



Message Integrity and Delivery Guidelines

Supply Chain – e-Procurement

Version 1.0 - 12/06/2008

Final

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.

Security

The content of this document is confidential. The information contained herein must only be used for the purpose for which it is supplied and must not be disclosed other than explicitly agreed in writing with NEHTA.

Copyright © 2006, 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 without the permission of NEHTA. All copies of this document must include the copyright and other information contained on this page.

Table of contents

1	Introduction	1
1.1	Purpose	1
1.2	Scope	1
2	Message Processing Stages	2
2.1	Stage Descriptions	3
3	Integrity and Validation Principles	5
3.1	Stage Details.....	6
3.1.1	Create	6
3.1.2	Prepare.....	6
3.1.3	Transmit	7
3.1.4	Decode	8
3.1.5	Process.....	8

This page has been left blank intentionally.

1 Introduction

1.1 Purpose

Retaining the integrity of the message is critical to e-Procurement as any compromise in integrity leads to the whole process being brought into question. Similarly, it is important that the message is received intact by the intended recipient. This guideline describes processes and activities that will assist in ensuring the integrity of the message, and steps to take if the integrity is compromised or the delivery process does not function correctly.

As part of that, it also describes the stages involved in e-Procurement messaging from initiation of the business document through to completion of processing by the receiver and how integrity will be retained throughout the process.

1.2 Scope

The Business Documents in scope are:

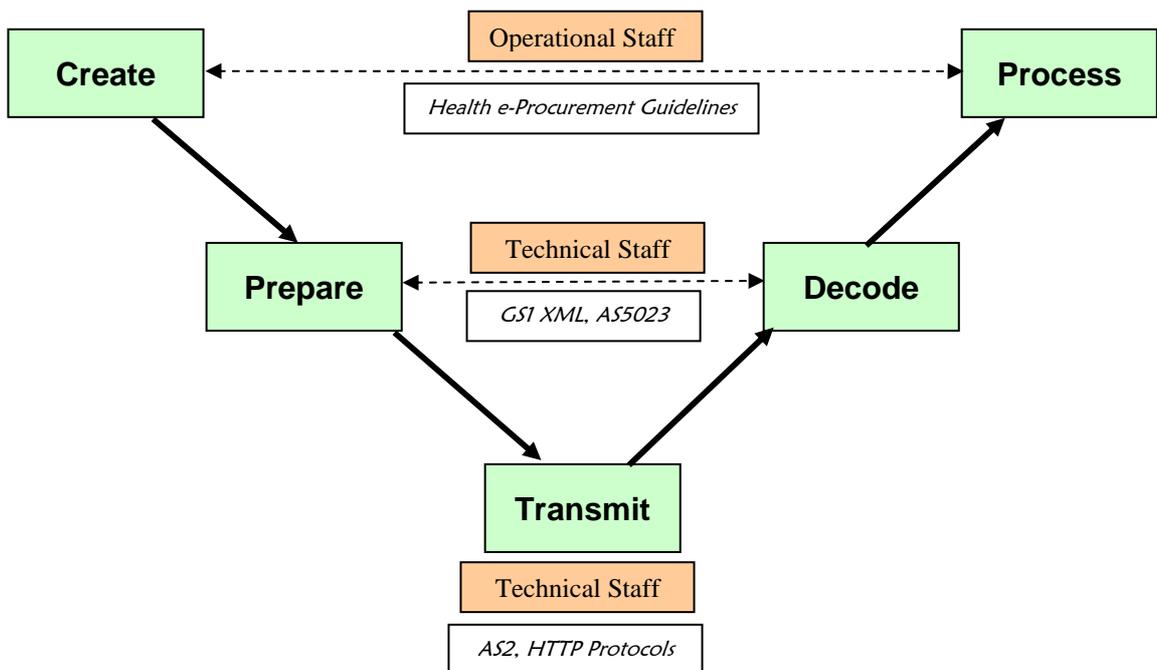
- Purchase Order
- Purchase Order Response
- Purchase Order Change
- Despatch Advice
- Invoice

2 Message Processing Stages

The message process goes through five stages, starting and finishing at an operational level with the technical levels in between, and can be understood by using a 'V' diagram.

The process starts with operational staff in the sending organisation creating the business document (Stage 1) according to the Health e-Procurement Guidelines¹ which is created by NEHTA in conjunction with the Health Jurisdictions. It finishes with the receiving organisation processing this document (Stage 5) by their operational staff according to the same guidelines.

The middle stage (Stage 3) is the Transmission of that document, which is managed by technical staff using AS2 and HTTP protocols; however the business document created in the Create stage must be converted into a standard format in order for the receiving organisation to correctly interpret it. This is the Preparation stage (Stage 2). It is managed by technical staff in the sending organisation according to GS1 XML and NEHTA standards. When the document reaches the receiving organisation, there is a corresponding process (Stage 4) to Decode the GS1 XML document into their local format to allow their operational staff to process the document.



¹ The Health e-Procurement Guidelines are a set of documents available for download from the NEHTA website.

2.1 Stage Descriptions

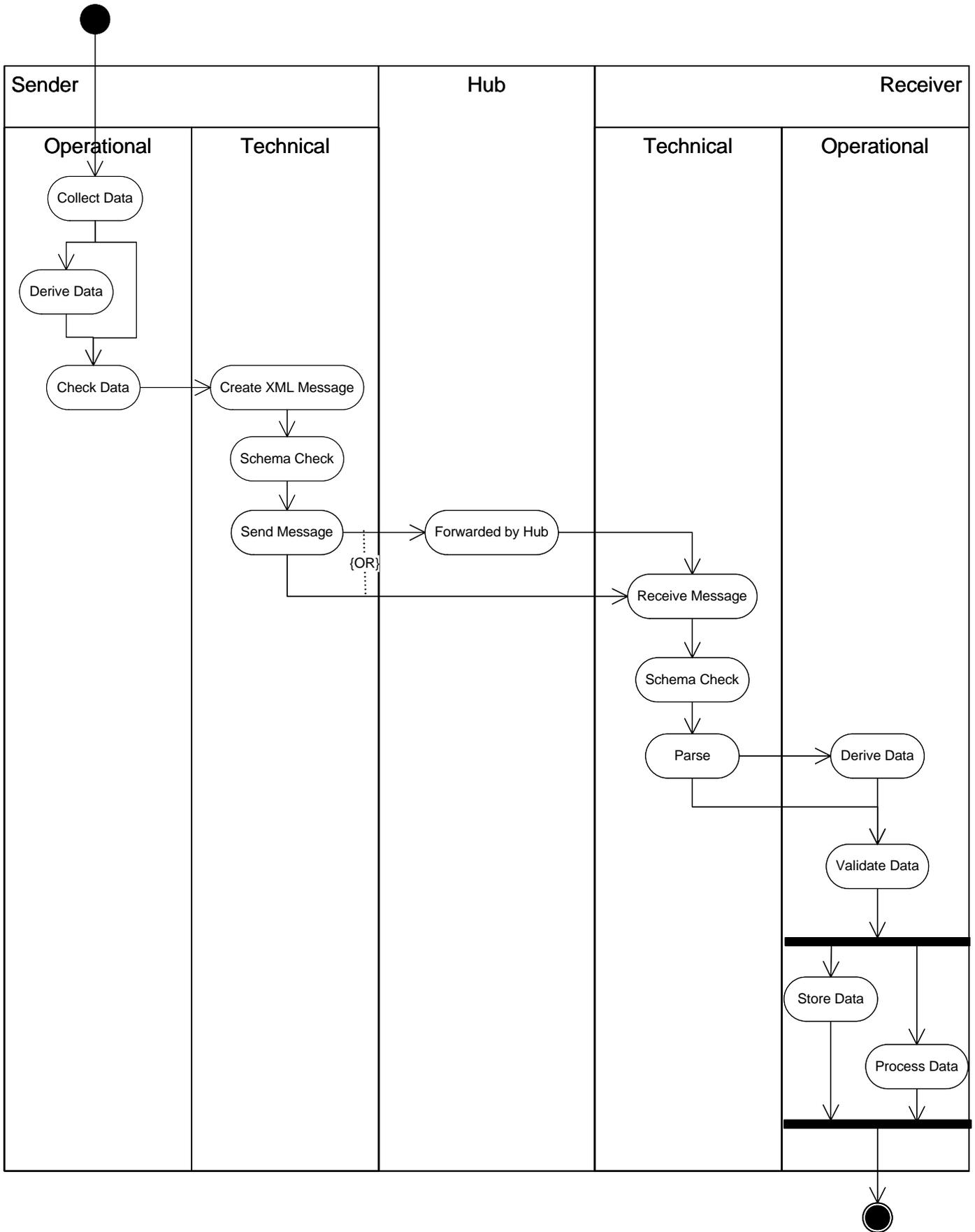
Each of the stages has a different activity required to retain integrity, and a different set of people responsible for integrity of the message. The following table list those details along with the key documents required for this process.

	<i>Stage Description</i>	<i>Validation Action</i>	<i>Responsible Party</i>	<i>Key Reference Documents</i>
1	Create Business Document	Ensure Business Rules are followed	Sender's Operational Staff	Health e-Procurement Guidelines
2	Prepare for Transmission	Ensure technical requirements are met	Sender's Technical Staff	GS1 XML, NEHTA standards
3	Transmit Business Document	Message transmission integrity	Sender's Technical Staff in conjunction with Hub Provider if used.	AS2 protocol
4	Decode Business Document	Ensure technical requirements are met	Receiver's Technical Staff	GS1 XML, NEHTA standards
5	Process Business Document	Ensure Business Rules are followed	Receiver's Operational Staff	Health e-Procurement Guidelines

Stages may overlap, particularly the first two and the last two. It is more important to consider the focus of and those responsible for each stage, rather than the timing of each stage. A good final solution will have a lot of integration and will be difficult to separate if viewed only from a timing perspective.

Each group may require assistance from any or all of the other groups; however the nominated group has the primary responsibility for integrity and validation.

The following diagram shows the messaging process from an Integrity and Delivery perspective. It shows the processes involved and those who are responsible for them.



3 Integrity and Validation Principles

The principles for validating messages and retaining integrity are:

1. *Error Prevention has priority over Error Detection and Correction*

Wherever possible, data that is known to be valid will be entered on behalf of the users rather than having them entering it manually. If this is not possible, then preference should be given to selecting values from pre-defined lists or in pre-defined formats. Free format fields should only be used where necessary.

If data is entered, it should be validated and, if required, corrected as soon as possible after entry.

2. *No message will leave the sender unless it has been fully validated and verifiably correct against both business and technical rules.*

The ultimate goal is to have 100% "Right First Time" as interrupting the process for any reason, including error correction, has a significant impact on efficiency. Therefore the principle here is to prove the data is correct before moving on to the next stage. The absence of error does not necessarily mean the data is correct.

3. *If the message is fully validated before sending, the only errors that can occur are due to either transmission errors (e.g. corruption, network down, expired certificates etc.) or a misalignment of data and/or rules between the two parties.*

Transmission errors will only occur in stage 3, and mechanisms to handle these are well established and should be utilised.

Once the system is setup, misalignment of data and/or rules should not occur if Change Control is implemented properly. Therefore Change Control over these elements is critical.

4. *If a technical issue occurs, it will be resolved without requiring the involvement of operational staff.*

Many of the business processes that create the business documents under discussion can not be easily repeated. For example, the PO document is created when the PO is approved, and a PO cannot be approved twice. For this reason, when the process enters Stage 2 - Prepare, copies of the data should be retained in enough detail and in a format that will allow the process to be restarted without going back to Stage 1 - Create. Unless required for Audit Trail purposes, this data is not required once it has been confirmed that the message has been correctly processed.

5. *Audit Trails will be retained in sufficient detail that will unambiguously describe all critical stages of the messaging process.*

Theoretically an Audit Trail is not required, however it is good insurance for those cases where the unexpected happens. The Audit Trail should have enough information for the process to be manually recreated should it be unexpectedly interrupted, or in dispute. There should be a minimum of one audit point at the end of each stage.

3.1 Stage Details

3.1.1 Create

In this stage the business document is initiated as a result of some external event. For example, a demand requirement could initiate a Purchase Order. Data is collected from the primary sources and checked against business rules. The business rules should ensure that the document meets all policy and procedural requirements, and that the data is complete and correct, and that the document conforms to the Health e-Procurement Guidelines.

Some data may need to be derived to meet the requirements of the party receiving the data. For example, the delivery point of a PO may be determined by the Cost Centre being charged for the order. Business rules need to cover these situations if they occur.

Although this process is managed and controlled by operational staff, it is expected that technical staff will be heavily involved in the mechanics of this process. Once the decision has been made as to what is valid and what is not, technical staff in most cases will implement system checks and routines to make sure the data meets these requirements. However technical staff will be working under the direction of the operational staff, and it is the responsibility of the operational staff to ensure the business document is valid.

Success Criteria: The document can be fully and correctly processed by the receiving organisation without needing any further activity from the sending organisation.

Reference Document: Health e-Procurement Guidelines

Responsibility: Designated Operations Officer

Preventative Action(s): A range of physical and IT procedures should be used as appropriate to the situation. These procedures should either prevent invalid data from being entered, or detect and correct the invalid data before it is processed.

Corrective Action(s): Refer to the responsible person. Corrective actions will be dependant on the nature of the error.

3.1.2 Prepare

This is the process of converting the business document into a GS1 XML message which is understood by all parties involved. At this stage, all data elements should be validated and the process is purely a translation into GS1 XML. This is purely a technical process and as such technical staff has the responsibility for its success.

This process involves both validating against the GS1 XML schema and ensuring that all data specified by operational staff is included in the message. It is possible for the XML document to be correctly validated against the schema, but not have data which meets the Health e-Procurement Guidelines. For example, the Business Scope Block is optional in the GS1 schema, but mandatory for Health e-Procurement.

At the start of this process, a copy of the data should be saved in case a restart is required. Data may also be saved at other critical points in the process. This data should be in a form that will allow it to be verified before restarting the process, and in a way that allows the process to be easily restarted. This data can be deleted once the message has been fully processed by the receiver.

Success Criteria: The XML document is successfully validated against GS1 XML schema, and meets NEHTA's standards.

Reference Documents: GS1 XML document suite
e-Procurement Technical Architecture (NEHTA)
Health e-Procurement Guidelines

Responsibility: Designated Technical Officer

Preventative Action(s): Validate XML document against GS1 XML schema and check against NEHTA technical rules.

Corrective Action(s): Remove the source of the error and restart the technical process using saved data.

Unless it is clear that the problem will be resolved within the timeframe of the Service Level Agreement, that officer shall also notify the Designated Operational Officer of the Sending Organisation who will review the transaction from a business impact perspective. The Operational Officer has the options of cancelling the transaction, completing it using alternative means, or requesting the Technical Officer to correct the problem and send the message.

3.1.3 Transmit

Once the message has been prepared, it will be transmitted using the AS2 protocol. It should be transmitted using the Secure Transmission Loop resulting in Non-Repudiation of Receipts as per GS1 guidelines. This requires the use of digital certificates, and the expiry of these certificates must be managed. A Change Control process must be used to manage the renewal of expired certificates so that all parties using them are kept in synchronisation.

Messages will be sent signed and encrypted. Receipts will be sent signed.

AS2 and HTTP error management routines will be used. Timeouts and retries will be agreed between all parties involved in the transmission. Responsibility for managing this process and resolving errors lies with the Technical Staff of the sending organisation. This responsibility can be delegated (but not abdicated) to the Hub Services Provider.

Success Criteria: The message will be sent and a valid Non-Repudiation Receipt received back.

Reference Document: RFC4130 and the documents that it references

Responsibility: Designated Technical Office of Sending Organisation

Preventative Action: Implement the AS2 protocol using signed and encrypted messages, and signed receipts. Manage Digital Certificates.

Corrective Actions: In all cases, the Designated Technical Officer shall be notified. Unless it is clear that the problem will be resolved within the timeframe of the Service Level Agreement, that officer shall also notify the Designated Operational Officer of the Sending Organisation who will review the transaction from a business impact perspective. The Operational Officer has the options of cancelling the transaction, completing it using alternative means, or requesting the Technical Officer to correct the problem and resend the message.

Expired Certificate: Generate a new certificate, synchronise with the receiving organisation, re-transmit using the new certificate, and then update all other receiving organisations.

Timeout: This includes timeout when sending a message and when waiting for the message receipt. Correct the problem or find an alternate mechanism, and re-transmit.

Corruption: Identify the source of the corruption, remove the source and re-transmit.

3.1.4 Decode

The decoding process commences after the AS2 process completes. This means that the message has been successfully decrypted and the contents of the message are valid from the sender's perspective. Any problems in the decoding stage must then be a result of mismatched schema. It is assumed that the decoding processes have been successfully implemented and there are no flaws in the processes themselves.

Success Criteria: A business document is created in the receiver's system which is ready for processing.

Reference Documents: GS1 XML document suite
e-Procurement Technical Architecture (NEHTA)
Health e-Procurement Guidelines

Responsibility: Designated Technical Officer

Preventative Action: Maintain accurate Change Control and synchronization over the GS1 XML schema. Retain a copy of the message as first received to facilitate reprocessing if an error occurs. This copy can be deleted when the message has been fully processed.

Corrective Action: Notify the Technical Officer at the sending organisation. Get the correct version of the schema and re-commence decoding. Unless it is clear that the problem will be resolved within the timeframe of the Service Level Agreement, that officer shall also notify the Designated Operational Officer of the Sending Organisation who will review the transaction from a business impact perspective. The Operational Officer has the options of cancelling the transaction, completing it using alternative means, or requesting the Technical Officer to correct the problem and continue decoding the message.

3.1.5 Process

Processing commences after decoding, and similarly to decoding by the time this stage is reached there should be no errors in the document. If there are, they are most likely due to misalignments between the sending and receiving organisations in the data and/or business rules.

Success Criteria: The business document is fully processed and, where required, an acknowledgment sent back to the sender.

Reference Document: Health e-Procurement Guidelines

Responsibility: Designated Operations Officer

Preventative Action: Maintain accurate Change Control and synchronization over the data and business rules. Retain a copy of the message as at the end of decoding to facilitate reprocessing if an error occurs. This copy can be deleted when the message has been fully processed.

Corrective Action: Notify the Operations Officer of the sending organisation unless it is clear that the problem will be resolved within the timeframes of the Service Level Agreement. The Sending Operations Officer will consult with the Receiving Operations Officer, and based on the impact to business will determine the best way to resolve the problem. If correcting the problem is the chosen course of action, the saved copy of the message can be used to restart the process once the problem has been resolved. If a manual workaround is chosen, then the automatic process must be managed so that the incomplete components do not cause any secondary problems.