
**Electronic business eXtensible
Markup Language (ebXML) —
Part 1:
Messaging service core specification**

iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

ISO 15000-1:2021

<https://standards.iteh.ai/catalog/standards/iso/06014f15-0458-466e-a490-5b131210a28f/iso-15000-1-2021>



iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

ISO 15000-1:2021

<https://standards.iteh.ai/catalog/standards/iso/06014f15-0458-466e-a490-5b131210a28f/iso-15000-1-2021>



COPYRIGHT PROTECTED DOCUMENT

© ISO 2021

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Foreword	vii
Introduction	ix
1. Scope	1
2. Normative references	1
3. Terms and definitions	3
4. Relevant messaging concepts.....	6
4.1. Web services and their role in an eBusiness messaging framework.....	6
4.2. Caveats and assumptions.....	7
4.3. XML notation.....	7
4.4. Namespace prefixes	7
4.5. Example domains	8
5. Messaging model	8
5.1. Model components	8
5.1.1. Components of the model.....	8
5.1.2. Messaging roles.....	9
5.1.3. Abstract messaging operations	10
5.2. Message exchange patterns	10
5.2.1. Rationale.....	10
5.2.2. General definition.....	11
5.2.3. MEP bindings.....	11
5.2.4. Relationship to SOAP MEPs.....	13
5.2.5. The One-Way/Push MEP.....	13
5.2.6. The One-Way/Pull MEP	14
5.2.7. The Two-Way/Sync MEP.....	15
5.2.8. Other transport-channel-bound MEPs.....	16
6. Message pulling and partitioning	17
6.1. Objectives.....	17
6.2. Supporting message pulling	17
6.3. Combining pulling with security and reliability.....	19
6.4. Message partition channels	20
6.4.1. Concept and purpose	20
6.4.2. Some use cases	22
6.4.3. Definition and usage requirements.....	23
7. Processing modes	24
7.1. General	24
7.2. Messaging service processing model	25
7.3. Processing mode features.....	26
7.4. Default features for processing mode	27

8.	Message packaging	28
8.1.	Message envelope and message parts	28
8.1.1.	MIME structure and SOAP profile	28
8.1.2.	MIME and XML considerations	31
8.1.3.	ebXML SOAP envelope extension	32
8.1.4.	ebMS header	33
8.1.5.	Payload containers	34
8.2.	The eb:Messaging container element	35
8.2.1.	General	35
8.2.2.	eb:Messaging element specification	36
8.2.3.	eb:Messaging/eb:UserMessage	37
8.2.4.	eb:Messaging/eb:SignalMessage	43
8.2.5.	Message unit bundling	44
8.3.	Examples of ebMS messages (informative)	45
8.3.2.	UserMessage example	45
8.3.3.	PullRequest message example	47
8.3.4.	Error message example	47
8.3.5.	Receipt message example	48
8.3.6.	"Bundled" message example	48
9.	Error handling	50
9.1.	General	50
9.2.	Packaging of ebMS errors	50
9.2.1.	eb:Error element	50
9.2.2.	eb:Error/@origin	50
9.2.3.	eb:Error/@category	51
9.2.4.	eb:Error/@errorCode	51
9.2.5.	eb:Error/@severity	51
9.2.6.	eb:Error/@refToMessageInError	51
9.2.7.	eb:Error/@shortDescription	51
9.2.8.	eb:Error/Description	51
9.2.9.	eb:Error/ErrorDetail	51
9.3.	ebMS Error message	51
9.4.	Extensibility of the eb:Error element	52
9.4.1.	Adding new ebMS errors	52
9.5.	Generating ebMS errors	52
9.6.	Error reporting	52
9.7.	Standard ebMS errors	53
9.7.1.	General	53
9.7.2.	ebMS processing errors	53
9.7.3.	Security processing errors	54
9.7.4.	Reliable messaging errors	55

10.	Security module	55
10.1.	General	55
10.2.	Security element	55
10.3.	Signing messages	56
10.4.	Signing SOAP with attachments messages	56
10.5.	Encrypting messages	57
10.6.	Encrypting SOAP with attachments messages	57
10.7.	Signing and encrypting messages	57
10.8.	Security token authentication	57
10.9.	Security policy errors	57
10.10.	Secured message examples	58
10.10.1.	Digitally signed and encrypted ebXML message	58
10.10.2.	Digitally signed and encrypted ebXML SOAP with attachments message	60
10.10.3.	Digitally signed receipt signal message	62
10.11.	Message authorization	63
10.12.	Securing the PullRequest signal	65
10.12.1.	Authentication	65
10.12.2.	Authorization	65
10.12.3.	Preventing replay attacks	65
10.13.	Countermeasure technologies	65
10.13.1.	Persistent digital signature	65
10.13.2.	Persistent signed receipt	66
10.13.3.	Non-persistent authentication	66
10.13.4.	Non-persistent integrity	66
10.13.5.	Persistent confidentiality	66
10.13.6.	Non-persistent confidentiality	66
10.13.7.	Persistent authorization	66
10.13.8.	Non-persistent authorization	66
10.14.	Security considerations	66
11.	Reliable messaging module	68
11.1.	The reliable messaging model	68
11.1.1.	General	68
11.1.2.	Message processing	68
11.1.3.	The reliable messaging processor in the MSH	68
11.2.	Reliable delivery of ebMS messages	71
11.2.1.	General	71
11.2.2.	Reliability contracts for the RMP	71
11.2.3.	Reliability contracts for the MSH	72
11.2.4.	Reliability for signal messages	73
11.2.5.	Handling of delivery failures	73

11.3. Reliability of ebMS MEPs	74
11.3.1. General	74
11.3.2. Reliability of the One-Way/Push MEP	75
11.3.3. Reliability of the One-Way/Pull MEP	76
11.3.4. Reliability of the Two-Way/Sync MEP	77
11.3.5. Reliability of other transport-channel-bound MEPs	78
Annex A (informative) The ebXML SOAP extension element schema.....	79
Annex B (informative) Reliable messaging bindings.....	83
Annex C (informative) SOAP format and bindings	90
Annex D (informative) Processing modes	94
Annex E (informative) P-Mode values and ebMS MEP bindings	103
Annex F (informative) Compatibility mapping to ebMS 2.0	106
Annex G (informative) Conformance	114
Bibliography.....	115

iTeh Standards
(<https://standards.itih.ai>)
Document Preview

[ISO 15000-1:2021](https://standards.itih.ai/catalog/standards/iso/06014f15-0458-466e-a490-5b131210a28f/iso-15000-1-2021)

<https://standards.itih.ai/catalog/standards/iso/06014f15-0458-466e-a490-5b131210a28f/iso-15000-1-2021>

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by the OASIS ebXML (Electronic business eXtensible Markup Language) Messaging Services Committee (as "OASIS ebXML Messaging Services Version 3.0") and drafted in accordance with its editorial rules. It was assigned to Technical Committee ISO/TC 154, *Processes, data elements and documents in commerce, industry and administration* and adopted under the "fast-track procedure".

This first edition incorporates content from ISO/TS 15000-2:2004 and ISO/TS 15000-1:2004, which have been withdrawn.

The main changes compared to ISO/TS 15000-2:2004 and ISO/TS 15000-1:2004 are as follows:

- The original ISO/TS 15000-2:2004 specification for the ebXML Messaging Service (ebMS) has been updated and refactored into multiple parts, including this document, the "Core" specification for ebMS, resubmitted to become this document.
- A separate "AS4 Profile of ebMS 3.0 Version 1.0" is submitted separately to ISO/TC 154. It provides a select limited profile of the ebMS3 specification sufficient for Web Services business-to-business messaging applications over the HTTP transport protocol, and is to become ISO 15000-2.
- This document defines the basic (and some optional) features necessary for reliable electronic messaging and the transactional interactions that support such messaging.
- This document noted the availability of several newer methodologies, represented by normative references and informative references included here, that were not available as of the 2004 version.

A list of all parts in the ISO 15000 series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

iTeh Standards
(<https://standards.itih.ai>)
Document Preview

ISO 15000-1:2021

<https://standards.itih.ai/catalog/standards/iso/06014f15-0458-466e-a490-5b131210a28f/iso-15000-1-2021>

Introduction

This document describes a communication-protocol neutral method for exchanging electronic business messages. It defines specific enveloping constructs supporting reliable, secure delivery of business information. Furthermore, the specification defines a flexible enveloping technique, permitting messages to contain payloads of any format type. This versatility ensures that legacy electronic business systems employing traditional syntaxes (i.e. UN/EDIFACT, ASC X12, or HL7) can leverage the advantages of the ebXML infrastructure along with users of emerging technologies.

The prime objective of the ebXML messaging service (ebMS) is to facilitate the exchange of electronic business messages within an XML framework that leverages common Internet standards, without making any assumption on the integration and consumption model these messages will follow on the back-end. These messages may be consumed in different ways that are out of scope of this document: they may bind to a legacy application, to a service, be queued, enter a message workflow process, be expected by an already-running business process, be batched for delayed processing, be routed over an Enterprise Service Bus (ESB) before reaching their consumer application, or be dispatched based on header data or payload data, etc.

It is becoming critical for broad adoption among all partners – large or small - of a supply-chain, to handle differences in message flow capacity, intermittent connectivity, lack of static IP addresses or firewall restrictions. Such new capabilities played an important role in the motivation that led to ebMS 3.0, along with the need to integrate and profile the emerging SOAP-based QoS-supporting standards. The message header profiling that provided, in ebMS 2.0, a standard business-level header, has also been extended to better address the diversity of back-end binding models, as well as the emerging trend in business activity monitoring, the eBusiness side of which a message handler should be able to support.

The ebXML messaging framework is not a restrictive one: business messages, identified as the 'payloads' of ebXML messages, are not limited to XML documents. Traditional EDI formats may also be transported by ebMS. These payloads can take any digital form—XML, ASC X12, HL7, AIAG E5, database tables, binary image files, etc. Multiple payloads, possibly of different MIME types, can be transported in a single ebMS message. An objective of ebXML Messaging protocol is to be capable of being carried over any available transfer protocol. This version of the specification provides bindings to HTTP and SMTP, but other protocols to which SOAP may bind can also be used. The choice of an XML framework rather reflects confidence in a growing XML-based Web infrastructure and development tools infrastructure, the components of which can be leveraged and reused by developers.

Electronic business eXtensible Markup Language (ebXML) —

Part 1: Messaging service core specification

1. Scope

This document provides a communication-protocol neutral method for exchanging electronic business messages. It defines specific enveloping constructs supporting reliable, secure delivery of business information. Furthermore, this document defines a flexible enveloping technique, permitting messages to contain payloads of any format type.

It specifies each of the following:

- Messaging model
- Message pulling and partitioning
- Processing modes
- Message packaging
- Error handling
- Security module
- Reliable messaging module

This document is applicable to all types of organizations (e.g., commercial enterprises, government agencies, not-for-profit organizations) that exchange documents or data electronically using messaging.

2. Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

INTERNET ASSIGNED NAMES AUTHORITY (IANA). *MIME Media Types*, Available from <http://www.iana.org/assignments/media-types/>.

INTERNET ENGINEERING TASK FORCE (IETF). RFC 2045. *Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies*, 1996. Edited by N Freed, et al. Available from <http://www.ietf.org/rfc/rfc2045.txt>.

INTERNET ENGINEERING TASK FORCE (IETF). RFC 2279. *UTF-8, a transformation format of ISO 10646*, 1998. Edited by F. Yergeau. Available from <http://www.ietf.org/rfc/rfc2279.txt>.

INTERNET ENGINEERING TASK FORCE (IETF). RFC 2387. *The MIME Multipart/Related Content-type*, 1998. Edited by E. Levinson, Available from <http://www.ietf.org/rfc/rfc2387.txt>.

INTERNET ENGINEERING TASK FORCE (IETF). RFC 2392. *Content-ID and Message-ID Uniform Resource Locators*, 1998. Edited by E. Levinson. Available from <http://www.ietf.org/rfc/rfc2392.txt>.

INTERNET ENGINEERING TASK FORCE (IETF). RFC 2396. *Content-ID and Message-ID Uniform Resource Locators*, 1998. Edited by T. Berners-Lee, et al. Available from <http://www.ietf.org/rfc/rfc2396.txt>.

INTERNET ENGINEERING TASK FORCE (IETF). RFC 2616. *Hypertext Transfer Protocol -- HTTP/1.1*, 1999. Edited by R. Fielding, et al. Available from <http://www.ietf.org/rfc/rfc2616.txt>.

INTERNET ENGINEERING TASK FORCE (IETF). RFC 2822. *Internet Message Format*, 2001. Edited by P. Resnick. Available from <http://www.ietf.org/rfc/rfc2822.txt>.

INTERNET ENGINEERING TASK FORCE (IETF). RFC 2821. *Simple Mail Transfer Protocol*, 2001. Edited by J. Klensin. Available from <http://www.ietf.org/rfc/rfc2821.txt>.

OASIS. *WS-Reliability 1.1*, 2004. Edited by Kazunori Iwasa, et al. Available from http://docs.oasis-open.org/wsrn/ws-reliability/v1.1/wsrn-ws_reliability-1.1-spec-os.pdf.

OASIS. *Web Services Reliable Messaging (WS-ReliableMessaging) Version 1.1*, 2007. Edited by D. Davis, et al. Available from <http://docs.oasis-open.org/ws-rx/wsrn/v1.1/wsrn.pdf>.

OASIS. *Web Services Reliable Messaging Policy (WS-RM Policy) Version 1.1*, 2007. Edited by D. Davis, et al. Available from <http://docs.oasis-open.org/ws-rx/wsrmp/v1.1/wsrmp.pdf>.

OASIS. *Web Services Security: SOAP Message Security 1.0*, 2004. Edited by Anthony Nadalin, et al. Available from <http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0.pdf>.

OASIS. *Web Services Security UsernameToken Profile 1.0*, 2004. Edited by P. Hallam-Baker, et al. Available from <http://docs.oasis-open.org/wss/2004/01/>.

OASIS. *Web Services Security X.509 Certificate Token Profile*, 2004. Edited by P. Hallam-Baker, et al. Available from <http://docs.oasis-open.org/wss/2004/01/>.

ASIS. *Web Services Security: SOAP Message Security 1.1*, 2005. Edited by Anthony Nadalin, et al. Available from <http://docs.oasis-open.org/wss/v1.1/>.

OASIS. *Web Services Security UsernameToken Profile 1.1*, 2006. Edited by A. Nadalin, et al. Available from <http://docs.oasis-open.org/wss/v1.1/>.

OASIS. *Web Services Security X.509 Certificate Token Profile 1.1*, 2006. Edited by A. Nadalin, et al. Available from <http://docs.oasis-open.org/wss/v1.1/>.

WEB SERVICES INTEROPERABILITY ORGANIZATION. *Attachments Profile Version 1.0*, 2004. Edited by Chris Ferris, et al. Available from <http://www.ws-i.org/Profiles/AttachmentsProfile-1.0-2004-08-24.html>.

WEB SERVICES INTEROPERABILITY ORGANIZATION. *Basic Security Profile Version 1.0*, 2005. Edited by Abbie Barbir, et al. Available from <http://www.ws-i.org/Profiles/BasicSecurityProfile-1.0.html>.

WORLD WIDE WEB CONSORTIUM. *Simple Object Access Protocol (SOAP) 1.1*, 2000. Edited by D. Box, et al. Available from <http://www.w3.org/TR/2000/NOTE-SOAP-20000508/>.

WORLD WIDE WEB CONSORTIUM. *SOAP Version 1.2 Part 1: Messaging Framework*, 2003. Edited by M. Gudgin, et al. Available from <http://www.w3.org/TR/soap12-part1/>.

WORLD WIDE WEB CONSORTIUM. *SOAP Messages with Attachments*, 2000. Edited by J. Barton, et al. Available from <http://www.w3.org/TR/SOAP-attachments>.

WORLD WIDE WEB CONSORTIUM. *Extensible Markup Language (XML) 1.0 (Third Edition)*, 2004. Edited by Tim Bray, et al. Available from <http://www.w3.org/TR/2004/REC-xml-20040204/>.

WORLD WIDE WEB CONSORTIUM. *XML Schema Part 1: Structures Second Edition*, 2004. Edited by Henry S. Thompson, et al. Available from <http://www.w3.org/TR/xmlschema-1/>.

WORLD WIDE WEB CONSORTIUM. *XML-Signature Syntax and Processing*, 2002. Edited by Donald Eastlake, et al. Available from <http://www.w3.org/TR/xmldsig-core/>.

WORLD WIDE WEB CONSORTIUM. *XML Encryption Syntax and Processing*, 2002. Edited by D. Eastlake, et al. Available from <http://www.w3.org/TR/xmlenc-core/>.

WORLD WIDE WEB CONSORTIUM. *Namespaces in XML*, 1999. Edited by Tim Bray, et al. Available from <http://www.w3.org/TR/REC-xml-names/>.

3. Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at <https://www.iso.org/obp>

— IEC Electropedia: available at <http://www.electropedia.org/>

3.1

ebMS error generation

Operation of creating an *ebMS error* (3.14) based on some failure or warning condition

3.2

ebMS error reporting

Operation of communicating an *ebMS error* (3.14) to some other entity

3.3

ebMS message

SOAP message (3.29) that contains SOAP header(s) qualified with the ebMS namespace and that conforms to this document

3.4

ebMS message exchange pattern

ebMS MEP

Choreography of *ebMS user messages* (3.11) which are all related through the use of the referencing feature (*eb:RefToMessageId*)

3.5

ebMS MEP transport channel binding

Binding of an *ebMS message exchange pattern* (3.4) that defines how the ebMS MEP maps abstractly to the channels allowed by an underlying transport protocol

3.6

ebMS MEP transport protocol binding

Binding of an *ebMS message exchange pattern* (3.4) that defines further how an *ebMS MEP transport channel binding* (3.5) is implemented over a specific underlying transport protocol

3.7

ebMS message unit

Logical unit of data that is a subset of an *ebMS Message* (3.3)

3.8

ebMS messaging service handler

ebMS MSH

Entity that is able to generate or process *ebMS messages* (3.3) that conform to this document

3.9

ebMS user message unit

ebMS message unit (3.7) that is represented by the XML infoset `eb:Messaging/eb:UserMessage`, together with any referenced payload items

Note 1 to entry: This is the part of the ebMS message that is submitted by a producer (via the “submit” operation) and that is subject to delivery to a consumer.

3.10

ebMS signal message unit

ebMS message unit (3.7) that is represented by the XML infoset `eb:Messaging/eb:SignalMessage`

Note 1 to entry: Its role is to activate a specific function in the receiving MSH. It is not intended to be delivered to a message consumer.

3.11

ebMS user message

ebMS message (3.3) that contains an *ebMS user message unit* (3.9)

3.12

ebMS signal message

ebMS message (3.3) that contains an *ebMS signal message unit* (3.10)

3.13

ebMS pull signal message

ebMS signal message (3.12) that contains an `eb:PullRequest` element

3.14

ebMS error

Particular case of *Error* (3.15) that is generated by the ebMS module in conformity with this document

3.15

Error

Object representing some failure or warning condition that originates in one of the defined modules (ebMS module, reliability module, security module)