as the hours of operation and percentage of time available;
- *Security guidelines*, which outline guidelines over and above the security requirements imposed by the Secure Messaging Architecture for authentication, authorisation and access control.

1 Introduction

1.1 Purpose

This document describes the manner in which operation of an e-procurement hub should be monitored and governed. It should be read by hub service providers, and all parties that will use their services. It addresses the non-functional characteristics of the technical architecture for E-Procurement. It is complimentary to the functional specification of the service for E-Procurement given in the E-Procurement Technical Architecture [EPTA2007].

This document is intended to be used as input to terms and conditions of Service Level Agreements or other commercial arrangements between Hub service providers and their clients (the jurisdictions and their suppliers).

1.2 Document Context

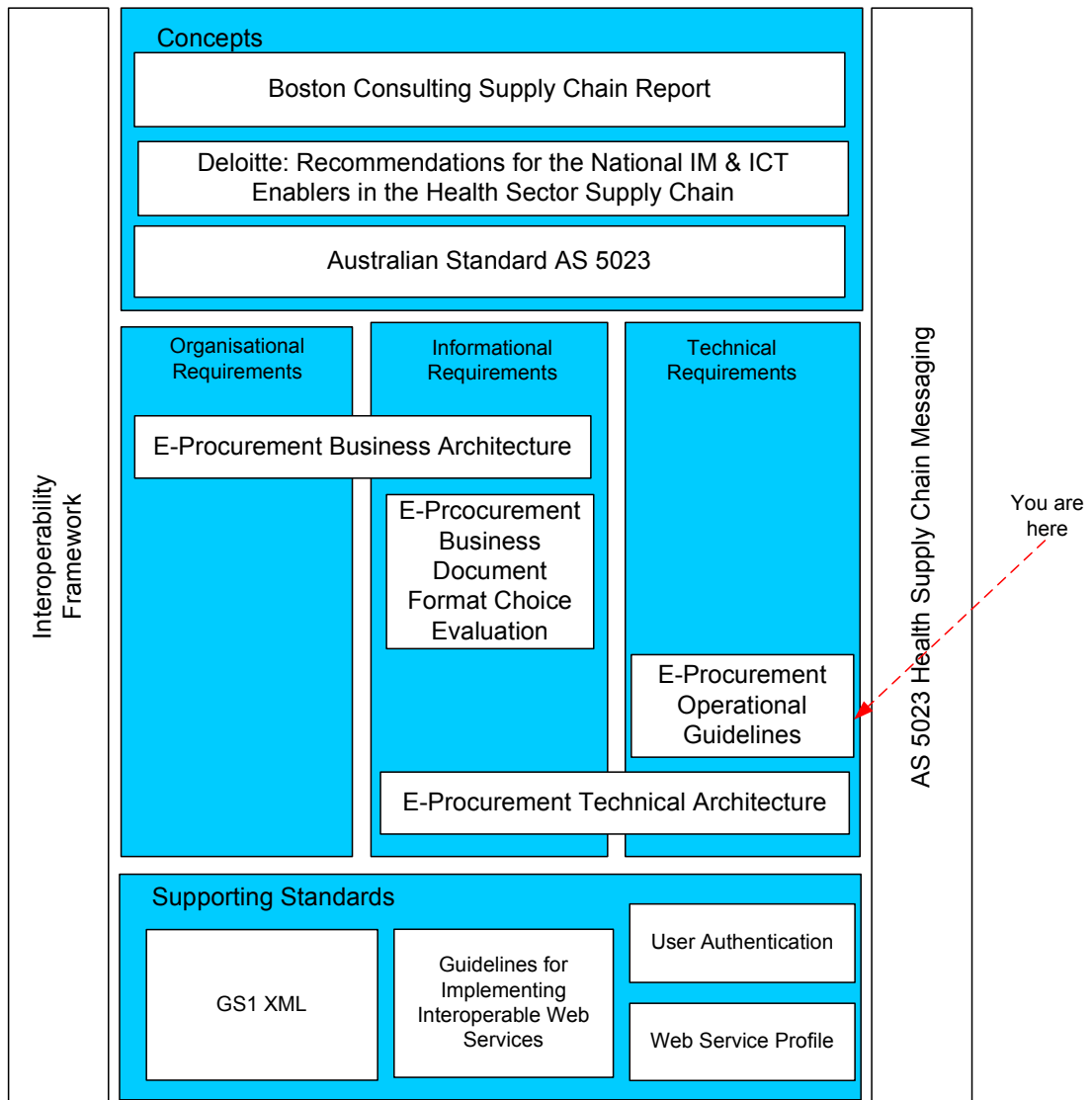


Figure 1: Document Roadmap

The documents shown in the middle block of Figure 1 make up the components of the NEHTA E-Procurement Solution. The AS 5023 standard [HSCM2004] underpins all of the technical documents.

1.3 Intended Audience

This document is intended for:

- Jurisdictional Representatives;
- Suppliers to the Jurisdictions;
- Hub Service Providers.

This document assumes the reader is familiar with the following documents:

- E-Procurement Business Architecture [EPBA2007]
- E-Procurement Technical Architecture [EPTA2007]

As the key focus of this document is operational considerations of e-procurement hub services, there are elements of the guidelines that are written for a technical audience.

1.4 Scope

This document is to provide operational guidelines for E-Procurement Hub Services. In addition, this document also provides guidance on expected behaviour of hubs for clients of E-Procurement Hubs.

This document is not intended to provide:

- Detailed system specifications. These will be provided by particular hubs when offering services to jurisdictions and suppliers.
- Operational guidelines for authentication and authorisation and access control services. These are provided in the *Web Services Standards Profile* [WSSP2006] and *Guidelines for Implementing Interoperable Web Services* [GIIWS2007] documents from the NEHTA Secure Messaging work, which underpin the technical architecture of the services that will be supported by hubs, as specified in [EPTA2007].
- Organisational and informational aspects of E-Procurement.

1.5 Sources of Guidelines

The key guidelines in this document have been drawn from a number of sources, including:

- E-Procurement Technical Architecture [EPTA2007]
- Contracts and Service Level Agreements provided by a number of Hub service providers.

In order to ensure that the guidelines are comprehensive, a number of other sources have been consulted. These include:

- HealthConnect Business Architecture Specification of Business Requirements, Version 1.9g Attachment

1.6 Limitations

The priority assigned to each guideline will be dependent on various governance and commercial arrangements between the hubs and their clients. Therefore this document does not assign priorities to guidelines. Aside from the Security Guidelines in Section 6, which express some mandatory requirements of Hub Services, the remainder of the guidelines only make recommendations.

1.7 Guideline Identification

The guidelines in this document are uniquely identified using the following format:

<Guideline category>.<guideline#>.<sub-guideline#>

Each of the guidelines comes from one of the following categories:

Guidelines Group	Title
AVL	Availability
PER	Performance
SCA	Scalability
SEC	Security

1.8 Language Used to Describe Imperatives

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

1.9 Definition of Terms

When the following terms are used in this document, they are used assuming the following document specific definitions:

Distributed	The dividing and spreading out of hardware and software, usually geographically, to avoid concentrating the system into a single unit. This is commonly desirable for availability and scalability purposes.
Failover	The automatic and transparent use of redundant hardware and/or software when a component fails, to ensure normal processing continues. Ideally, the users of the system will not become aware of the failure, that is they will perceive that the system is working normally.
Instance	A single physical occurrence of a system. The following are examples relevant to this document: <ul style="list-style-type: none"> – a distributed system is made up of multiple instances working together, or – the failure of one instance will trigger the failover to another instance to continue the processing.
Persistent	A property of data that guarantees it will be preserved. This property normally refers to the difference between data that has been saved to disk and data that is held in volatile memory. Data will be persistent after it has been saved, but before it is saved it can be lost if the computer crashes. An example relevant to this document is the persistence of auditing data access. The system needs to guarantee that if transmits or receives a business document then immediately crashes, that the audit trail will still contain a record of the transmission.
Redundant	Additional capacity (hardware or software resources) that is not used to satisfy normal system requirements. This capacity can be used in a failover situation to maintain system availability. An example relevant to this document is the need for redundant servers, networks and software instances such that the failure of any one will not stop buyers and sellers exchanging business documents.

Throughput The quantity of work processed by the system. An example relevant to this document is the number of event summaries being stored per day. This is distinct from the response of the system which is how fast each request is processed.

2 Context

As illustrated in Figure 2, the E-Procurement Hub Service sits between buyers and suppliers, with the ability to forward messages via other hubs to parties connected to those hubs.

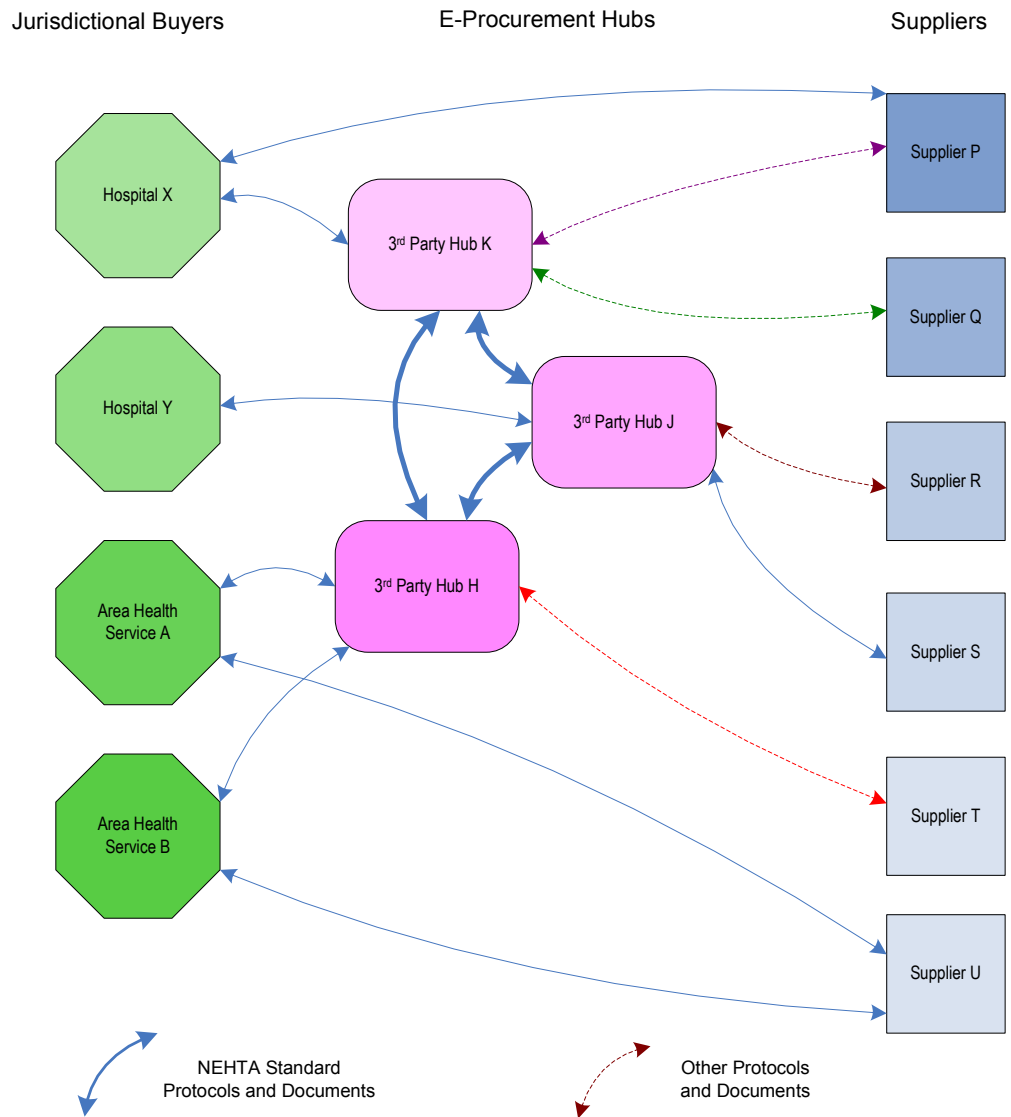


Figure 2: Architectural Context

3 Performance Guidelines

The guidelines in this section apply to the E-Procurement Hub Service(s).

3.1 Transaction Rates

PER.01.01 Each E-Procurement Hub Service SHOULD handle the normal and peak loads for Business Document transmission as well as meeting the response time targets.

PER.01.02 Each E-Procurement Hub Service SHOULD handle a sustained transaction rate. There are several different types of transactions that the E-Procurement Hub Service must handle. Each transaction type has the same response time and throughput targets, although a slower response is permitted for unusually large documents.

PER.01.03 Each E-Procurement Hub Service SHOULD handle a peak load over a specified window.

Peak loads will often occur at a known busy time but the E-Procurement Hub Service SHOULD handle the peak load at any time. During the window the normal guidelines for response time are relaxed. The window for handling a peak load is the amount of time the E-Procurement Hub Service SHOULD maintain the peak throughput and response times. If a peak period lasts longer than the peak window the E-Procurement Hub Service MAY further degrade.

PER.01.04 Each E-Procurement Hub Service SHOULD handle the following transaction response times for sustained throughput (off peak) and peak loads.

Transaction Type	Off-Peak Times (seconds)	Peak Times (seconds)	Assumed Peak Window
Time to receive document of less than 1Mb, translate if necessary, and make available for pickup by receiving party – 90% case	180	360	0.5 hours
Time to receive document of less than 1Mb, translate if necessary, and make available for pickup by receiving party – 10% case	600	600	0.5 hours
Time to receive document of between 1Mb and 10Mb, translate if necessary, and make available for pickup by receiving party – 90% case	300	600	0.5 hours

Time to receive document of between 1Mb and 10Mb, translate if necessary, and make available for pickup by receiving party – 10% case	600	900	0.5 hours
---	-----	-----	-----------

3.2 Queuing Characteristics

- PER.02.01** Each E-Procurement Hub Service SHOULD buffer and queue a set of business documents, as high availability of recipients for these documents is not assumed. A Hub accepting a business document is expected to store this document in multiply redundant storage until such time as the recipient is available to receive a copy.
- PER.02.02** Buyers MUST be provided with a capability by the hub to set per-Supplier non-receipt notification thresholds with a granularity of no less than 15 minutes.

4 Scalability Guidelines

The guidelines in this section apply to the E-Procurement Hub Service.

4.1 General

SCA.01.01 The E-Procurement Hub Service SHOULD scale in terms of:

- Throughput, and
- Response time

SCA.01.02 As the transaction load on the E-Procurement Hub Service increases, the throughput SHOULD increase. Otherwise the transactions will eventually become backlogged.

SCA.01.03 The E-Procurement Hub Service SHOULD maintain the response time targets (see section 3.1) as the load grows.

5 Availability Guidelines

The guidelines in this section apply to the E-Procurement Hub Service.

It is expected that once the E-Procurement Hub Services are in common use, their extended unavailability would cause material disruption to the provision of health care.

The E-Procurement Hub Service should maintain availability of core document transmission services. This does not mean that parts of the E-Procurement Hub Service cannot fail, it specifically means that the failure of the core services will not be noticed by the end user. From the perspective of the end users, the system will interact with them and function correctly. This generally involves an alternative component (usually with identical functionality) taking over from a component that, for any reason (bottlenecked or crashed), cannot service a user's request. This requires redundant capacity to be available.

5.1 Availability Characteristics

AVL.01.01 The E-Procurement Hub Service SHOULD deliver availability of the core business document transmission services for at least 98% of the time, excepting scheduled outages, over any monthly period. This equates to a combined total of 14.6 hours each month where Buyers *could* experience loss of service.

Availability percentage	98%
Total hours per month, other than scheduled outages, where users can experience loss of service	14.6 hrs/month
Maximum unavailability within 24 hours during week days ¹ – midnight Sun to midnight Fri (10% of month tot)	1.46 hrs (87.6 min)
Maximum continuous unavailability during business hours 9am-5pm Monday to Friday ² (3% of month tot)	26.28 min

It would be undesirable if the system was not available for use for a single continuous period of 14.6 hours in a month – especially if this overlapped significantly with a business day. Therefore there are limits to the total downtime during given periods, and continuous downtime during other periods. The total time unavailable in a 24 hour period from midnight Sunday to midnight Friday SHOULD NOT exceed 87.6 minutes (or 10% of the monthly total), excluding scheduled outages. It is best practice that scheduled outages will occur on Sundays.

¹ It is expected that scheduled outages may occur from time to time outside of business hours on weeknights.

² It is NOT expected that any scheduled outages will occur during business hours.

During business hours (9am to 5pm, weekdays, in the time zone of the Buyer), any one period of unavailability SHOULD be limited to 3% of the monthly total. This requires no more than 26.28 minutes of continuous unavailability during business hours. Any period of unavailability during business hours SHOULD be followed by at least one hour of availability.

- AVL.01.02** The availability target in **AVL.01.01** is for the core service of transmitting business documents, including:
- Accepting documents from Buyers and Sellers.
 - Translation of formats between those used by buyers and sellers (e.g. GS1 XML, and legacy EDI, or CSV files)
 - Forwarding of documents to their intended recipient, or to another hub.
- AVL.01.03** The availability target in **AVL.01.01** does not include:
- Uploading of consolidated transactions (or other non-core services)
 - Running and viewing reports
 - Administration and operation functions
- AVL.01.04** Disaster recovery is completely excluded from the availability target in **AVL.01.01**. See section 5.4 for the guidelines to address a disaster.

5.2 Hours of Operation

- AVL.02.01** The E-Procurement Hub Service SHOULD support business document delivery 24 hours of the day. However, it is expected that the bulk of transactions will occur during business hours. Therefore the capacity of the system may reduce outside those peak hours, and resources may be directed to other activities such as backups and maintenance.

5.3 Failover Characteristics

The guidelines in this section apply to the selected core services as specified in **AVL.01.02**.

- AVL.03.01** As far as practical, the E-Procurement Hub Service SHOULD ensure that unplanned failures are handled without the Hub's clients having to deal with the failure. This implies failing over to redundant services if the primary service fails.

5.3.1 Unplanned Failover

- AVL.03.02** The E-Procurement Hub Service SHOULD monitor and detect failures in components and automatically route requests to functioning components to maintain continuity of service.
- AVL.03.03** An unplanned failover SHOULD preserve business documents which have received positive technical acknowledgements³, and deliver these to their intended destinations, but it is not required to preserve user sessions. New requests for user

³ In the case of the E-Procurement Web Services specification, the correct return of a WS operation invocation without failure is considered to be a technical acknowledgement.

sessions SHOULD be processed to allow users to re-connect and continue working.

5.3.2 Planned Failover

AVL.03.04 The E-Procurement Hub Service SHOULD support planned failovers to allow for administration, and maintenance (including upgrades) of the system. Planned failovers allow components to be taken offline without causing any disruption to service. Planned Failover SHOULD be transparent to users.

5.4 Disaster Recovery

A disaster is a severe, infrequent and unexpected event that affects the availability of the E-Procurement Hub Service. Without appropriate disaster recovery planning, a disaster can easily cause the system to completely fail and recovery may take an unacceptably long period of time, or be impossible. It is impossible to protect against all possible events and a disaster recovery strategy based on a comprehensive risk assessment is best practice. This strategy would be used in the event of a catastrophic disaster.

AVL.04.01 A disaster recovery strategy SHOULD have been developed on the basis of a comprehensive risk assessment.

AVL.04.02 The distasted recovery strategy SHOULD be available for perusal by clients of an E-Procurement Hub Service.

6 Security Guidelines

These guidelines for security are in addition to those specified in the mandatory implementation framework for NEHTA recommended Web Services specifications given in the *Web Services Standards Profile* [WSSP2006], and the *Guidelines for Implementing Interoperable Web Services* [GIIWS2007].

6.1 Attribution

SEC.02.01 The E-Procurement Hub Service **MUST** attribute all transmissions and receptions of business documents to a single user or system, accurately and persistently. The E-Procurement Hub Service **MUST** retain the necessary attribution data that a user or system transmitted a document at a specific date and time.

For example, Northern Area Health Service sent a Purchase Order, or a Medicorp received a Purchase Order Change, or IntelliHub forwarded an Invoice to B2BAustralia.

SEC.02.02 The E-Procurement Hub **MUST NOT** transmit a document, or accept a document that cannot be attributed to a single user or system. This means that the Hub will be able to identify who is responsible for each document transmitted through its systems.

6.2 Access Control

SEC.03.01 The E-Procurement Hub Service **MUST** only allow access to authenticated users and systems.

SEC.03.02 The user attribution associated by an E-Procurement Hub Service to an organisation for administrative and other functions, and the access control policies afforded those users, is outside the scope of this specification.

6.3 Audit

SEC.04.01 The E-Procurement Hub Service **MUST NOT** process document transmission or administrative requests if for any reason a record of the access cannot be kept persistently.

Appendix A: References

- [BDFCHEP2007] NEHTA, *Business Document Format Choices for Health E-Procurement - A Final Evaluation*, 2007.
- [EDIFACT-UN] United Nations Economic Commission for Europe, 13 December 2006, *United Nations Directories for Electronic Data Interchange for Administration, Commerce and Transport*, accessed 28 June 2007, <<http://www.unece.org/trade/untdid/welcome.htm>>
- [EPBA2007] NEHTA, *E-Procurement Business Architecture*, Version 1.0, June 2007.
- [EPTA2007] NEHTA, *E-Procurement Technical Architecture*, Version 1.0, June 2007.
- [GIIWS2007] NEHTA, *Guidelines for Implementing Interoperable Web Services*, version 1.0, 2007.
- [GS1-XML] GS1, *GS1 XML – Technical*, accessed 28 June 2007, <<http://gs1.org/productssolutions/ecom/xml/technical/>>
- [HSCM2004] Standards Australia, Australian Standard 5023.[1-4], *Health Supply Chain Messaging*, 19 March 2004.
- [NIF2006] NEHTA, *Interoperability Framework*, 2006.
- [TAIS2006] NEHTA, *Technical Architecture for Implementing Services v1.0*, December 2006.
- [SBDH2004] UN/CEFACT, *UN/CEFACT Standard Business Document Header*, Technical Specification, Version 1.3, 4 June 2004.
- [SBDH2007] GS1, *Standard Business Document Header (SBDH)*, Version 1.0, Technical Implementation Guide, Draft 0.3, May 2007.
- [WSSP2006] NEHTA, *Web Services Standards Profile*, version 2.0, 2006.