



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.

Documents

Document Sharing Hub

Australian Standard[®]

E-health XML secured payload profiles

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

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 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

	<i>Page</i>
SECTION 1 SCOPE AND GENERAL	
1.1 SCOPE AND INTENDED AUDIENCE	4
1.2 OVERVIEW	5
1.3 REFERENCED DOCUMENTS	5
1.4 DEFINITIONS	6
1.5 ACRONYMS AND ABBREVIATIONS	6
1.6 XML NAMESPACES	7
SECTION 2 SIGNED CONTAINER	
2.1 INTRODUCTION	8
2.2 GENERAL	8
2.3 XML SCHEMA DEFINITION	8
SECTION 3 ENCRYPTED CONTAINER	
3.1 INTRODUCTION	12
3.2 GENERAL	12
3.3 XML SCHEMA DEFINITION	12
SECTION 4 XML SIGNATURE PROFILE	
4.1 INTRODUCTION	15
4.2 GENERAL	15
4.3 ds:Signature	16
4.4 ds:SignedInfo in ds:Signature	17
4.5 ds:SignatureValue in ds:Signature	22
4.6 ds:KeyInfo in ds:Signature and ds:X509Data in ds:KeyInfo	22
4.7 ds:Object in ds:Signature	23
SECTION 5 XML ENCRYPTION PROFILE	
5.1 INTRODUCTION	24
5.2 GENERAL	24
5.3 xenc:EncryptedData	25
5.4 xenc:EncryptionMethod in xenc:EncryptedData	26
5.5 ds:KeyInfo in xenc:EncryptedData	27
5.6 xenc:CipherData in xenc:EncryptedData	28
5.7 xenc:EncryptionProperties in xenc:EncryptedData	28
5.8 xenc:EncryptedKey and related elements	29

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 keys 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.

- (c) Testers who check an implementation for conformance to those interface or software specifications. They will use this Standard for the definition of conformant artefacts and the interface or software specification for the behaviour to be tested.

The reader is expected to have detailed knowledge of XML, XML Encryption, XML Signature and Public Key Infrastructure (PKI).

1.2 OVERVIEW

This Standard defines the following four mechanisms:

- (a) Signed Container (Section 2).
- (b) Encrypted Container (Section 3).
- (c) XML Signature Profile (Section 4).
- (d) XML Encryption Profile (Section 5).

1.3 REFERENCED DOCUMENTS

The following documents are referred to in this Standard.

AS 5550	E-health web services profiles
ACSI33	Defence Signals Directorate, Australian Government Information and Communications Technology Security Manual, ACSI 33, 19 September 2005.
EXC2002	W3C, Exclusive XML Canonicalization, Version 1.0, W3C Recommendation, 18 July 2002. http://www.w3.org/TR/2002/REC-xml-exc-c14n-20020718/
FIPS197	FIPS, Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, 26 November 2001.
MCIN2005	Michael McIntosh and Paula Austel, XML Signature Element Wrapping Attacks and Countermeasures, IBM Research Report, RC23691 (W0508 064), 9 August 2005.
PKCS-1993	RSA, PKCS #1: RSA Encryption Standard, Version 1.5, RSA Laboratories Technical Note, 1 November 1993.
RFC3986	IETF, RFC 3986 Uniform Resource Identifier (URI): Generic Syntax, T. Berners-Lee, R. Fielding, L. Masinter, January 2005.
XENC2002	W3C, XML Encryption Syntax and Processing, W3C Recommendation, 10 December 2002. http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/
XEXSD2002	W3C, XML Encryption Syntax and Processing, W3C Recommendation XML Schema, 10 December 2002. http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/xenc-schema.xsd
XML2008	W3C, Extensible Markup Language (XML) 1.0 (Fifth Edition), W3C Recommendation, 26 November 2008. http://www.w3.org/TR/2008/REC-xml-20081126
XSBP2009	W3C, XML Signature Best Practices, W3C Working Draft, 30 July 2009. http://www.w3.org/TR/xmlsig-bestpractices

XSD2004a	W3C, XML Schema Part 1: Structures, Second Edition, W3C Recommendation, 28 October 2004. http://www.w3.org/TR/2004/REC-xmlschema-1-20041028/
XSD2004b	W3C, XML Schema Part 2: Datatypes, Second Edition, W3C Recommendation, 28 October 2004. http://www.w3.org/TR/2004/REC-xmlschema-2-20041028/
XSSP2002	W3C, XML Signature Syntax and Processing, W3C Recommendation, 12 February 2002. http://www.w3.org/TR/2002/REC-xmlsig-core-20020212/xmlsig-core-schema.xsd

1.4 DEFINITIONS

For the purpose of this Standard, the definitions below apply.

1.4.1 Conformance point

A provision or possible action against which the conformance of a system can be attested. A requirement, indicated by the use of the word ‘shall’, is mandatory for compliance with this Standard [or Technical Specification]. A recommendation, indicated by the word ‘should’, provides best practice solutions that are not mandatory.

1.4.2 Payload

The data being secured. It is the data that is being signed or encrypted.

1.4.3 Profile

Identifies a set of specifications and how they are to be used.

1.4.4 Shall

Indicates that a statement is mandatory.

1.4.5 Should

Indicates a recommendation.

1.4.6 XML fragment

A region (consecutive sequence of characters) of an XML document that matches element production number [39] in XML2008. Informally this means the start tag, end tag, and contents of the element.

1.5 ACRONYMS AND ABBREVIATIONS

AES	Advanced Encryption Standard
DES	Data Encryption Standard
IETF	Internet Engineering Task Force
PKI	Public Key Infrastructure
RFC	Request For Comments
SHA	Secure Hash Algorithm
SKI	Subject Key Identifier
XML	Extensible Markup Language

1.6 XML NAMESPACES

In this Standard the following namespace prefixes are used to refer to these XML namespaces:

ds	http://www.w3.org/2000/09/xmldsig#
ep	http://ns.electronichealth.net.au/xsp/xsd/EncryptedPayload/2010
sp	http://ns.electronichealth.net.au/xsp/xsd/SignedPayload/2010
xenc	http://www.w3.org/2001/04/xmlenc#

SECTION 2 SIGNED CONTAINER

2.1 INTRODUCTION

The Signed Container is an XML element that represents an XML fragment that is digitally signed using the XML Signature Profile (Section 4). It supplements the XML Signature Profile by defining an XML element to represent the XML fragment as well as one or more signatures on that XML fragment. This Signed Container can be used when integrity or attestation of the XML fragment is required.

2.2 GENERAL

This Section defines the `sp:signedPayload` element. This element can be used to represent XML fragments and one or more signatures on those XML fragments. The element is defined using the XML Schema definition language [XSD2004a] [XSD2004b].

The payload data can be any XML fragment as defined by Clause 1.4.6. Since the signed container is represented as an XML element, it is possible to nest a signed container inside another signed container to achieve particular security properties. The way the signed container is used will need to be defined by the specification that makes use of the signed container.

The `sp:signedPayload` element can either be used to define an XML fragment inside a larger XML document, or it can be used as the root element of an XML document.

2.3 XML SCHEMA DEFINITION

2.3.1 General

The Signed Payload is a container for holding an XML fragment and one or more digital signatures on the XML fragment.

2.3.2 Signed Payload

2.3.2.1 Conformance points

The following conformance points apply:

- (a) An XML element that conforms to a signed container shall be an `sp:signedPayload` element that is valid against the Signed Payload XML Schema complex type shown in XML Schema 1.
- (b) The `id` attribute on the `ds:signedPayloadData` element shall be set to a value unique to all attributes with the XML Schema datatype of `ID` in the XML document containing the signed container.
- (c) Every `ds:Signature` element in the signed container shall conform with the XML Signature Profile which is defined in Section 4.
- (d) Every `ds:Signature` element in the signed container shall contain exactly one `dsig:Reference` element.
- (e) Every `dsig:Reference` element in the signed container shall have its `URI` attribute set to the value of a hash followed by the value of the `id` attribute on the `sp:signedPayloadData` element in the same signed container.

2.3.2.2 XML Schema 1

```
<?xml version="1.0"?>

<xsd:schema
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  targetNamespace=
    "http://ns.electronichealth.net.au/xsp/xsd/SignedPayload/2010"
  xmlns:tns=
    "http://ns.electronichealth.net.au/xsp/xsd/SignedPayload/2010"
  xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
  elementFormDefault="qualified">

  <xsd:import
    namespace="http://www.w3.org/2000/09/xmldsig#"
    schemaLocation=
      "http://www.w3.org/TR/xmldsig-core/xmldsig-core-schema.xsd"/>

  <xsd:complexType name="SignedPayloadDataType">
    <xsd:sequence>
      <xsd:any processContents="lax" minOccurs="1" maxOccurs="1"/>
    </xsd:sequence>
    <xsd:attribute name="id" type="xsd:ID" use="required"/>
  </xsd:complexType>

  <xsd:complexType name="SignatureListType">
    <xsd:sequence>
      <xsd:element ref="ds:Signature"
        minOccurs="1" maxOccurs="unbounded"/>
    </xsd:sequence>
  </xsd:complexType>

  <xsd:complexType name="SignedPayloadType">
    <xsd:sequence>
      <xsd:element name="signatures" type="tns:SignatureListType"
        minOccurs="1" maxOccurs="1"/>
    </xsd:sequence>
    <xsd:element name="signedPayloadData"
      type="tns:SignedPayloadDataType" minOccurs="1" maxOccurs="1"/>
  </xsd:complexType>

  <xsd:element name="signedPayload" type="tns:SignedPayloadType"/>

</xsd:schema>
```

2.3.2.3 Informative notes

This XML Schema is available for download from <http://ns.electronichealth.net.au>.

This XML Schema defines the `sp:signedPayload` element as the `sp:SignedPayloadType` complex type, which contains the `sp:signedPayloadData` element and the `sp:signatures` element.

The `sp:signedPayloadData` element contains the XML fragment that is to be signed. The `xsd:any` element within the `sp:signedPayloadData` element is a placeholder for the XML fragment. The `id` attribute on the `sp:signedPayloadData` element is used to hold a value that is used by XML Signature as a reference to the data that has been signed.

Conformance point 2.3.2.1(b) requires the `id` attribute's value to be unique in the scope of the XML document. This is a consequence of its datatype being `xsd:ID`. This datatype is defined in Section 3.3.8 of XSD2004b and its validity constraint is defined in Section 3.3.1 of XML2008.

The signer signs the `sp:signedPayloadData` element using their private key to create a digital signature, which is represented by a `ds:Signature` element. This `ds:Signature` element is added to the `sp:signatures` element.

The receiver retrieves the `ds:Signature` element within the `sp:signatures` element and verifies the digital signature using the public key of the signer.

The `sp:signatures` element can contain one or more signatures of the `sp:signedPayloadData` element. This allows the payload to be signed by multiple private keys. Each signer creates a digital signature and adds it to the `sp:signatures` element. The corresponding public key is used to check each signature. With this profile, the certificate (which contains the public key) is included with the signatures, but it is recommended that the checker validates that certificate before trusting it. The checker could also use a certificate obtained by another mechanism to check the signature.

Specifications that use this signed payload container need to define how many signatures are expected, whether a receiver needs to verify all or a subset of the expected signatures, how the identity of the signer is to be established and how the trust of individual certificates is established.

The contents of the `ds:signedPayloadData` are defined as an `xsd:any` with 'lax' contents processing. The behaviour of 'lax' when there are `xsi:type` declarations in the XML is not clearly defined in XML Schema, so different XML implementations might handle them differently.

NOTE: The XML Signature Profile (Section 4) allows one or more references to be present in a signature (allowing one signature to sign multiple XML fragments). However, this signed payload container restricts that to only one reference (and that reference can only reference the `sp:signedPayloadData` element).