

Secure Messaging Integration Toolkit v1.2.1 Release Note

11 May 2016

Approved for external information

End product identifier: EP-2326:2016

Release rationale

Version 1.2.1 of the Secure Messaging Integration Toolkit provides an update to the *Secure Message Delivery B2B Client Library* (SMD Library) to accommodate a requirement introduced by a security patch for the .NET framework that was published by Microsoft on 8 March 2016.

This update addresses an issue that can affect both the transmission and reception of clinical documents via secure messaging.

Note: Some systems which do *not* use the SMD Library are also known to be affected. The changes implemented in this version of the SMD Library may be used as guidance for the developers of such systems.

The new .NET requirement has the potential to affect a large number of sites using Windows Vista, 7, 8.1, 10, 2008 or 2012 that have installed the Microsoft security patch published on 8 March 2016. More detailed information is available in the Affected Systems section below.

Issue details

The SMD Library uses functionality of the Microsoft .NET framework for the generation and verification of digital signatures.

The 8 March 2016 security update for the .NET framework introduced a mandatory requirement for signature identifiers to start with a letter ("NCName" syntax). This leads to a "malformed reference element" error for GUID-based identifiers starting with a digit. Identifiers starting with an alpha character, "a" to "f", are still recognised as valid identifiers.

The updated SMD Library prefixes the signature identifier with the sequence "Id_" to avoid triggering the .NET framework issue. For the extraction of SealedMessages that were generated with signature identifiers not conformant with the required syntax, the update now ignores the "malformed reference element" error and continues with the processing of the content of the SealedMessage.

The update does not include any other changes to the functionality of the SMD Library.

Implementation of the updated SMD library

Vendors are encouraged to ascertain the suitability of the amendment in the SMD Library prior to implementing it in their systems. This should include assessment of the following points:

- Does the software generate the "malformed reference element" error in either of the following scenarios on systems that have the .NET patch installed?
 - Create and digitally sign a Sealed Message;

- Validate a digital signature within a Sealed Message.
- Does the software use the most recent previous version 1.0.5 of the SMD Library?

For more information, please contact the NEHTA Help Centre at help@nehta.gov.au or phone 1300 901 001.

Affected systems

The table below details the type of systems that will be affected by this issue if they have installed the Microsoft security patch published on 8 March 2016.

Windows version	.NET 2.0	.NET 3.0	.NET 3.5 & 3.5.1	.NET 4.5.2	.NET 4.6 & 4.6.1
Windows 8.1, Windows RT 8.1, Windows Server 2012 R2			3135985 and 3135991	3135994	3135998
Windows Server 2012			3135989 and 3135984	3135995	3135997
Windows 7 SP 1, Windows Server 2008 R2 SP 1		3135988	3135983	3135996	3136000
Windows Vista SP 2, Windows Server 2008 SP 2	3135982	3135987		3135996	3136000
Windows 10			3140745	3140745	3140745
Windows 10 Version 1511			3140768	3140768	3140768

Details of the security patch are laid out in [Microsoft Security Bulletin MS16-035: Security Update for .NET Framework to Address Security Feature Bypass \(3141780\)](#).

Package inclusions

Updated (supersedes previous version)

Identifier	Name and version
NEHTA-2328:2016	<i>Secure Message Delivery B2B Client Library - .NET Sample Code v1.1.0</i>
NEHTA-2327:2016	<i>Secure Messaging Integration Toolkit - Release Note v1.2.1 (this document)</i>

Unchanged

Identifier	Name and version
NEHTA-1621:2014	<i>Endpoint Location Service B2B Client Library - Product Data Sheet v1.1</i>
NEHTA-1622:2012	<i>Endpoint Location Service B2B Client Library - .NET Sample Code v1.0.2</i>
NEHTA-1623:2012	<i>Endpoint Location Service B2B Client Library - Java Sample Code v1.0.0</i>

Identifier	Name and version
NEHTA-1627:2014	<i>HL7™¹ MDM Library - Product Data Sheet v1.1</i>
NEHTA-1625:2013	<i>HL7 MDM Library - .NET Sample Code v1.0.6</i>
NEHTA-1626:2013	<i>HL7 MDM Library - Java Sample Code v1.1.4</i>
NEHTA-1628:2014	<i>Secure Message Delivery B2B Client Library - Product Data Sheet v1.1</i>
NEHTA-1631:2012	<i>Secure Message Delivery B2B Client Library - Compiled WSDLs for Java v1.0.2</i>
NEHTA-1937:2014	<i>Secure Message Delivery B2B Client Library - Java Sample Code v1.0.3</i>
NEHTA-2208:2015	<i>Secure Messaging Conformance Test Tools – Software Package v1.0</i>
NEHTA-2030:2015	<i>Secure Messaging Conformance Test Tools – Product Data Sheet v1.0</i>

Audience

Software vendors

Known issues

None known

Support

For further support or to provide feedback, please email the NEHTA Help Centre at help@nehta.gov.au or phone 1300 901 001. Your views on the scope and usability of the Secure Messaging Integration Toolkit will inform future releases.

Future releases

The Secure Messaging Integration Toolkit will be released on an ad-hoc basis, based on providing new functionality or other changes as required.

¹ HL7 is a trademarks of Health Level Seven International and is registered with the United States Patent and Trademark Office.

Previous releases

Date	Version
17 Dec 2015	<p data-bbox="365 288 1145 315">EP-2207:2015 Secure Messaging Integration Toolkit v1.2</p> <p data-bbox="365 331 525 358">Release note</p> <p data-bbox="365 371 604 398">Release rationale</p> <p data-bbox="365 412 1445 468">This release includes the <i>Secure Messaging Conformance Test Tools – Software Package</i> and its product data sheet, which give further details of the software package.</p> <p data-bbox="365 483 751 510">The software package includes:</p> <ol data-bbox="365 526 1410 694" style="list-style-type: none"><li data-bbox="365 526 1410 622">1. Secure Messaging Test Harness, which automates the mandatory test cases for all four secure messaging roles (sender, receiver, sender intermediary and receiver intermediary), and also automates the test cases for immediate mode delivery.<li data-bbox="365 629 1386 694">2. Secure Message Delivery Agent (SMDA), which is an example implementation of secure messaging and includes an Endpoint Location Service (ELS). <p data-bbox="365 705 1326 761">The secure messaging conformance test tools support the Australian Technical Specification for Secure Message Delivery (ATS 5822-2010).</p> <p data-bbox="365 777 1410 837">Earlier versions of some of this content were previously available on the Test Interest Group (TIG) site.</p>
19 Dec 2014	<p data-bbox="365 869 1145 896">EP-1939:2014 Secure Messaging Integration Toolkit v1.1</p> <p data-bbox="365 911 525 938">Release note</p> <p data-bbox="365 952 604 978">Release rationale</p> <p data-bbox="365 992 1445 1048">The Java library has been updated and aligned with all other Java-based code to support up to Java version 7.2.1.</p> <p data-bbox="365 1064 722 1090">Updated product component:</p> <ul data-bbox="365 1104 1275 1131" style="list-style-type: none"><li data-bbox="365 1104 1275 1131">• Secure Message Delivery B2B Client Library - Java Sample Code v1.0.3
11 Mar 2014	<p data-bbox="365 1162 1145 1189">EP-1636:2014 Secure Messaging Integration Toolkit v1.0</p> <p data-bbox="365 1202 525 1229">Release note</p> <p data-bbox="365 1243 604 1270">Release rationale</p> <p data-bbox="365 1283 1230 1310">First release as new end product Secure Messaging Integration Toolkit.</p> <p data-bbox="365 1323 1422 1440">Note that the product components included in this release were previously released on nehta.gov.au as part of two end products (Common – Clinical Document and Secure Messaging). See release note for a mapping of the relevant product component identifiers.</p> <p data-bbox="365 1456 911 1482">Updated product components in this release.</p> <ul data-bbox="365 1496 1445 1673" style="list-style-type: none"><li data-bbox="365 1496 1378 1552">• NEHTA-1621:2014 Endpoint Location Service B2B Client Library - Product Data Sheet v1.1<li data-bbox="365 1565 1182 1592">• NEHTA-1627:2014 HL7 MDM Library - Product Data Sheet v1.1<li data-bbox="365 1606 1445 1673">• NEHTA-1628:2014 Secure Message Delivery B2B Client Library - Product Data Sheet v1.1

Document date: 11 May 2016

Contact for enquiries

Telephone: 1300 901 001 or email: help@nehta.gov.au

Disclaimer

The National E-Health Transition Authority Ltd (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.

Copyright © 2016 National E-Health Transition Authority Ltd

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.

Acknowledgement

The National E-Health Transition Authority is jointly funded by the Australian Government and all State and Territory Governments.