INTERNATIONAL STANDARD

ISO/IEC 24824-3

First edition
2008-05-01

Information technology — Generic applications of ASN.1: Fast infoset security

Technologies de l'information — Applications génériques de l'ASN.1: Sécurité d'Infoset rapide

Reference number
ISO/IEC 24824-3:2008(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

CONTENTS

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 24824-3 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 6, *Telecommunications and information exchange between systems*, in collaboration with ITU-T. The identical text is published as ITU-T Rec. X.893 (05/07).

Introduction

This Recommendation | International Standard specifies:

a) the application of integrity to one or more parts of an XML infoset using Fast Infoset serialization and W3C XML Signature;

b) the application of encryption to one or more parts of an XML infoset using Fast Infoset serialization and W3C XML Encryption.

W3C XML Signature specifies a means of generating W3C XML Signature information items that contain (*inter alia*):

a) explicit (using URIs) or implicit (dependent on the use of the XML infoset signature information item) identification of one or more data objects (a data object is anything that either already is, or can be transformed into, a string of octets);

b) a (possibly empty) list of sequential transforms (specified by URIs for the algorithm to be used in performing the transform) from those data objects to a sequence of octets; these transforms can select all or part of the identified data objects, but are required to result in a sequence of octets;

c) digest and encryption information for the production of a signature of the resulting sequence of octets; and

d) the resulting signature.

This Recommendation | International Standard specifies four (canonical Fast Infoset) algorithms that can be referenced in a W3C XML Signature transform (and provides URIs for them) and can also be (independently) used as the algorithm for the W3C XML Signature canonicalization method.

NOTE 1 – The same Fast Infoset algorithm could be used for both the transform and the canonicalization method, but use of two different Fast Infoset algorithms (or a Fast Infoset algorithm and some other algorithm) is not excluded.

In all four cases, the input to the canonical Fast Infoset algorithm is either an XML infoset, or an XPath node set (restricted, in accordance with 6.1.4 b, to those node sets that produce a well-formed XML document when serialized).

The output of all four canonical Fast Infoset algorithms is a sequence of octets (the octets of a fast infoset document, see ITU-T Rec. X.891 | ISO/IEC 24824-1) that are suitable for digest and hashing in order to provide a signature in accordance with W3C XML Signature.

NOTE 2 – This will usually be the last transform in the sequential list of W3C XML Signature transforms, but need not be.

A typical use will be to sign one or more parts of a single XML infoset.

NOTE 3 – Use to sign parts of multiple XML infosets is not excluded.

It is expected, but not required, that the resulting W3C XML Signature information items will be used either as a detached signature, or as an enveloping or enveloped signature (see W3C XML Signature) for the XML infoset that is signed, and that the resulting XML infoset will be serialized using ITU-T Rec. X.891 | ISO/IEC 24824-1.

This Recommendation | International Standard specifies application-level extensions (see 3.2.1) to W3C XML Encryption. These application-level extensions enable encryption to be applied to part of an XML infoset using octets provided by a Fast Infoset serialization, rather than to the octets provided by an XML serialization of those parts.

NOTE 4 – W3C XML Encryption can be applied to a complete fast infoset document as specified in W3C XML Encryption, 3.1, without the use of this Recommendation | International Standard. The **MimeType** attribute will have the value **"application/fastinfoset"**.

The means of identifying the parts of the XML infoset that are encrypted is specified by W3C XML Encryption and allows the encryption of:

a) an element information item and its properties, including any direct or indirect child information items (and their properties); and

b) the child information items of the child property of an element information item and their properties, including any direct or indirect child information items (and their properties).

Encryption requires that those parts of an XML infoset that are to be encrypted have to be first serialized into a string of octets for input to an encryption algorithm.

The ability to produce a serialization of a and b above is not supported by ITU-T Rec. X.891 | ISO/IEC 24824-1, but is specified in clause 8 of ITU-T Rec. X.893 | ISO/IEC 24824-3 (using ITU-T Rec. X.891 | ISO/IEC 24824-1). This is done by converting such fragments (in a defined way) to a complete XML infoset and then applying ITU-T Rec. X.891 | ISO/IEC 24824-1 to the complete XML infoset.

This Recommendation | International Standard also specifies two URIs, one for a above and one for b above, that are used in XML Encryption to identify the application-level extensions which determine the use of Fast Infoset serialization rather than XML serialization for the production of the octets to be input to an encryption algorithm.

Use of Fast Infoset serialization to determine the octets for input to an encryption algorithm in general reduces the number of octets that have to be encrypted and decrypted, and would be normal (but not necessary) if the XML infoset is transferred using a Fast Infoset serialization.

NOTE 5 – It is also possible (but would be unusual) to use Fast Infoset serialization to determine the octets for input to an encryption algorithm when the XML infoset is to be transferred using an XML serialization.

The serialization of an XML infoset containing W3C XML Signature information items and/or W3C XML Encryption information items to a fast infoset document has the following advantages over serialization to an XML document:

a) repeating information such as multiple signed references or multiple encrypted parts with the same XML tags or content will be encoded more efficiently; and

b) the (binary) octets associated with signature values, digest values, cipher values or keys may be encoded directly (see ITU-T Rec. X.891 | ISO/IEC 24824-1, 10.3) if a (binary) fast infoset document is used to serialize the XML infoset; when serializing an XML infoset to an XML document (which is a string of characters), such octets are required to be base64 encoded, increasing processing speed and size.

Clause 6 specifies four canonical Fast Infoset algorithms that can be referenced in a W3C XML Signature transform.

Clause 7 specifies the use of W3C XML Signature with canonical Fast Infoset algorithms.

Clause 8 specifies the use of W3C XML Encryption for the encryption of parts of an XML infoset that are serialized to fast infoset documents.

Annex A does not form an integral part of this Recommendation | International Standard and provides examples of signing and validating a SOAP XML infoset (that makes use of canonical Fast Infoset algorithms), and encrypting and decrypting a SOAP message infoset (that makes use of the encryption of part of the SOAP message infoset that is serialized to a fast infoset document).

Annexes B and C do not form an integral part this Recommendation | International Standard, and provide examples of a signed SOAP message infoset and a signed and encrypted SOAP message infoset, respectively.

INTERNATIONAL STANDARD
ITU-T RECOMMENDATION

Information technology – Generic applications of ASN.1: Fast infoset security

1 Scope

This Recommendation | International Standard specifies four (canonical Fast Infoset) algorithms that can be used in the application of W3C XML Signature (and provides URIs for them).

It also specifies application-level extensions to the W3C XML Encryption processing rules for the encryption of part of an XML infoset (see 8.1) serialized as a fast infoset document and for the decryption of an encrypted part (see 8.3) that was serialized as a fast infoset document.

The use of any resulting W3C XML Signature information items or W3C XML Encryption information items is not within the scope of this Recommendation | International Standard.

2 Normative references

The following Recommendations and International Standards contain provisions which, through reference in this text, constitute provisions of this Recommendation | International Standard. At the time of publication, the editions indicated were valid. All Recommendations and Standards are subject to revision, and parties to agreements based on this Recommendation | International Standard are encouraged to investigate the possibility of applying the most recent edition of the Recommendations and Standards listed below. Members of IEC and ISO maintain registers of currently valid International Standards. The Telecommunication Standardization Bureau of the ITU maintains a list of currently valid ITU-T Recommendations. The IETF maintains a list of RFCs, together with those that have been obsoleted by later RFCs. The reference to a document within this Recommendation | International Standard does not give it, as a stand-alone document, the status of a Recommendation or International Standard.

2.1 Identical Recommendations | International Standards

– ITU-T Recommendation X.891 (2005) | ISO/IEC 24824-1:2007, *Information technology – Generic applications of ASN.1: Fast infoset*.

2.2 Additional references

– ISO/IEC 10646:2003, *Information technology – Universal Multiple-Octet Coded Character Set (UCS)*.

– W3C Canonical XML:2001, *W3C Canonical XML Version 1.0, W3C Recommendation, Copyright © [15 March 2001] World Wide Web Consortium, (Massachusetts Institute of Technology, Institut National de Recherche en Informatique et en Automatique, Keio University), http://www.w3.org/TR/2001/REC-xml-c14n-20010315*.

– W3C XML Encryption:2002, *XML Encryption Syntax and Processing, W3C Recommendation, Copyright © [10 December 2002] World Wide Web Consortium (Massachusetts Institute of Technology, Institut National de Recherche en Informatique et en Automatique, Keio University), http://www.w3.org/TR/2002/REC-xmlenc-core-20021210*.

– W3C Exclusive Canonical XML:2002, *W3C Exclusive XML Canonicalization Version 1.0, W3C Recommendation, Copyright © [18 July 2002] World Wide Web Consortium, (Massachusetts Institute of Technology, Institut National de Recherche en Informatique et en Automatique, Keio University), http://www.w3.org/TR/2002/REC-xml-exc-c14n-20020718.*

– W3C XML Information Set:2004, *XML Information Set (Second Edition), W3C Recommendation, Copyright © [04 February 2004] World Wide Web Consortium (Massachusetts Institute of Technology, Institut National de Recherche en Informatique et en Automatique, Keio University), http://www.w3.org/TR/2004/REC-xml-infoset-20040204.*

– W3C XML Signature:2002, *XML-Signature Syntax and Processing, W3C Recommendation, Copyright © [12 February 2002] World Wide Web Consortium (Massachusetts Institute of Technology, Institut National de Recherche en Informatique et en Automatique, Keio University), http://www.w3.org/TR/2002/REC-xmldsig-core-20020212*.

– W3C XPath:1999, *XML Path Language (XPath) Version 1.0, W3C Recommendation, Copyright © [16 November 1999] World Wide Web Consortium (Massachusetts Institute of Technology, Institut National de Recherche en Informatique et en Automatique, Keio University), http://www.w3.org/TR/1999/REC-xpath-19991116.*