

Australian Technical Specification

E-health XML secured payload profiles



This Australian Technical Specification was prepared by Committee IT-014, Health Informatics. It was approved on behalf of the Council of Standards Australia on 22 February 2010.

This Technical Specification was published on 5 March 2010.

The following are represented on Committee IT-014:

- Australian and New Zealand College of Anaesthetists
 - Australian College of Health Informatics
 - Australian Industry Group
 - Australian Institute of Health & Welfare
 - Australian Institute of Radiography
 - Australian Private Hospitals Association
 - Central Queensland University
 - Commonwealth Department of Health and Ageing
 - Consumers' Federation of Australia
 - Consumers' Health Forum of Australia
 - CSIRO e-Health Research Centre
 - Department of Health Western Australia
 - Department of Human Services (Victoria)
 - Engineers Australia
 - Health Informatics Society of Australia
 - Health Information Management Association of Australia
 - HL7 Australia
 - Medical Software Industry Association
 - Medicare Australia
 - National E Health Transition Authority
 - NSW Health Department
 - Queensland Health
 - Royal Australian College of General Practitioners
 - Royal Australian College of Medical Administrators
 - Royal College of Nursing, Australia
 - Royal College of Pathologists of Australasia
 - The Royal Australian and New Zealand College of Radiologists
 - The University of Sydney
 - University of Western Sydney
-

Standards Australia wishes to acknowledge the participation of the expert individuals that contributed to the development of this Technical Specification through their representation on the Committee.

Keeping Standards up-to-date

Australian Standards® are living documents that reflect progress in science, technology and systems. To maintain their currency, all Standards are periodically reviewed, and new editions are published. Between editions, amendments may be issued.

Standards may also be withdrawn. It is important that readers assure themselves they are using a current Standard, which should include any amendments that may have been published since the Standard was published.

Detailed information about Australian Standards, drafts, amendments and new projects can be found by visiting www.standards.org.au

Standards Australia welcomes suggestions for improvements, and encourages readers to notify us immediately of any apparent inaccuracies or ambiguities. Contact us via email at mail@standards.org.au, or write to Standards Australia, GPO Box 476, Sydney, NSW 2001.

Australian Technical Specification

E-health XML secured payload profiles

First published as ATS 5821—2010.
Reissued incorporating Amendment No. 1 (November 2010).

COPYRIGHT

© Standards Australia Limited

All rights are reserved. No part of this work may be reproduced or copied in any form or by any means, electronic or mechanical, including photocopying, without the written permission of the publisher, unless otherwise permitted under the Copyright Act 1968.

Published by SAI Global Limited under licence from Standards Australia Limited, GPO Box 476, Sydney, NSW 2001, Australia

ISBN 978 0 7337 9423 0

PREFACE

This Technical Specification was prepared by the Standards Australia Committee IT-014, Health Informatics.

This Standard incorporates Amendment No. 1 (November 2010). The changes required by the Amendment are indicated in the text by a marginal bar and amendment number against the clause, note, table, figure or part thereof affected.

The objective of this Technical Specification is to define a common set of interoperable mechanisms for representing secured XML data for e-health. Security here refers to the use of digital signatures, cryptographic encryption, or a combination of them. This includes multiple levels of signing and multiple levels of encryption, if necessary.

Mechanisms for representing secured XML data have been defined by the World Wide Web Consortium (W3C) with XML Signature and XML Encryption. However, those specifications cover a broad range of situations, so they contain optional and implementation defined features.

This Technical Specification defines a profile of XML Signature and a profile of XML Encryption. It clarifies those optional and implementation defined features. This reduces the potential for those features from being used in an incompatible manner.

This Technical Specification also defines two XML elements for representing signed XML data and encrypted XML data. These can be used as common building blocks for exchanging data that needs to be secured.

The four profiles defined in this Technical Specification can be used whenever there is XML data what needs to be secured and represented as XML. For example, it can be used to define the contents of SOAP Web services messages or static XML documents.

A1

Funding for this publication has been provided by the Commonwealth Department of Health and Ageing. The Commonwealth makes no representation or warranty that the information in this publication is correct and accurate.

CONTENTS

	<i>Page</i>
SECTION 1 SCOPE AND GENERAL	
1.1 SCOPE AND INTENDED AUDIENCE.....	4
1.2 REFERENCED DOCUMENTS	5
1.3 OVERVIEW.....	6
1.4 DEFINITIONS	6
1.5 ACRONYMS.....	6
1.6 XML NAMESPACES	6
SECTION 2 SIGNED CONTAINER PROFILE	
2.1 INTRODUCTION	7
2.2 GENERAL	7
2.3 XML SCHEMA DEFINITION.....	7
SECTION 3 ENCRYPTED CONTAINER PROFILE	
3.1 INTRODUCTION	10
3.2 GENERAL	10
3.3 XML SCHEMA DEFINITION.....	10
SECTION 4 XML SIGNATURE PROFILE	
4.1 INTRODUCTION	14
4.2 GENERAL	14
4.3 SPECIFICATIONS.....	15
4.4 ds:Signature	17
4.5 ds:SignedInfo.....	17
4.6 ds:SignatureValue.....	21
4.7 ds:KeyInfo	21
4.8 ds:Object.....	22
SECTION 5 XML ENCRYPTION PROFILE	
5.1 INTRODUCTION	23
5.2 GENERAL	23
5.3 SPECIFICATIONS.....	24
5.4 xenc:EncryptedData.....	25
5.5 xenc:EncryptionMethod.....	26
5.6 ds:KeyInfo	26
5.7 xenc:CipherData	27
5.8 xenc:EncryptionProperties.....	28
5.9 xenc:EncryptedKey.....	28

This is a free preview. Purchase the entire publication at the link below:

ATS 5821 : 2010 : EN PDF

-
- ⊙ Looking for additional Standards? Visit SAI Global Infostore
 - ⊙ Learn about LexConnect, All Jurisdictions, Standards referenced in Australian legislation
-

Need to speak with a Customer Service Representative - Contact Us