



**International
Standard**

ISO 28005-1

**Ships and marine technology —
Electronic port clearance (EPC) —**

**Part 1:
Message structures and application
programming interfaces**

*Navires et technologie maritime — Opérations portuaires
assistées par systèmes électroniques —*

*Partie 1: Structures des messages et interfaces de programmation
des applications*

[ISO 28005-1:2024](https://standards.iteh.ai/catalog/standards/iso/5296b075-b844-43ad-a8f4-e6850297e483/iso-28005-1-2024)

**Second edition
2024-12**

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

[ISO 28005-1:2024](https://standards.iteh.ai/catalog/standards/iso/5296b075-b844-43ad-a8f4-e6850297e483/iso-28005-1-2024)

<https://standards.iteh.ai/catalog/standards/iso/5296b075-b844-43ad-a8f4-e6850297e483/iso-28005-1-2024>



COPYRIGHT PROTECTED DOCUMENT

© ISO 2024

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

	Page
Foreword	ix
Introduction	xi
1 Scope	1
2 Normative references	1
3 Terms, definitions, and abbreviated terms	1
3.1 Terms and definitions.....	1
3.2 Abbreviated terms.....	5
4 Structure of XSD data type and object definitions	6
4.1 General.....	6
4.2 Principles for XML descriptions in the ISO 28005 series.....	7
4.2.1 No use of XML attributes.....	7
4.2.2 Defaults for minOccurs and maxOccurs.....	7
4.2.3 Signalling empty XML tags.....	7
4.2.4 Order of child elements in XSD files.....	7
4.2.5 Character set.....	7
4.2.6 Principles for defining types with code lists.....	7
4.2.7 XSD name space for general XSD data types.....	8
4.2.8 ISO 28005 name space.....	8
4.2.9 Use of Xpath expressions.....	8
4.3 Structure of clauses defining data types.....	8
4.3.1 Clause and data type name.....	8
4.3.2 Definition.....	8
4.3.3 Type defined as XSD code.....	9
4.3.4 Representation.....	9
4.4 Creating valid XSD schema files.....	9
4.4.1 File structure.....	9
4.4.2 Numbering of XSD files and message version code.....	10
4.4.3 Location of XSD files.....	11
4.5 Reference to data types defined in ISO 28005-2:2021.....	11
5 Adapted XSD data types for ISO 28005	12
5.1 General.....	12
5.2 epc:anyURI – Generalized URI.....	12
5.2.1 Definition.....	12
5.2.2 Type.....	12
5.2.3 Representation.....	12
5.3 epc:boolean – Boolean flag.....	12
5.3.1 Definition.....	12
5.3.2 Type.....	12
5.3.3 Representation.....	12
5.4 epc:date – General date.....	12
5.4.1 Definition.....	12
5.4.2 Type.....	12
5.4.3 Representation.....	13
5.5 epc:dateTime – Time and date, with time zone.....	13
5.5.1 Definition.....	13
5.5.2 Type.....	13
5.5.3 Representation.....	13
5.6 epc:decimal – decimal number.....	13
5.6.1 Definition.....	13
5.6.2 Type.....	13
5.6.3 Representation.....	13
5.7 epc:duration – Time duration.....	14
5.7.1 Definition.....	14

ISO 28005-1:2024(en)

5.7.2	Type	14
5.7.3	Representation	14
5.8	epc:int – Integer number	14
5.8.1	Definition	14
5.8.2	Type	14
5.8.3	Representation	14
5.9	epc:string – General string	14
5.9.1	Definition	14
5.9.2	Type	14
5.9.3	Representation	15
5.10	epc:token – Computer-understandable string	15
5.10.1	Definition	15
5.10.2	Type	15
5.10.3	Representation	15
5.11	epc:xpath – Identification of an XML data item	15
5.11.1	Definition	15
5.11.2	Type	15
5.11.3	Representation	15
6	General ISO 28005 data types	15
6.1	General	15
6.2	epc:AuthenticatorType – Authenticator of information	15
6.2.1	Definition	15
6.2.2	Type	16
6.2.3	Representation	16
6.3	epc:AuthorizationTokenType – Authorization token	16
6.3.1	Definition	16
6.3.2	Type	16
6.3.3	Representation	16
6.4	epc:ContactInfoType – Contact information	16
6.4.1	Definition	16
6.4.2	Type	17
6.4.3	Representation	17
6.5	epc:CommunicationNumberType – Communication number information	17
6.5.1	Definition	17
6.5.2	Type	17
6.5.3	Representation	18
6.6	epc:CountryCodeContentType – Country identification	18
6.6.1	Definition	18
6.6.2	Type	18
6.6.3	Representation	18
6.7	epc:CountrySubdivisionCodeContentType – Country subdivision identification	18
6.7.1	Definition	18
6.7.2	Type	18
6.7.3	Representation	19
6.8	epc:CrewDutyType – Duty onboard or on shore	19
6.8.1	Definition	19
6.8.2	Type	19
6.8.3	Representation	19
6.9	epc:LocationType – Identification of a location	19
6.9.1	Definition	19
6.9.2	Type	19
6.9.3	Representation	21
6.10	epc:NameType – Name of person	21
6.10.1	Definition	21
6.10.2	Type	21
6.10.3	Representation	21
6.11	epc:OrganizationType – Description of an organization	22
6.11.1	Definition	22

ISO 28005-1:2024(en)

6.11.2	Type	22
6.11.3	Representation	22
6.12	epc:PostalAddressType – A postal mail address	22
6.12.1	Definition	22
6.12.2	Type	22
6.12.3	Representation	23
6.13	epc:ShipIDType – Ship identity	23
6.13.1	Definition	23
6.13.2	Type	23
6.13.3	Representation	23
6.14	epc:ReportingSystemType – Name of a reporting system	24
6.14.1	Definition	24
6.14.2	Type	24
6.14.3	Representation	24
6.15	epc:AttachmentType – Reference to an attached document	24
6.15.1	Definition	24
6.15.2	Type	24
6.15.3	Representation	24
6.16	epc:ReferenceCodeType – General reference code	25
6.16.1	Definition	25
6.16.2	Type	25
6.16.3	Representation	25
6.17	epc:SystemIdType – Identity code for a software system	25
6.17.1	Definition	25
6.17.2	Type	25
6.17.3	Representation	25
6.18	epc:SignatureCertificateIdType – Name of digital signature holder	26
6.18.1	Definition	26
6.18.2	Type	26
6.18.3	Representation	26
6.19	epc:VersionType – Version code	26
6.19.1	Definition	26
6.19.2	Type	26
6.19.3	Representation	27
7	ISO 28005 design principles	27
7.1	Harmonization with the IMO reference data model	27
7.2	Fully automated machine to machine	27
7.3	Using carrier independent and internet-based protocols	28
7.4	General format of message sequence diagrams	28
7.5	Sender and receiver versus client and server — asynchronous message transfers	29
7.6	Generalization of service	30
7.7	Different levels of sessions	30
7.7.1	HTTP session	30
7.7.2	Session	31
7.7.3	Session context	32
7.8	One service per request and session	33
7.9	Linking receivers to service providers	33
7.10	Service request states	33
7.10.1	Message processing	33
7.10.2	State diagram for service requests	34
7.10.3	Message functions	36
7.10.4	Specification of request timeout	36
7.10.5	Message and service request return values	37
7.11	Send data once only	37
7.12	Message context	37
7.13	General message structure	39
7.14	Digital signatures	40
7.15	Secure data transfer	40

ISO 28005-1:2024(en)

7.16	Additional authorization for accessing API.....	40
7.17	Message implementation guide.....	41
7.18	Other formats than XML for the message body.....	41
7.19	No explicit service discovery.....	41
8	Message exchange patterns.....	41
8.1	General rules.....	41
8.1.1	Application of this specification.....	41
8.1.2	Use of reference codes.....	42
8.1.3	Use of final flag in message header.....	42
8.1.4	Use of service timeout or session context end.....	43
8.1.5	Status and error codes.....	43
8.1.6	Multiple senders.....	44
8.1.7	Interleaving update requests with status messages.....	45
8.2	Sequence diagrams.....	45
8.2.1	Pattern 1: Service request and updates.....	45
8.2.2	Pattern 2: Status poll.....	47
8.2.3	Pattern 3: Simple report.....	47
8.2.4	Pattern 4: Request information.....	48
8.2.5	Pattern 5: Subscribe to service or information.....	48
9	Using HTTP multi-part message.....	49
9.1	General.....	49
9.2	Example of an ISO 28005-1 multi-part message.....	50
9.3	Content-Type: multipart/form-data.....	50
9.4	Content-Encoding: gzip.....	51
9.5	Prose text.....	51
9.6	Content-Type: application, image or other.....	51
9.7	Content-Disposition: form-data; name = name; filename = file.name;.....	51
10	Definitions related to the message header part.....	52
10.1	General.....	52
10.2	epc:MessageFunctionCodeContentType - Message function code.....	52
10.2.1	Definition.....	52
10.2.2	Type.....	52
10.2.3	Representation.....	52
10.3	epc:ReplyInformationType - Type of sender response code.....	52
10.3.1	Definition.....	52
10.3.2	Type.....	52
10.3.3	Representation.....	53
10.4	epc:MessageBodyFormatContentType - Format of body data.....	53
10.4.1	Definition.....	53
10.4.2	Type.....	53
10.4.3	Representation.....	53
10.5	epc:ServiceTypeCodeContentType - Code for identification of service type.....	53
10.5.1	Definition.....	53
10.5.2	Type.....	54
10.5.3	Representation.....	54
10.6	epc:ServiceCodeContentType - Code for identification of a service in a group.....	54
10.6.1	Definition.....	54
10.6.2	Type.....	54
10.6.3	Representation.....	54
10.7	epc:StatusType - General message and service request status and error codes.....	54
10.7.1	Definition.....	54
10.7.2	Type.....	54
10.7.3	Representation.....	55
10.8	epc:SpecialAttachmentType - Description of special attachment.....	55
10.8.1	Definition.....	55
10.8.2	Type.....	55
10.8.3	Representation.....	56

ISO 28005-1:2024(en)

10.9	epc:MessageManifestType – Number of message parts	56
10.9.1	Definition	56
10.9.2	Type	56
10.9.3	Representation	56
10.10	epc:EPCMessageHeaderType – Standard header for an EPC message	56
10.10.1	Definition	56
10.10.2	Type	56
10.10.3	Representation	59
11	Definitions related to the message body part	61
11.1	General	61
11.2	XML message body	61
11.2.1	epc:EPCMessageBodyType – the XML body data type	61
11.2.2	Structure of message body definition table	62
11.3	Encryption of selected content	62
11.4	UN/EDIFACT message body	63
11.5	UN/EDIFACT status message	63
11.6	JSON message body	63
12	Definitions related to attachment message parts	63
12.1	General	63
12.2	Reference to an attached document in an XML body	63
13	Definitions related to X.509 certificate message parts	64
14	Definitions related to the digital signature message part	64
14.1	General	64
14.2	Signers	64
14.3	epc:EPCMessageSignatureType – Digital signatures of message parts	65
14.3.1	Definition	65
14.3.2	Type	65
14.3.3	Representation	65
15	General definitions related to the use of HTTP	65
15.1	Conceptual structure of a receiver	65
15.2	Conceptual structure of a sender	66
15.3	Transmission protocol	67
15.4	Avoid use of HTTP redirect and similar mechanisms	67
15.5	Optional use of HTTP keep-alive	67
15.6	API access point URL	67
15.7	HTTP methods	67
15.8	Different types of synchronous return values	68
15.8.1	General	68
15.8.2	Connection error	68
15.8.3	HTTP error codes	68
15.8.4	Message status	68
15.8.5	Service request status	69
16	API access points for asynchronous HTTP communication	69
16.1	General	69
16.2	Message patterns to use	69
16.3	No authorization on the sender's URL	69
17	API access point for synchronous HTTP communication	69
17.1	General	69
17.2	Message patterns to use	69
18	Authorization to access API access point	70
18.1	General	70
18.2	The message pattern	70
18.3	epc:ServiceAuthorizationType – Type of service authorization	71
18.3.1	Definition	71
18.3.2	Type	71

ISO 28005-1:2024(en)

18.3.3	Representation.....	71
18.4	The message body.....	72
19	Specifications for the message implementation guide (MIG).....	72
19.1	General structure of MIG.....	72
19.2	MIG Introduction.....	72
19.3	High level description of use case.....	72
19.4	Prerequisites.....	72
19.5	Message sequence diagrams.....	72
Annex A	(normative) EPC request body.....	74
Annex B	(informative) Message implementation guide for access authorization.....	75
Annex C	(informative) Message implementation guide for maritime single window and mandatory ship reporting system.....	80
Annex D	(normative) Code list for special attachments.....	87
Annex E	(normative) Message function codes for XML messages.....	88
Annex F	(normative) Message and service request status codes.....	89
Annex G	(normative) Service codes.....	90
Annex H	(normative) Software system type codes.....	94
Annex I	(normative) Code list for authenticator and contact point roles.....	95
Annex J	(normative) Codes for digital signatures.....	96
Annex K	(informative) IMO FAL mapping.....	97
Bibliography	99

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

[ISO 28005-1:2024](https://standards.iteh.ai/catalog/standards/iso/5296b075-b844-43ad-a8f4-e6850297e483/iso-28005-1-2024)

<https://standards.iteh.ai/catalog/standards/iso/5296b075-b844-43ad-a8f4-e6850297e483/iso-28005-1-2024>

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 document 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).

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents. ISO shall not be held responsible for identifying any or all such patent rights.

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 Technical Committee ISO/TC 8, *Ships and marine technology*, Subcommittee SC 11, *Intermodal and short sea shipping*.

This second edition cancels and replaces the first edition (ISO 28005-1:2013), which has been technically revised.

The main changes are as follows:

- a general introduction to all documents in the ISO 28005 series, including the structure of XML and XSD files and general XML type definitions, has been added in [Clauses 4 to 6](#);
- [Clause 7](#) defining the general design principles for the ISO 28005 series has been added;
- [Clause 8](#) has added general message exchange patterns that can be referenced in message implementation guides;
- [Clause 9](#) has added a more general multi-part message structure based on the HTTP multi-part form structure. This includes a formalization of how attachments to the XML based message body can be added to the message. It also includes possibilities for using EDIFACT or JSON as a message body or as attachments to the standardized XML message body or adding encrypted message parts as attachments (detailed in [Clauses 11](#) and [12](#));
- the message header has been updated so that it contains sufficient information to do frontend message processing before forwarding the message to the service specific software modules (see [Clause 10](#));
- support for digital signatures has been added in [Clause 13](#). Digital signature certificates can be attached to a message (see [Clause 14](#));
- a definition of a HTTP-based transport protocol has been added in [Clauses 15 to 17](#);
- a possibility for access authorization has been added in [Clause 18](#);
- a definition for the structure of message implementation guides has been added in [Clause 19](#);

ISO 28005-1:2024(en)

- message implementation guides for access authorization have been added in [Annex B](#), and a maritime single window and mandatory reporting systems have been added in [Annex C](#).

A list of all parts in the ISO 28005 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.iteh.ai>) Document Preview

[ISO 28005-1:2024](#)

<https://standards.iteh.ai/catalog/standards/iso/5296b075-b844-43ad-a8f4-e6850297e483/iso-28005-1-2024>

Introduction

This document contains technical specifications that facilitate an efficient exchange of electronic information between ships and shore parties for coastal transit or port calls. It defines the general message format, general message exchange patterns and a message transfer protocol. Other parts of the ISO 28005 series define data models for various types of message transfers.

The message transfer protocol specified in this document uses HTTP over TLS. While many HTTP type application program interfaces (API) are built on the representational state transfer (REST) principle, this document does not use REST. APIs developed according to this document can support physical services such as ordering tugs or pilots, where state changes cannot be guaranteed to be compliant with REST.

This document can be used as a specification of a message format that can be transmitted over other transport protocols than the one defined in this document.

This document is aligned with the IMO FAL guidelines on authentication, integrity and confidentiality in information exchanges via maritime single windows and related services (IMO FAL.5/Circ.46)^[1] and the IMO FAL guidelines for harmonized communication and electronic exchange of operational data for port calls, 31 March 2023 (IMO FAL.5/Circ.52).^[2] The specifications in this document are aligned with the requirements in ISO 23807.^[3]

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

[ISO 28005-1:2024](https://standards.iteh.ai/catalog/standards/iso/5296b075-b844-43ad-a8f4-e6850297e483/iso-28005-1-2024)

<https://standards.iteh.ai/catalog/standards/iso/5296b075-b844-43ad-a8f4-e6850297e483/iso-28005-1-2024>

Ships and marine technology — Electronic port clearance (EPC) —

Part 1: Message structures and application programming interfaces

1 Scope

This document defines the principles, methods and requirements for message exchanges between ships, ship representatives, and other shore parties via a peer-to-peer communication system. This document defines the message structure, including how the data content is assembled from other parts of the ISO 28005 series, and how digital signatures for authentication, integrity, and confidentiality of the message can be used. It also specifies a transport protocol, the basic message exchange patterns, and the protocol related roles of each party in the message exchange. Furthermore, it specifies how more specific message implementation guides (MIGs) are provided for each type of communication application.

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.

ISO 3166-1, *Codes for the representation of names of countries and their subdivisions — Part 1: Country code*

ISO 3166-2, *Codes for the representation of names of countries and their subdivisions — Part 2: Country subdivision code*

ISO 6709, *Standard representation of geographic point location by coordinates*

RFC 1952, *GZIP file format specification version 4.3*

RFC 3986, *Uniform resource identifier (URI): Generic syntax*.

RFC 5246, *The transport layer security (TLS) protocol version 1.2*

RFC 7578, *Returning values from forms: multipart/form-data*

RFC 8446, *The transport layer security (TLS) Protocol Version 1.3*

UN/EDIFACT code list 3035 – Party function code qualifier, Release D.00A, <https://service.unece.org/trade/untdid/d00a/tred/tred3035.htm>

UN/EDIFACT code list 3139 - Contact function code, Release D.23A, <https://service.unece.org/trade/untdid/latest/tred/tred3139.htm>

3 Terms, definitions, and abbreviated terms

3.1 Terms and definitions

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

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

- ISO Online browsing platform: available at <https://www.iso.org/obp>
- IEC Electropedia: available at <https://www.electropedia.org/>

3.1.1

HTTP

hypertext transfer protocol

client/server communication protocol used to transfer information in the World Wide Web

Note 1 to entry: HTTP is defined in RFC 2068^[4] as a generic and stateless application-level protocol for distributed and collaborative, information systems.

Note 2 to entry: In this document, the term HTTP is used to mean HTTP implemented over *transport layer security* (3.1.2), i.e. *HTTPS* (3.1.3), unless otherwise specified.

3.1.2

TLS

transport layer security

protocol for secure communication over the internet

Note 1 to entry: TLS is defined in RFC 5246 (Version 1.2) and RFC 8446 (Version 1.3).

3.1.3

HTTPS

hypertext transfer protocol secure

HTTP (3.1.1) over *transport layer security* (TLS) (3.1.2)

Note 1 to entry: HTTPS is an extension of HTTP used for secure communication and is defined in RFC 2818.^[6] It uses TLS to encrypt the communication.

Note 2 to entry: In this document, the term HTTP is used to mean HTTP implemented over TLS, i.e. HTTPS, unless otherwise specified.

3.1.4

PKI

public key infrastructure

set of hardware, software, people, policies and procedures needed to create, manage, distribute, use, store and revoke digital certificates and manage public-key encryption

[SOURCE: ISO 20415:2019, 3.14]

3.1.5

digital signature

data appended to, or cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the unit and protect against forgery by, for example, the recipient

[SOURCE: ISO 20415:2019, 3.5]

3.1.6

API

application programming interface

collection of communication methods and associated parameters used by a *client* (3.1.11) to exchange information with a *server* (3.1.12)

Note 1 to entry: In this document, the term API is used in the meaning of one specific arrow in the sequence diagram (see [Figure 2](#)). Thus, a session will normally require the use of several APIs. This document describes one general *API access point* (3.1.17) that can be used by all APIs by changing the number of message components as well as the contents of one or more message parts.