Australian Government
Australian Digital Health Agency

Secure Messaging
Release Note

6 March 2025 v2.1
Approved for external information
Document ID: DH-4113:2025

End product identifier: EP-4112:2025

Release rationale

This release of the Secure Messaging end product reflects the introduction of the:

- NSMN Declaration of Conformance
- NSMN Conformance Profile
- NSMN Conformance Assessment Scheme

The NSMN Declaration of Conformance is formal statement from software vendors affirming their system meets NSMN requirements. It outlines the legal obligations and steps for submitting a valid declaration, including executing a Vendor Deed Poll to ensure security, reliability, and interoperability.

The NSMN Conformance Profile defines the technical, security, and functional requirements for systems in the secure messaging network. It describes key roles (sending systems, receiving systems, core nodes) and sets standards for interoperability, security, and audit logging.

The NSMN Conformance Assessment Scheme outlines the process for evaluating system compliance with NSMN standards.

Package inclusions

New (to this end product)

Identifier	Name and version
DH-4110:2025	*NSMN Declaration of Conformance v1.0*
DH-4109:2025	*NSMN Conformance Assessment Scheme v1.0*
DH-4111:2025	*NSMN Conformance Profile v1.0*

Update (supersedes previous version)

Identifier	Name and version
DH-4113:2025	*Secure Messaging - Release Note v2.1 (this document)*

No change

Identifier	Name and version
DH-3568:2023	*National Secure Messaging Network - Blueprint v1.0 - current*
DH-3569:2023	*National Secure Messaging Network - Interoperability Specification v1.0 - current*
DH-3798:2023	*Secure Messaging - HL7 v2 MDM message for CDA package v2.5 - current*
DH-3799:2023	*Secure Messaging - Addressing Implementation Guide v1.1 - current*
NEHTA-1894:2011	*Secure Message Delivery - Conformance Test Specification v1.13 - current*
NEHTA-0637:2010	*Secure Message Delivery - Qualified Certificate Reference v1.2 - current*
NEHTA-0640:2010	*Secure Message Delivery - Qualified Identifiers v2.0 - current*
NEHTA-1000:2009	*Secure Message Delivery - Technical Overview v1.0 - current*
NEHTA-0999:2009	*Secure Message Delivery - Overview v1.0 - current*

Audience

This document is intended for:

- developers and implementers of clinical information systems
- developers and implementers of secure messaging systems

Support

For further support or to provide feedback, please email help@digitalhealth.gov.au

Previous releases

Version	Date	Version
2.0	23 August 2024	End Product: EP-3806:2023 Secure Messaging v2.0 **Release rationale** This release of the Secure Messaging end product reflects the introduction of the: • National Secure Messaging Network Blueprint; and • National Secure Messaging Network Interoperability Specification The Blueprint describes the key roles within the secure messaging national network and the capabilities required of each role, as well as providing examples of how specific implementations might fulfil those roles. The Interoperability Specification (IS) details the technical requirements that underpin the National Secure Messaging Network. The IS defines the requirements that each role must meet, and any solution constraints that must be adhered to when meeting those requirements.
1.1	3 March 2021	End Product: EP-3365:2021 Secure Messaging v1.1 **Release rationale** This release of the Secure Messaging end product reflects the following changes: • The introduction of FHIR provider directories as a replacement for Endpoint Location Services; and • The discontinuation of the Conformance Assessment Scheme for Secure Message Delivery HL7 Australia produced the Australian Provider Directory FHIR Implementation Guide which is available from https://build.fhir.org/ig/hl7au/au-fhir-pd/index.html. This release of the Secure Messaging end product provides guidance and clarity on how directory identifiers and secure message addressing interact. It also introduces the *Use of HL7 v2 MDM message for CDA package v2.4* to update and replace *Clarification on Messaging and CDA Packaging v1.4* from the *Clinical Documents v1.5.4* end product. This update describes how HL7 v2 addressing components are supported by the Australian Provider Directory FHIR Implementation Guide. The Conformance Assessment Scheme for Secure Message Delivery relies on NATA-accredited testing laboratories. No NATA-accredited testing laboratories continue to offer testing for Secure Message Delivery. For this reason, the Conformance Assessment Scheme is withdrawn, and the Agency will work with industry to develop a new scheme.

1.0.3	22 Oct 2014	End Product: EP-1880:2014 Secure Messaging v1.0.3 **Release rationale** Migration of website content The following documents were previously published on the eHealth Collaborate web site, and have now been moved to the NEHTA website: • Secure Message Delivery – Conformance Assessment Scheme: the process for assessing the conformance of health software that implements Standards Australia's 2010 Australian Technical Specifications ATS 5822 E-health secure message delivery, ATS 5821 E-health XML secured payload profiles, and ATS 5820 E-health web services profiles. • Secure Message Delivery – Conformance Test Specifications: test cases and test scenarios for secure message delivery. • Secure Message Delivery – Declaration of Conformity: for declaring conformance of health software to the secure message delivery Australian Technical Specifications. • Secure Message Delivery – Implementation Conformance Statement Proforma: for providing detailed information about conformance to the Australian Technical Specifications. • Secure Message Delivery – Test Summary Report Template: for use by the software test laboratories that are accredited to perform secure message delivery conformance tests. Note that the last three documents have had some minor editorial updates to the content, but no material changes. The conformance assessment scheme does not mandate the use of any specific test tools to automate the test cases; however secure messaging test tools are available from NEHTA that automate the tests cases for the mandatory requirements for each of

Version	Date	Version
		the four secure message delivery roles, as well as the test cases for immediate mode delivery.
1.0.2	24 Mar 2014	End Product: EP-1644:2014 Secure Messaging v1.0.2 **Release rationale** This release of the Secure Messaging end product removes the developer resource product components and related product data sheets. These have been republished in a new end product, Secure Messaging Integration Toolkit v1.0, available from the link below. http://www.nehta.gov.au/implementation-resources/ehealth-reference-platform/securemessaging-integration-toolkit The Secure Messaging Integration Toolkit contains libraries for B2B connectivity to Secure Message Delivery (SMD) and Endpoint Location Services (ELS), providing sample code for all operations, as well as a Medical Document Management (MDM) library to create the payload for SMD. This release also removes two product components, which are no longer relevant.
1.0.1	19 Dec 2013	End Product: EP-1566:2013 Secure Messaging v1.0.1 **Release rationale** This incremental release includes: • Two new product data sheets (Endpoint Location Service Client Library and Secure Message Delivery Client Library) • File name change to some of the Endpoint Location Service and Secure Message Delivery product components to group them logically in the product component list (no change to content of the files). These files are marked with an asterisk in the second table below.
1.0	28 Dec 2009	End Product: EP-0998:2009 Secure Messaging v1.0 **Release rationale** Initial release of Secure Messaging end product

Publication date: 6 March 2025

Australian Digital Health Agency ABN 84 425 496 912, Level 25, 175 Liverpool Street, Sydney, NSW 2000 digitalhealth.gov.au
Telephone 1300 901 001 or email help@digitalhealth.gov.au

Acknowledgements
The Australian Digital Health Agency is jointly funded by the Australian Government and all state and territory governments.