Secure Message Delivery

Conformance Assessment Scheme

Version 3.2 — 29 April 2011

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.

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.

Table of contents

Table of contents iii

Document information iv

Executive Summary 1

1 Introduction 2
1.1 Document purpose 2
1.2 Intended audience 2
1.3 Contact details 2

2 Abbreviations and terminology 3

3 Requirements for SMD conformance 4
3.1 The approach to conformance testing 4
3.2 Organisations participating in conformance assessment 4
3.3 Test laboratory accreditation 5
3.4 Reference to technical specifications 5
3.5 Minimum conformance requirements 5
3.6 Objects of conformance assessment 6
3.7 Conformance with Healthcare Identifier specifications 6

4 Conformance assessment process 7
4.1 SMD conformance assessment 7
4.2 Implementation Conformance Statement 8
4.3 Conformance test specifications 9
4.4 Success criteria 10
4.5 Conformance test reporting 11
4.6 Declaring conformance 11

5 Ongoing validity of conformance 12
5.1 Conformance and versioning 12
5.2 Validity period 12

Appendix A : References 13

Document information

Revision history

Version	Date	Comments
1.0 draft	28/09/09	Initial draft for internal review.
1.1 draft	10/10/09	Draft incorporating CCA team comments.
1.2 draft	21/10/09	Second draft incorporating CCA team comments.
1.3 draft	02/11/09	Draft incorporating NEHTA review comments.
1.4 draft	09/11/09	PIP references have been deleted (to appear in a separate document).
1.5 draft	27/11/09	Terminology was updated for consistency with other publications.
1.6 draft	01/12/09	The sections on test software and test laboratories were updated.
1.7 draft	07/12/09	Various modifications resulting from an internal NEHTA review.
1.8 draft	13/01/10	References to ‘vendors’ changed to ‘developers’.
2.0 draft	12/02/10	References to specifications were updated to refer to the Standards Australia documents.
2.1 draft	19/03/10	The minimum conformance tests have now been absorbed into the test case specifications.
2.2 draft	11/05/10	Modifications from the PIP conformance subcommittee have been included.
2.3	29/06/10	Modifications made resulting from a PIP conformance subcommittee meeting.
3.0	02/11/10	Minor wording changes. Updated information about NATA accreditation. Included reference to the E-health Register.
3.1	11/11/10	Minor wording changes.
3.2	29/04/11	References were updated and sections were rearranged for readability.

Executive Summary

Standards Australia has published E-Health Secure Message Delivery (SMD) specifications that define a set of interfaces and associated application behaviour suitable for clinical messaging over the Internet. SMD may be implemented either as a direct extension to a medical software system or indirectly via a separate messaging system or service.

The objective of the SMD conformance assessment scheme and the associated test specifications is to define sufficient and consistent software testing for SMD implementations. With the number and diversity of systems that are expected to inter-connect in the national e-health market there is a significant risk that implementations will not interoperate unless they are assessed for conformance. Independent testing is prescribed to reduce the risk that implementations will not interoperate.

Therefore conformance assessment of SMD implementations is based on independent third-party testing by test laboratories accredited for testing conformance of implementations to the SMD specifications using the process described in this conformance assessment scheme.

Detailed conformance points for SMD implementations are listed in the specifications published by Standards Australia. The SMD specifications are built upon the foundation provided by those for the e-health web services profiles (WSP) and e-health XML secured payload profiles (XSP), published by Standards Australia.

The SMD conformance test specifications contain a set of conformance test cases derived directly from the conformance points defined in the SMD, WSP and XSP specifications. The conformance test specifications have both positive and negative functional test cases, to provide assurance of correct handling of wrong behaviour or wrong data.

The test cases are grouped by messaging role (e.g. sender, receiver); by test scenario and whether they pertain to a mandatory or optional conformance points in the SMD specifications. This provides a developer or test lab with a succinct view of what is required for conformance.

The common use by vendors and health jurisdictions of the SMD conformance test specifications and test process will ensure sufficiency and consistency of SMD conformance testing throughout the Australian medical software industry. This approach supports the goal of broad-based interoperability and security of messaging systems in the health sector.

1 Introduction

1.1 Document purpose

This document describes the scheme for assessing the conformance of e-health software to the Secure Message Delivery Australian Technical Specifications published by Standards Australia.

1.2 Intended audience

The intended audience includes:

- Vendors of e-health secure messaging products;
- Operators of e-health secure messaging services;
- Health jurisdictions, healthcare providers and systems integrators that implement software systems to the Secure Message Delivery specifications; and
- Software test laboratories.

A reference to ‘developers’ in this document should be interpreted as a reference to any organisation that develops a medical software system with secure messaging capability.

1.3 Contact details

Any comments or feedback should be sent to the NEHTA Compliance, Conformance and Accreditation unit: **cca@nehta.gov.au**.

2 Abbreviations and terminology

Conformance	Conformance is a measurement (by testing) of the adherence of an implementation to a specification or standard.
Conformance point	A conformance point is an item in the specification that may be supported by a developer's implementation.
Developer	An organisation that creates an implementation using secure message delivery specifications. A developer may be an organisation that develops a software product, or a provider of e-health services (e.g. a message broker). Health jurisdictions, healthcare providers and systems integrators may also develop secure messaging systems for healthcare. The conformance assessment process applies to all of these organisations.
ELS	Endpoint Location Service
ICS	Implementation Conformance Statement. This is provided by a developer and lists the conformance points that are supported by their implementation.
Implementation	A software system created by a developer to conform to a specification or standard.
NATA	National Association of Testing Authorities. NATA is Australia's national authority for accrediting test laboratories.
Object of assessment	An e-health system or service, or a component of an e-health system or service, which is assessed for conformance.
SMD	Secure Message Delivery
Test Summary Report	A Test Summary Report documents the results of tests performed by a test laboratory on behalf of a developer.
WSP	Web Services Profile
XSP	XML Secured Payload

3 Requirements for SMD conformance

Assessing the conformance of an SMD implementation is based on testing the conformance of the software to the technical specifications. Conformance testing may be performed manually or by using conformance test software to automate most of the process.

3.1 The approach to conformance testing

The SMD specifications were developed to meet the following goals:

- Any medical software system should be able to exchange messages with any other medical software system[1], even if both systems are developed by different vendors or health jurisdictions; and
- The contents of a clinical message should be secure as they are transmitted between healthcare providers.

SMD implementations will be provided by many vendors and health jurisdictions, and so the most significant risk to achieving these goals is that one implementation will not interoperate with one or more of the many other implementations due to differing interpretations of the specifications.

To mitigate this risk and achieve the goals of SMD:

- The conformance tests should be derived directly from the conformance points defined in the SMD technical specifications; and include both positive and negative functional test cases to provide assurance of correct handling of wrong behaviour or wrong data.
- Software conformance testing should be performed by accredited and independent third parties.

The objective of this approach to SMD conformance testing is to deliver a sufficient and consistent base for conformance, in support of broad-based interoperability and security of messaging systems in the health sector.

3.2 Organisations participating in conformance assessment

The types of organisations participating in SMD conformance assessment are listed in Table 3.1.

[1] SMD provides interoperability at the message transport level. Full interoperability will be achieved when medical software systems also share a common understanding of the contents of the message.

Organisation	Description
Developer	An organisation that creates an implementation using secure message delivery specifications. See section 2 for information about developers.
Test laboratory	An independent assessor of conformance to secure message delivery specifications. See section 3.3 for information about test laboratories.

Table 4.1: Organisations that participate in SMD conformance assessment

3.3 Test laboratory accreditation

A prerequisite for recognising conformance of an SMD implementation is that the independent assessment of conformance be performed by a test laboratory with the following accreditations issued by NATA (www.nata.asn.au):

1. General requirements for testing laboratories; and
2. Include specific accreditation for testing implementations for conformance to the SMD specifications using the process described in the SMD conformance assessment scheme (this document). This is subclass 22.40.01 of '22.40 Healthcare Tests'.

3.4 Reference to technical specifications

Detailed conformance points for SMD implementations are listed in the following specifications, plus any amendments:

1. E-Health Secure Message Delivery [SMD2010];
2. E-Health Web Services Profile [WSP2010]; and
3. E-Health XML Secured Payload Profiles [XSP2010].

3.5 Minimum conformance requirements

The Secure Message Delivery specifications [SMD2010] define conformance for four distinct messaging profiles - also called endpoints or roles:

1. Senders;
2. Receivers;
3. Sender intermediaries; and
4. Receiver intermediaries.

To conform to SMD specifications, an implementation must:

1. Implement the mandatory conformance points for at least one of these profiles;
2. Not implement any prohibited capabilities for the profiles; and
3. Implement any optional capabilities in a conformant manner.

The mandatory conformance points for SMD include mandatory conformance points for Web Services Profile (WSP) and XML Secured Payload Profiles (XSP). The implementation of any optional capability is not required for conformance.

3.6 Objects of conformance assessment

This conformance assessment scheme applies to the assessment of objects described in Table 4.1.

Object of Assessment	**Examples/Description**
Secure messaging capability	A secure messaging capability allowing medical information to be securely exchanged using the SMD specification. A secure messaging capability may be provided as a direct extension to a medical software system, or indirectly via a separate messaging system or service.

Table 4.1: Objects of conformance assessment

3.7 Conformance with Healthcare Identifier specifications

An implementation of SMD may access the Healthcare Identifier Service to find the address and certificate for an Endpoint Location Service that stores the web services endpoint location for the healthcare provider that is the recipient of a secure message. Such implementations are assessed for conformance to Healthcare Identifier requirements according to the process described in the Healthcare Identifiers Software Conformance Assessment Scheme [NEHTA2011a].

4 Conformance assessment process

This section describes the process for assessing the conformance of an implementation to SMD specifications.

4.1 SMD conformance assessment

SMD conformance assessment tasks are illustrated in Figure 4.1.

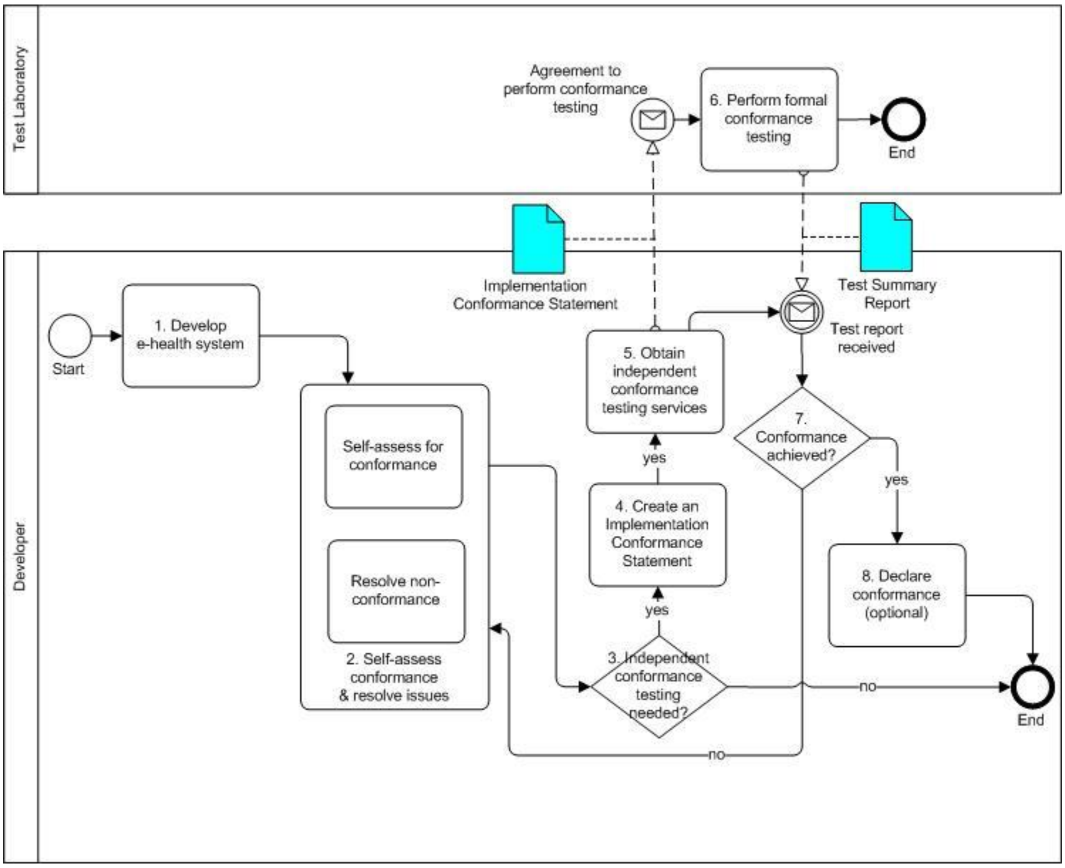
Test Laboratory
Agreement to perform conformance testing
6. Perform formal conformance testing
End
Implementation Conformance Statement
Test Summary Report
Developer
Start
1. Develop e-health system
Self-assess for conformance
Resolve non-conformance
2. Self-assess conformance & resolve issues
5. Obtain independent conformance testing services
yes
4. Create an Implementation Conformance Statement
yes
3. Independent conformance testing needed?
Test report received
7. Conformance achieved?
yes
8. Declare conformance (optional)
no
End
no

Figure 4.1: Conformance assessment process

SMD conformance testing tasks are described in Table 4.2, including decisions to determine if some of these tasks need to be performed.

	Process Item	Type	Description
1	Develop e-health system	Task	The developer creates, or modifies, a system to implement the SMD specifications.
2	Self-assess conformance & resolve issues	Task	Once an implementation has been created or modified to support SMD specifications, the developer may perform their own assessment of the implementation's conformance to these specifications. Conformance test documentation describes the tests to be applied (see section 4.3). Test software may be applied to efficiently perform the conformance tests.

3	Independent conformance testing needed?	Decision	The SMD implementation should be submitted to a test laboratory for an independent assessment of conformance, if any of the following is true: • The implementation has not previously been declared conformant; • A new version of the implementation has been created that affects the implementation's conformance to SMD (see section 5.1); • A previous version of the implementation has been declared conformant but the developer has subsequently enhanced the implementation to support additional SMD conformance points and wants to claim conformance for these; or • A new version of an SMD specification has been issued and the developer wants to claim conformance to this new version.
4	Create an Implementation Conformance Statement (optional)	Task	If the implementation supports optional conformance points the developer may create an Implementation Conformance Statement to indicate the conformance points that are supported (see section 4.2).
5	Obtain independent conformance testing services	Task	One or more organisations may be considered by the developer when choosing a test laboratory to independently test the conformance of the SMD implementation. The test laboratory must have the required accreditation (see section 3.3) to meet the prerequisites for declaring conformance (see section 4.6).
6	Perform formal conformance testing	Task	Formal conformance assessment is performed by the selected accredited test laboratory.
7	Conformance achieved?	Decision	The selected test laboratory will advise the developer whether their implementation conforms to SMD specifications.
9	Declare conformance (optional)	Task	When the developer's SMD implementation has passed conformance testing, the developer may optionally declare the conformance of their implementation (see section 4.6).

Table 4.2: SMD conformance assessment tasks and decisions

4.2 Implementation Conformance Statement

To test the conformance of a particular implementation, a statement of the capabilities and options that have been implemented may be needed. This is called an Implementation Conformance Statement (ICS).

An ICS:

- Enables a developer to precisely state the conformance points that are supported by a SMD implementation, and may be used in communications with a test laboratory and potential purchasers of an implementation; and
- May be used by an organisation wanting to procure an SMD implementation, to specify the features they require.

As the primary use of the ICS is to support the conformance test process, the SMD ICS only lists conformance points that are testable [NEHTA2010f].

Implementation Conformance Statements for WSP and XSP are not required.

An Implementation Conformance Statement proforma is available and may be used by developers. The developer is responsible for describing their implementation in the Implementation Conformance Statement.

The ICS is used as follows:

1. The developer may obtain an ICS proforma, along with instructions for completing the proforma;
2. The developer uses tables within the ICS to indicate which conformance points are supported by the implementation;
3. If formal conformance assessment is required, the developer may send the ICS to a test laboratory;
4. The test laboratory will only test those features that the developer includes in the ICS; and
5. The developer revises the ICS to only claim support for those conformance points that the test laboratory determines are supported by the implementation.

4.3 Conformance test specifications

The conformance test specifications provide details of tests performed when assessing conformance. Table 4.3 describes the documents within the set of conformance test specifications.

Conformance test document type	**Description**
Conformance test case specification	Test cases translate conformance points into concise, self-contained tests with a clear objective and criteria for passing. A test case is a set of inputs, execution conditions and expected results that have been developed to verify conformance to specifications. Conformance test case specifications identify one or more test cases for each conformance point. Test cases reference items in the proforma Implementation Conformance Statement, so that applicable test cases can be performed. For each conformance point, applying a subset of the full set of test cases for that conformance point may be sufficient to claim conformance. The set of 'mandatory' test cases is the minimum subset of test cases that must be applied to claim conformance. Selection of the minimum subset of test cases was based on an assessment of risk, impact and benefit. Conformance test specifications have been produced to support SMD conformance testing [NEHTA2011b].
Conformance test scenarios	The SMD conformance test scenarios provide a guide on how conformance test cases are to be applied when testing the conformance of health software to each of the four messaging roles. Conformance test scenarios identify which messaging roles and interaction types are in scope for testing. Each test scenario represents a main (expected) path the tests should follow, and also a number of alternative (unexpected) paths to provide test coverage of software behaviour for correct handling of errors and abnormal conditions. This has the advantage of delivering a structured approach to testing which enables more efficient development and quicker testing The following documents have been produced: 1. Conformance test scenarios for SMD receiver intermediaries [NEHTA2011c]; 2. Conformance test scenarios for SMD receivers [NEHTA2011d]; 3. Conformance test scenarios for SMD sender intermediaries [NEHTA2011e]; and 4. Conformance test scenarios for SMD senders [NEHTA2011f].

Table 4.3: SMD conformance test specifications

4.4 Success criteria

Criteria for successfully claiming conformance to the SMD specifications are:

1. The minimum conformance requirements stated in section 3.5 must be met;
2. A 100% pass rate is required for the tests listed in the set of 'minimum test cases' (section 4.3) for all mandatory conformance points for each profile (sender, receiver, sender intermediary and receiver intermediary) for which conformance is claimed; and

3. A 100% pass rate is required for all conformance tests for optional conformance points for which a developer wants to claim conformance.

4.5 Conformance test reporting

A conformance test summary report must be produced by the test laboratory and delivered to the developer. The conformance test summary report must include:

1. The name of the organisation and person that performed the conformance tests;
2. Details of the organisation's accreditation to perform SMD conformance testing;
3. The date on which the tests were performed;
4. The full suite of information required to identify the SMD implementation tested for conformance, including the name and version number;
5. The names and versions of the conformance test specifications and tools that were used to perform the tests;
6. Information about the computing environment used to perform the tests, such as the operating system name and version;
7. The result of executing each test case for each conformance point that the developer claims to have implemented; and
8. A statement indicating if the implementation meets the minimum conformance requirements for each of the SMD roles of Sender, Sender Intermediary, Receiver and Receiver Intermediary (section 3.5).

4.6 Declaring conformance

Prerequisites for declaring conformance of an SMD implementation are:

1. Conformance test success criteria must be met (section 4.4); and
2. Conformance testing must be performed by a test laboratory with the appropriate accreditation (section 3.3).

The developer may then declare the conformance of their implementation by requesting the inclusion of the implementation in the Australian eHealth Register of Conformity (the 'eHealth Register'). A developer wanting to declare conformance should contact NEHTA for information about submitting a declaration for inclusion on the eHealth Register.

5 Ongoing validity of conformance

5.1 Conformance and versioning

A developer may revise their implementation to create a new version, including:

- A major version, which may contain significant new functionality compared to the preceding version;
- A minor version, which may contain incremental additional functionality compared to the preceding version; and
- A maintenance version, which may correct one or more defects in a previously issued version.

Regardless of whether a new version is major, minor or a maintenance version, the new version should be submitted to an accredited test laboratory for formal conformance testing if there has been:

1. Explicit modifications to the SMD component(s) of an implementation; or
2. Modifications to a non-SMD component(s) of the implementation that may have an effect on the SMD component(s) of the implementation.

If neither condition applies, the developer may declare the conformance of their implementation but should state in their declaration the reasons why formal conformance testing was not required.

A developer may submit their implementation for formal conformance testing regardless of the scope of the revision.

5.2 Validity period

A declaration of conformance for a SMD implementation has no expiry date. The declaration only applies to the version of the implementation identified in the declaration of conformance.

Appendix A : References

This appendix lists specifications and other documents that provide information for or about this document. 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.

[ELS2010] Technical Report: Endpoint location service, TR 5823-2010, Standards Australia, 2010

[NEHTA2011a] Healthcare Identifiers Software Conformance Assessment Scheme, Version 2.2, NEHTA, 20 April 2011

[NEHTA2011b] Conformance Test Specifications for SMD (Functional Test Case Listing), version 1.11, NEHTA, April 2011.

[NEHTA2011c] Conformance Test Specifications for SMD (Receiver Intermediary Role), version 1.11, NEHTA, April 2011.

[NEHTA2011d] Conformance Test Specifications for SMD (Receiver Role), version 1.11, NEHTA, April 2011.

[NEHTA2011e] Conformance Test Specifications for SMD (Sender Intermediary Role), version 1.11, NEHTA, April 2011.

[NEHTA2011f] Conformance Test Specifications for SMD (Sender Role), version 1.11, NEHTA, April 2011.

[NEHTA2010f] Secure Message Delivery Implementation Conformance Statement Proforma, Version 0.2, NEHTA, 24 May 2010

[SMD2010] E-Health Secure Message Delivery, Australian Technical Specification 5822—2010, Standards Australia, 2010

[WSP2010] E-Health Web Services Profile Australian Technical Specification 5820—2010, Standards Australia, 2010

[XSP2010] E-Health XML Secured Payload Profiles Australian Technical Specification 5821—2010, Standards Australia, 2010