AS 5551—2013

E-health XML secured payload profiles

This Australian Standard® was prepared by Committee IT-014, Health Informatics. It was approved on behalf of the Council of Standards Australia on 3 December 2013.
This Standard was published on 17 December 2013.

The following are represented on Committee IT-014:

- Aged Care Association Australia
- Allied Health Professions Australia
- Australasian College of Health Informatics
- Australian and New Zealand College of Anaesthetists
- Australian Association of Pathology Practices
- Australian College of Nursing
- Australian Commission on Safety and Quality in Healthcare
- Australian Healthcare and Hospital Association
- Australian Industry Group
- Australian Information Industry Association
- Australian Institute of Health and Welfare
- Australian Institute of Radiography
- Australian Medical Association
- Australian Private Hospitals Association
- Commonwealth Department of Health
- Consumers' Federation of Australia
- Consumers' Health Forum of Australia
- CSIRO e-Health Research Centre
- Department of Health (SA)
- Department of Health (Vic.)
- Department of Health (WA)
- Department of Human Services
- Edith Cowan University
- Engineers Australia
- GS1 Australia
- Health Informatics Society of Australia
- Health Information Management Association of Australia
- HL7 Australia
- Integrating the Healthcare Enterprise Australia
- Medical Software Industry Association
- National E-Health Transition Authority
- National ICT Australia
- NSW Ministry of Health
- Queensland Health
- Royal Australian College of Medical Administrators
- Royal College of Pathologists of Australasia
- Services for Australian Rural and Remote Allied Health
- The Pharmacy Guild of Australia
- The Royal Australian and New Zealand College of Radiologists
- The University of Sydney
- University of Western Sydney

Additional Interests:

- ACT Health
- Australian Healthcare Messaging Laboratory
- Buderim Gastroenterology Centre
- CAL2CAL Australia
- Casprel
- Deontik
- DH4
- Flinders University Northern Territory
- Global Health
- Global Informatic Health
- Health Communication Network
- Healthscope
- HL7 Systems and Services
- Kestral Computing
- Lantana Group
- Laughing Mind
- Llewelyn Grain Informatics
- MacIsaac Informatics
- Macquarie Health Corporation
- Medical Objects
- MediSecure
- Michael Legg and Associates
- Montage Systems
- Norman Disney and Young
- Ocean Informatics
- Oridashi
- Primary Healthcare
- Semantic Identity
- Smart Health Solutions
- Sullivan Nicolaides Pathology
- University of Wollongong
- Victoria Avenue Medical Centre

This Standard was issued in draft form for comment as DR AS 5551.

Standards Australia wishes to acknowledge the participation of the expert individuals that contributed to the development of this Standard through their representation on the Committee and through the public comment period.

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 Standard®

E-health XML secured payload profiles

Originally as ATS 5821—2010.
Revised and redesignated as AS 5551—2013.

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

ISBN 978 1 74342 640 1

PREFACE

This Standard was prepared by the Standards Australia Technical Committee IT-014, Health Informatics, to supersede ATS 5821—2010, *E-health XML secured payload profiles*.

This Standard is designed to be compatible with implementations of ATS 5821—2010. The XML namespaces are unchanged and there have only been minor corrections and clarifications to the conformance points and the XML Schemas. The changes are not expected to impact communications between implementations of ATS 5821—2010 and this Standard.

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

Mechanisms for representing secured XML 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 Standard defines four XML elements for representing secured XML fragments. One or more of these XML elements can be used whenever there are XML fragments to be secured and represented as XML. For example, these XML elements can be used to define the contents of SOAP Web services messages or static XML documents that contain secured XML fragments.

The XML elements are based on XML Signature and XML Encryption, clarifying the optional and implementation defined features defined therein. Two of the XML elements are strict profiles (i.e. subsets) of those specifications. The other two XML elements are new elements, which extend as well as incorporate a profile of those specifications.

This publication has been developed with assistance from the Australian Government Department of Health. The Australian Government makes no representation or warranty that the information in this publication is correct and accurate.

Standards Australia wishes to thank the Department of Health for its continued financial support in helping to develop this Australian Standard.

CONTENTS

Page

STANDARDS AUSTRALIA

Australian Standard
E-health XML secured payload profiles

SECTION 1 SCOPE AND GENERAL

1.1 SCOPE AND INTENDED AUDIENCE

1.1.1 Scope

This Standard defines mechanisms for representing signed XML fragments and encrypted XML fragments.

This Standard does not specify when these mechanisms are to be used—that is the responsibility of the organizations that use this Standard. Signing and encrypting are mechanisms for obtaining different security properties: authentication, integrity, confidentiality and non-repudiation. It is outside the scope of this Standard to determine the levels of security an application requires and whether these mechanisms are suitable for that application. Security also depends on a number of external factors, such as key management and policies, which are also outside the scope of this Standard.

This Standard contains conformance points that define the format of XML Secured Payloads. The format directly implies certain obligations for programs that create XML Secured Payloads or consume XML Secured Payloads, but explicitly defining those obligations is outside the scope of this Standard.

The mechanisms in this Standard are designed for data represented as XML fragments. If data is not an XML fragment, it will need to be converted to an XML fragment before it can be used with these profiles.

The mechanisms only cover situations where both the signature and the XML fragment being signed, or the encryption key and ciphertext, are represented together in the same XML document. Situations where they are represented separately are outside the scope of this Standard.

1.1.2 Intended audience

This Standard is intended for the following:

(a) Specification authors who create service interface specifications or software specifications. They will be able to use this Standard by referencing these mechanisms in their specifications and specifying conformance points for producing and consuming conformant and non-conformant artefacts.

(b) Software developers who create implementations of those specifications. The profiles chosen will depend on the interface or software specification being implemented. Software that produces the artefacts will usually implement code to create conformant profile artefacts; software that consumes the artefacts will usually implement code to process conformant profile artefacts and detect non-conformant profile artefacts. But there could be implementations that could exist to create non-conformant profile artefacts and to process them. They will be able to use this Standard for the definition of conformant artefacts, and the interface or software specification for the behaviour to be implemented.

NOTE: Developers will usually use existing toolkits or libraries for performing XML Encryption and XML Signature operations. They will not normally implement them from scratch.