

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.893

(05/2007)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

OSI applications – Generic applications of ASN.1

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

ITU-T Recommendation X.893



International
Telecommunication
Union

Document Sharing Hub

ITU-T X-SERIES RECOMMENDATIONS
DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	
Services and facilities	X.1–X.19
Interfaces	X.20–X.49
Transmission, signalling and switching	X.50–X.89
Network aspects	X.90–X.149
Maintenance	X.150–X.179
Administrative arrangements	X.180–X.199
OPEN SYSTEMS INTERCONNECTION	
Model and notation	X.200–X.209
Service definitions	X.210–X.219
Connection-mode protocol specifications	X.220–X.229
Connectionless-mode protocol specifications	X.230–X.239
PICS proformas	X.240–X.259
Protocol Identification	X.260–X.269
Security Protocols	X.270–X.279
Layer Managed Objects	X.280–X.289
Conformance testing	X.290–X.299
INTERWORKING BETWEEN NETWORKS	
General	X.300–X.349
Satellite data transmission systems	X.350–X.369
IP-based networks	X.370–X.379
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	
Networking	X.600–X.629
Efficiency	X.630–X.639
Quality of service	X.640–X.649
Naming, Addressing and Registration	X.650–X.679
Abstract Syntax Notation One (ASN.1)	X.680–X.699
OSI MANAGEMENT	
Systems Management framework and architecture	X.700–X.709
Management Communication Service and Protocol	X.710–X.719
Structure of Management Information	X.720–X.729
Management functions and ODMA functions	X.730–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	
Commitment, Concurrency and Recovery	X.850–X.859
Transaction processing	X.860–X.879
Remote operations	X.880–X.889
Generic applications of ASN.1	X.890–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
TELECOMMUNICATION SECURITY	X.1000–

For further details, please refer to the list of ITU-T Recommendations.

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

Summary

ITU-T Rec. X.893 | ISO/IEC 24824-3 specifies the application of encryption and integrity (either separately or in combination) to a fragment of an XML infoset that is serialized using the Fast Infoset specification in ITU-T Rec. X.891 | ISO/IEC 24824-1. The specification of encryption uses the W3C Recommendation *XML Encryption Syntax and Processing*. The specification of integrity uses the W3C Recommendations *W3C Canonical XML Version 1.0*, *W3C Exclusive XML Canonicalization Version 1.0* and *XML-Signature Syntax and Processing*.

Source

ITU-T Recommendation X.893 was approved on 29 May 2007 by ITU-T Study Group 17 (2005-2008) under the ITU-T Recommendation A.8 procedure. An identical text is also published as ISO/IEC 24824-3.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications. The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure e.g. interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at <http://www.itu.int/ITU-T/ipr/>.

© ITU 2008

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

CONTENTS

		<i>Page</i>
1	Scope	1
2	Normative references	1
2.1	Identical Recommendations International Standards	1
2.2	Additional references	1
3	Definitions	2
3.1	Imported definitions	2
3.2	Additional definitions	2
4	Abbreviations	2
5	Notation	2
6	Canonical Fast Infoset algorithms	3
6.1	Requirements on canonical Fast Infoset algorithms	3
6.2	Requirements on canonical XML algorithms for use by a canonical Fast Infoset algorithm.....	3
6.3	Restrictions when serializing an XML infoset to a canonical fast infoset document	3
6.4	Canonical Fast Infoset algorithms.....	4
7	W3C XML Signature and Fast Infoset	4
8	W3C XML Encryption and Fast Infoset	5
8.1	Application-level extensions for encryption.....	5
8.2	Generation of a complete XML infoset from part of an XML infoset.....	5
8.3	Application-level extensions for decryption.....	6
Annex A	Examples of signing and encrypting an XML infoset.....	7
A.1	Introduction of examples	7
A.2	Signing and verifying the SOAP message infoset	7
A.3	Encrypting and decrypting the SOAP message infoset.....	10
Annex B	Signed SOAP message infoset.....	12
Annex C	Signed and encrypted SOAP message infoset	13
Bibliography		14

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.

