BS ISO 28005-1:2013

BSI Standards Publication

Security management systems for the supply chain — Electronic port clearance (EPC)

Part 1: Message structures

raising standards worldwide™

National foreword

This British Standard is the UK implementation of ISO 28005-1:2013. It supersedes PD ISO/PAS 28005-1:2012 which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee SME/32, Ships and marine technology - Steering committee.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

ISBN 978 0 580 71008 7

ICS 35.240.60; 47.020.99

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 March 2013.

Amendments issued since publication

Date	Text affected

BS ISO 28005-1:2013

INTERNATIONAL STANDARD

ISO 28005-1

First edition
2013-03-01

Security management systems for the supply chain — Electronic port clearance (EPC) —

Part 1: Message structures

Systèmes de management de la sécurité pour la chaîne d'approvisionnement — Opérations portuaires assistées par systèmes électroniques —

Partie 1: Structures des messages

Reference number
ISO 28005-1:2013(E)

COPYRIGHT PROTECTED DOCUMENT

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

Page

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. 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. 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.

The committee responsible for this document is ISO/TC 8, *Ships and marine technology*.

This first edition of ISO 28005-1 cancels and replaces the first edition of ISO/PAS 28005-1:2012.

ISO 28005 consists of the following parts, under the general title *Security management systems for the supply chain — Electronic port clearance (EPC)*:

— *Part 1: Message structures — Implementation of a maritime single window system*

— *Part 2: Core data elements*

Introduction

This part of ISO 28005 contains technical specifications that facilitate an efficient exchange of electronic information between ships and shore for coastal transit or port calls. This part of ISO 28005 is intended to cover the exchange of safety and security information required under the IMO Convention on Facilitation of International Maritime Traffic (FAL) and other international specifications as defined in ISO 28005-2. This part of ISO 28005 is based on XML and is intended as a complementary International Standard to the UN/EDIFACT (electronic data interchange for administration, commerce and transport) standards specified in the FAL compendium. Normally, implementers of this part of ISO 28005 are expected to also provide electronic interfaces supporting the use of UN/EDIFACT standards. Parties with economic interests related to the ship, cargo, passengers or crew, such as land transporters, receiving parties, insurers, financial entities can also find value in configuring their data reception capability to receive information formatted in accordance with this part of ISO 28005; however, this is not a requirement of this part of ISO 28005.

There are a number of other data exchanges related to port calls taking place that are outside of the scope of this part of ISO 28005 such as:

a) administrative- and trade-related data exchanges;

b) customs clearance for import and export of goods;

c) logistics arrangements for loading and discharge of cargo, including bay plans, mooring instructions, tug orders and other needs;

d) commercial exchanges related to freight costs, ownership and insurance of cargo. Ship operational exchanges related to the ordering of consumables, water, bunkers and spare parts, or the exchange of crews;

e) commercial exchanges related to port logs/statements of fact, calculations of demurrage and port fees.

The following International Standards and Technical Specifications (developed under Technical Committee ISO/TC 154) support information interchange between and within individual organizations with economic interests:

— ISO 8601 (date and time);

— ISO 6422 with ISO 8440;

— ISO 7372 (trade data elements directory);

— ISO 9735 (all parts) on electronic data interchange for administration, commerce and transport (EDIFACT);

— ISO/TS 20625;

— ISO/TS 15000-5 (ebCCTS core components);

— ISO 14533 (all parts) (long term signature profiles);

— ISO 17369 [statistical data and metadata exchange (SDMX)].

This part of ISO 28005, possibly together with other standards, can be used to implement a single window (SW) for port clearance. This SW can provide for: a) the simplified electronic means for clearance of ships in maritime transport; b) standardization in logistics activities, interface and information in overall maritime transport; c) improved maritime logistics efficiency and strengthened maritime logistics competitiveness of IMO member states. The SW standard for maritime transport is built upon general SW concepts and characteristics and has been expanded to integrate the requirements of maritime transport.

This part of ISO 28005 specifies the overall configuration of electronic port clearance (EPC) and defines the message structures for use in EPC. ISO 28005-2 contains definitions of core data elements used in the message structures.

INTERNATIONAL STANDARD ISO 28005-1:2013(E)

Security management systems for the supply chain — Electronic port clearance (EPC) —

Part 1: Message structures

1 Scope

This part of ISO 28005 specifies necessary guidance information related to electronic port clearance (EPC), such as message transmission requirements, business scenarios, message structures and software requirements. Within the context of this part of ISO 28005, EPC incudes the activities that a user, such as a ship's master, a shipping agency or a ship owner undertakes to submit electronic data to appropriate organizations that approve or reject the clearance for the ship to enter or leave port.

Annex A provides implementation advice for a single window (SW). Annex B suggests a methodology for the development of a SW.

This part of ISO 28005 defines XML message structures for the transmission of information between a ship or its representatives and certain organizations responsible for the processing of the ship's port clearance request. The information intended to be transferred is that which is defined by the FAL Convention and other related international instruments as identified by ISO 28005-2. These message structures are primary intended for machine-to-machine data transfers.

This part of ISO 28005 allows different configurations of the SW, from a minimum solution to support basic clearance requirements to a more complex system to facilitate more extensive cooperation between ship and shore organizations.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 28005-2, *Security management systems for the supply chain — Electronic port clearance (EPC) — Part 2: Core data elements*

3 Terms and definitions

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

3.1
acknowledgement
message sent from authorities giving the final acknowledgement of a request with the result of the request as an approval or denial

3.2
authority
entity or entities acting on behalf of the port state under national legislation

3.3
cancellation
message sent from the ship to the single window to cancel a previous request,

Note 1 to entry: If the request is for port call clearance, the cancellation applies to all requests associated with that port call.

3.4
electronic port clearance
EPC
port clearance carried out through electronic message sending through a single window between port authorities and users

3.5
empty tag
tag containing data elements that cannot be given a value by the sender and that is empty

Note 1 to entry: See ISO 28005-2.

3.6
journal number
reference code assigned by the single window to one specific call from one specific ship to the port

Note 1 to entry: The journal number is normally assigned as a result of a first request message, but can also be assigned by other methods. A scheduled service could get a pre-assigned series of journal numbers to cover a certain period. The journal number is used in the exchanges between ship and single window to identify to which port call a certain transaction refers.

3.7
port
location on a coast or shore containing one or more port facilities where ships can berth and transfer people or cargo to or from land

Note 1 to entry: Clearance to port usually implies clearance for one specific port facility as defined in SOLAS Chapter XI-2 [International Ship and Port Facility Security Code (ISPS)]. Shifting the ship from one port facility to another requires additional clearance, although not as extensive as for the general port clerance. For the purposes of this part of ISO 28005, the term port is used with the meaning of a port and an associated specific port facility in the port.

3.8
port clearance
process undertaken by an entity or entities for the purpose of determining if a ship may enter the port, berth at a facility, conduct certain operations and/or depart the port

Note 1 to entry: For cargo, additional clearance may be required to allow the unloading of the cargo or import of the cargo from the tax-free areas.

3.9
receipt
message sent from the single window as an inital response to a request

Note 1 to entry: The receipt shows that the message was received and read and that necessary processing has been initiated. In cases where all the processing is done within the single window, the receipt may be the only response to the request.

3.10
request
message sent from the ship to the single window, containing a request for some form of clearance or other service from one or more authorities connected to the single window

3.11
ship
ship itself, an agent in the port of call, the owner or management company, or any other entity that can legally represent the ship in the transaction

Note 1 to entry: The term "ship" is used as one of the parties to a communication with a single window.

3.12
single window
SW
facility that allows parties involved in trade and transport to lodge standardized information and documents with a single entry point to fulfil all import, export and transit-related regulatory requirements

Note 1 to entry: If information is electronic, individual data elements should only be submitted once.

Note 2 to entry: In this part of ISO 28005, the term "single window" is restricted to a single window that is used for the clearance of ships according to requirements in the FAL Convention. This is sometimes called a maritime single window.

Note 3 to entry: It is defined in UN/CEFACT Recommendation No. 33.

3.13
uniform resource identifier
URI
string of characters used to identify a name or a resource

Note 1 to entry: Such identification enables interaction with representations of the resource over a network (typically, the World Wide Web) using specific protocols. Schemes specifying a concrete syntax and associated protocols define each URI.

Note 2 to entry: A valid URI is specified according to ISOC RFC 3305; schemes, such as "mailto", "http" and "https", are used in this part of ISO 28005.

4 Conceptual system design

4.1 General SW functionality

This part of ISO 28005 does not directly define the functionality of an SW. However, it is assumed that a SW exists and that it implements functionality to provide an electronic interface between the ship or the ship representatives and authorities ashore.

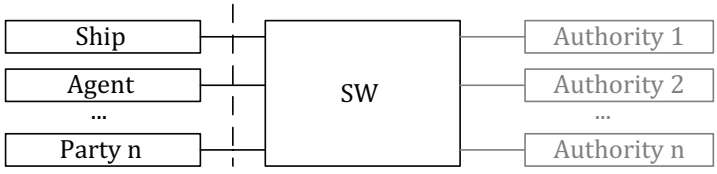

Figure 1 — General topology of SW system

The expected system configuration is shown in Figure 1. The SW acts as a single message centre for data sent to or received from the ship or its representatives. The relevant authorities use the SW to perform their clearance functions. The dashed line is the interface covered by this part of ISO 28005.

4.2 Business-to-administration or business-to-business system

The definition of SW implies that the SW is uniquely a mechanism that implements a business-to-administration (B2A) relationship. However, in the context of the interface between ship and port state authorities, the port will in some cases operate as an authority and in other cases as a private entity. Thus, this part of ISO 28005 will support both types of SW as illustrated by Figure 2.

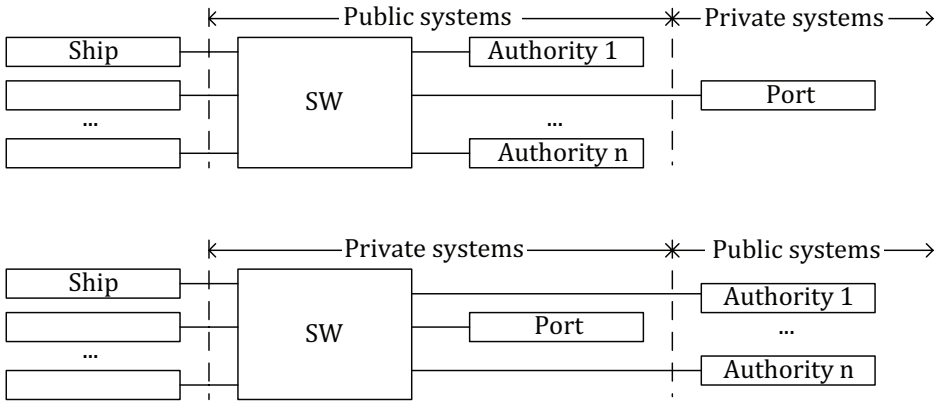

Figure 2 — Alternative SW solutions

Thus, a SW may in principle be implemented by private parties in the port and transfer data to public authorities or vice versa. Also, data transfer could be between the ship and public authorities and the port itself might not be part of the message exchange at all. This part of ISO 28005 does not mandate any particular organization of the SW.

4.3 Alternative message sequences

Port clearance can be a simple process where one clearance request is sent from a ship and one clearance acknowledgement is returned from the SW when the ship has been cleared by the relevant authorities. However, it may also be more complex, involving early bookings, updates, as well as cancellations of the whole port call as illustrated by Figure 3.

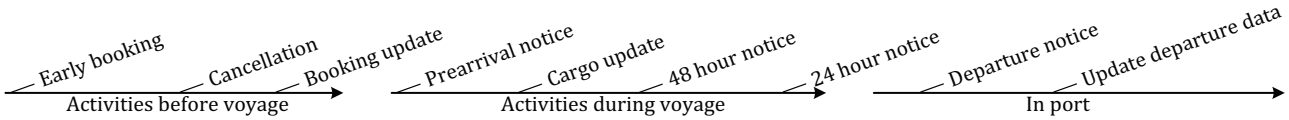

Figure 3 — Example of a more complex ship voyage time line

This part of ISO 28005 supports both simple and more complex clearance processes. Actual message requirements, timing and updates may be restricted by local legislation. Minimum requirements are defined in 5.1.

4.4 Information sent by ship or agent

Some ships might not have Internet access or might have delegated reporting responsibilities to an agent for other reasons. This part of ISO 28005 supports information transmissions both from ship and agent. Even if ships have access to the Internet, this might not be available at all times so the SW needs to support some form of store and forward (e-mail) transmission mechanism in addition to direct web-based access. This does not have any direct consequence for message formats.

4.5 Data to be input once

This part of ISO 28005 defines message structures that require information to be input only once. This also includes provisions for the SW to accept certain data in other formats than those defined in this part of ISO 28005.

5 General transaction requirements

5.1 General transaction pattern

The general transaction pattern is shown in Figure 4. The shaded areas represent message exchanges that are optional in this part of ISO 28005.

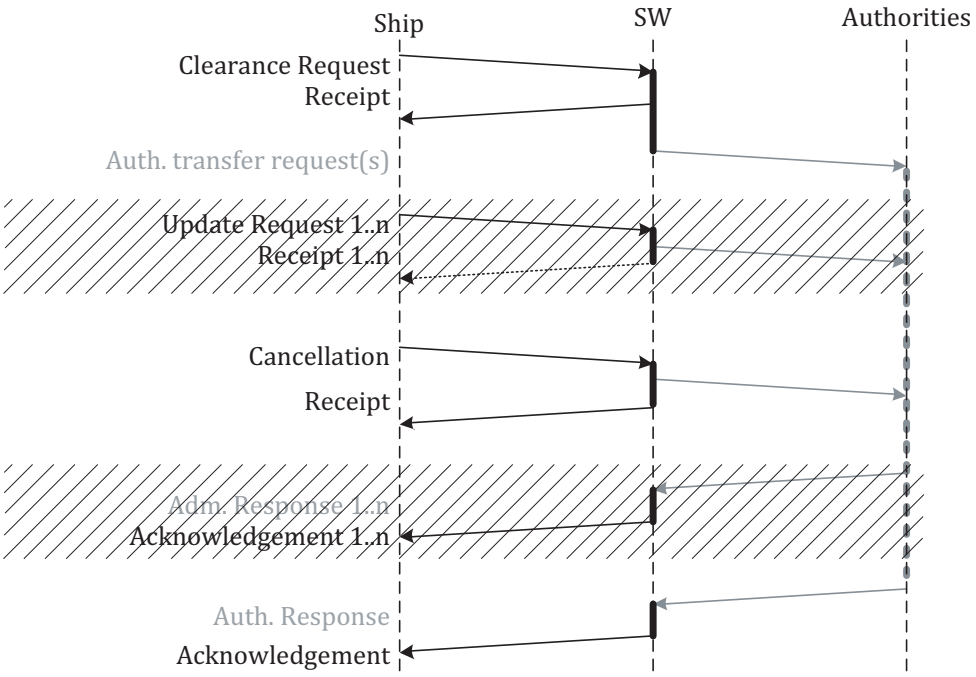

Figure 4 — General transaction pattern

5.1.1 Unique journal number

With the following exception, all message exchanges between the ship (or agent) and the SW relating to one specific port call shall be identified by a unique journal number for the port call. The journal number is a field in the message header structure. The exception to this rule is that the first clearance request from the ship (or agent) to the SW shall have an empty tag for the journal number if the journal number is unknown to the ship or agent at the time of transmission. The receipt message from the SW, if the receipt accepts the request, will contain the journal number to be used in all subsequent message exchanges. This ensures that all messages related to one particular port call can be easily and uniquely identified.

NOTE The SW needs to construct a unique journal number for each ship's port call and embed it in a token string.

5.1.2 Request

A request message is sent to request clearance to enter or leave the port. The request message may also be used for other purposes as described in 5.3 if the SW accepts such messages.

The SW may allow a request message to be updated for the puposes of changing or adding information related to the port call.

The SW is, however, not required to accept updates of request messages. If updates are not allowed, approval or denial of port clearance will be based on the initial request submission and further requests will automatically receive a negative receipt message. In this case, if the orginal request message was; in error, incomplete, or the information had subsequently changed, the original request should be cancelled and a new request submitted.

When information contained in an accepted update is received, the authorities requiring that information shall be informed by the SW and previous approvals issued by that authority, which were based on the original information, shall be automatically cancelled. The corresponding status of all required acknowledgements will be transmitted to the ship in the receipt message.

The ship shall keep track of the status of the required approvals.

The request message shall list the copy-to parties (parties that should be copied on all responses to the request). The SW may limit the number of recipients and this should be conveyed in the receipt message.

5.1.3 Receipt

All messages from the ship to the SW, which can be processed by the SW, will receive a receipt message from the SW. The receipt message signifies one of the following two cases.

a) The information and syntax of the message sent from the ship is free of syntax errors and sufficiently complete to be forwarded to some or all authorities involved. The receipt message lists those authorities to which the request message had been forwarded. Upon receipt of the forwarded message, the authorities begin processing the information for the purpose of issuing a request approval or denial through an acknowledgement message. Port clearance approval or denial is sent to the ship once processing is complete. The receipt message also specifies which, if any, authorities do not have enough information to process their approval or denial decision.

b) The message from the ship contained syntax errors, is incomplete, or contains information that cannot be processed by the SW. The message cannot be forwarded to the authorities and cannot cause any further processing. Incomplete request messages to a SW that do not allow for updates shall be ignored. The message needs to be corrected and resent. Examples of information that cannot be processed include excessively long lists of parties that are copied (copy-to parties), an illegal number of message bodies, illegal message codes or similar.

Messages that cannot be processed by the SW parties shall be silently ignored and shall not receive a receipt.

5.1.4 Cancellation

A cancellation message may be sent to the SW to cancel a previously submitted request. A cancellation message that received a receipt ceases any further processing of the request and all previously received acknowledgement messages, if any, will be voided.

NOTE A successful cancellation only applies to the SW process and there can still be consequences related to, for instance port fees.

5.1.5 Acknowledgement

An acknowledgement message is sent to the ship when one or more authorities process(es) a request and make a decision. An example of a transaction pattern is shown in Figure 5.

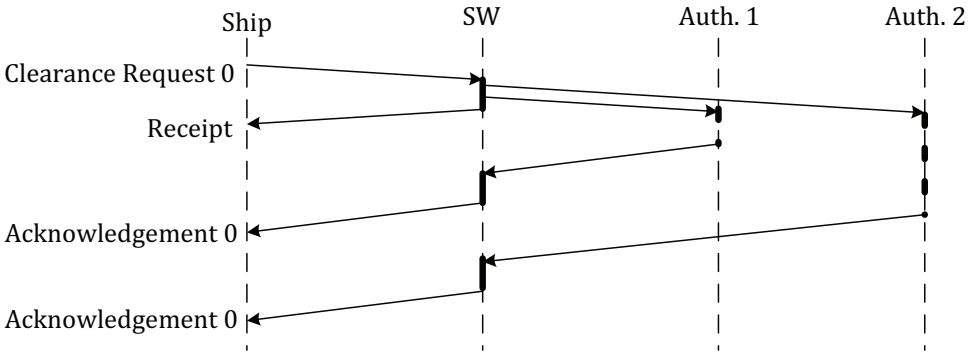

Figure 5 — Normal approval/denial sequence

If the SW allows multiple updates to a request and these updates result in retransmission of certain approval/denial (acknowledgement) messages, the ship shall keep track of acknowledgement messages so that an accurate at-the-moment status can be maintained. The SW is not required to forward acknowledgement messages for requests that have already been updated or cancelled.

This part of ISO 28005 allows for the SW to buffer and merge acknowledgements from two or more authorities and send only one acknowledgement message to the ship. In this case, the initial receipt shall specifiy one authority (the SW itself) as place holder for merged acknowledgements.

5.2 Multiple parties copied

This part of ISO 28005 allows for the SW to send copies of receipts and acknowledgements to multiple parties. If multiple copied parties are allowed and used, they shall be listed in the initial request message. However, this part of ISO 28005 neither requires the SW to permit multiple copied parties nor does it prohibit the SW from restricting the number of parties being copied to a certain limit.

5.3 Support for other reporting requirements

This part of ISO 28005 allows the SW to accept messages for other purposes, such as advance notice of arrival, passing national baseline, entering VTS or ship reporting areas. The request message format has provisions to allow for such reporting and may be used for this purpose. However, the SW is not required to implement this functionality.

5.4 Support for alternative data sources

This part of ISO 28005 allows the SW to use previous requests, other databases and sources to populate request applications. This can be done to save ship and agent resources to submit full requests, for instance for a scheduled shipping operation.

5.5 Support for alternative information transfer mechanisms

This part of ISO 28005 does not prohibit a SW from using message formats or information transfer mechanisms other than those specified in this part of ISO 28005. This may be to support local regulations or to make use of other International Standards, e.g. trade related.

If possible, the SW implementation should attempt to integrate such messages into the clearance process by making use of the information contained in these messages where appropriate.The procedure for integrating such messages is not specified in this part of ISO 28005.

NOTE This subclause allows, for example a mix of UN/EDIFACT or other ISO messages and messages from this part of ISO 28005 to be used by one and the same SW.

5.6 Electronic communication interface requirements

5.6.1 Ship interface

The ship interface shall, at a minimum, support the “mailto” URI scheme for incoming messages.

5.6.2 SW interface

The SW interface shall, at a minimum, support a synchronous (“mailto”) and synchronous (“http”) URI schemes for incoming messages.

The SW shall, at a minimum, support “mailto” and “http” URI schemes for outgoing messages to ship.

5.7 Operational security

As the SW shall be used for transactions that can have commercial as well legal importance, it shall address the issue of information security. Security normally involves some or all of the following concepts (see Reference [15]):

— confidentiality: assurance that information is not disclosed to unauthorized individuals or systems;

— integrity: assurance that the received (or sent) information is correct and logically consistent;

— authentication: assurance that the identity of the sender (or receiver) is the one specified;

— authorization: assurance that the sender or receiver has the authority to provide or receive the information;

— availability: assurance that the system is available when needed;

— non-repudiation: assurance that the sender or receiver of information cannot deny that the information was sent or received;

— message transmission: assurance that messages through the SW are traceable and that some concept of guaranteed delivery is applied.

Necessary emphasis shall be placed on implementing technical features that address the relevant security issues.

6 Message requirements

6.1 Example of message descriptions

Messages and associated data types are described in a table as exemplified in Table 1 and Table 2 below.

Table 1 — Message: ExampleMessage

Tag	Type	Card.	Description
EPCMessageHeaderType	epc:EPCMessageHeaderType	1..1	Message header
ExampleBody	ExampleBodyType	1..1	Body of message

Table 2 — Data type: ExampleBodyType

Tag	Type	Card.	Description
PassengerList	epc:PassengerListType	0..1	Passenger list, if needed
CrewList	epc:CrewListType	0..1	Crew list

Messages and data types are descibed in the same table type. Messages consisting of nested data types require the definition of each of the data types as well as the message itself in separate tables.

In this example, a new message “ExampleMessage” is defined; it consists of two mandatory data types: the header and the body of the message. Cardinality (Card.) shows how many times the element can be repreated where 0..1 means optional, up to one time; 1..1 mean exactly once; and 1..n means any number from at least one time to infinite. The type column defines the data type. The type codes prefixed by “epc:” are defined in ISO 28005-2. Those without the prefix are defined in this part of ISO 28005, either in the same clause or in 6.3 for data types used in more than one message.

Most elements in the body of a message are optional and have cardinality from zero upwards. This allows different subtypes of message to be assembled from one and the same schema.

The description column gives a brief description of the element. If necessary, a more extensive description is given in the text of the clause.

6.2 XML schema

6.2.1 XML schema to be used

To ensure ships can interact with all SW systems that have adopted this part of ISO 28005, the following XML Schema shall be used

6.2.2 File header and end

The file needs a header with the following structure:

```
<?xml version=”1.0” ?>
<xs:schema xmlns:xs=”http://www.w3.org/2001/XMLSchema”
       xmlns:epc=”http://www.iso.org/28005-2”
     targetNamespace=”http://www.iso.org/28005-2”>

<xs:include schemaLocation=”iso28005-2.xsd”/>
```

This defines name space and includes definitions from ISO 28005-2.

After the content described below, the file is terminated by a single end of schema statement:

```
</xs:schema>
```

6.2.3 New data type definitions

This part of ISO 28005 defines some new data types in addition to those defined in ISO 28005-2. These shall be included in the schema file. The data type in question is EPCClearanceStatusType, which is defined in 7.4.

6.2.4 Data block definitions

The data blocks EPCRequestBody, EPCCancelBody, EPCReceiptBody and EPCAcknowledgeBody shall be defined. Each table line entry should be mapped to an XSD element definition as shown below.

```
<xs:complexType name=”EPCRequestBodyType”>
  <xs:sequence>
    <xs:element name=”OtherServiceRequest” type=”epc:OtherServiceRequestType”
             minOccurs=”0” maxOccurs=”unbounded”/>
          ...
    <xs:element name=”InmarsatCallNumber” type=”epc:InmarsatCallNumberType”
             minOccurs=”0”/>
    <xs:element name=”NameofMaster” type=”epc:NameofMasterType” minOccurs=”0”/>
          ...
    <xs:any processContents=”lax” minOccurs=”0” maxOccurs=”unbounded”/>
  </xs:sequence>
</xs:complexType>
```

The structure is given directly from the information in the table where minOccur and maxOccur are used to define cardinality where this is not exactly one.

6.2.5 Message definitions

The actual definition of the message format shall be in accordance with the XSD statements shown below. Note the use of the choice structure to specify that exactly one of the message bodies shall be included.

```
<xs:element name="EPCMessage">
  <xs:complexType>
    <xs:sequence>
      <xs:element name="EPCMessageHeader" type="epc:EPCMessageHeaderType"/>
      <xs:choice>
        <xs:element name="EPCRequestBody" type="epc:EPCRequestBodyType"
                    minOccurs="0"/>
        <xs:element name="EPCCancelBody" type="epc:EPCCancelBodyType"
                    minOccurs="0"/>
        <xs:element name="EPCReceiptBody" type="epc:EPCReceiptBodyType"
                    minOccurs="0"/>
        <xs:element name="EPCAcknowledgeBody" type="epc:EPCAcknowledgeBodyType"
                    minOccurs="0"/>
        <xs:element name="EPCComment" type="epc:string" minOccurs="0"/>
      </xs:choice>
      <xs:any processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>
```

6.3 Structure of the EPC message

All EPC messages use the same XML Schema and may be parsed by the same general parser software. However, the four basic types of messages: request, cancel, receipt and acknowledge, shall be processed differently, and these differences are described in the following subclauses. This subclause defines the general structure of the EPC message as well as the header (see Table 3) .

Table 3 — Message: EPCMessage

Tag	Type	Card.	Description
EPCMessageHeader	epc:EPCMessageHeaderType	1..1	Uniform message header
EPCRequestBody	EPCRequestBodyType	0..1	Request message body
EPCCancelBody	EPCCancelBodyType	0..1	Cancel message body
EPCReceiptBody	EPCReceiptBodyType	0..1	Receipt message body
EPCAcknowledgeBody	EPCAcknowledgeBodyType	0..1	Acknowledgement message body
EPCComment	epc:string	0..1	General comment to ship, port or authority to be read by human operator

The message consists of two parts: the header and the body. The message body may be one of the four optional types. The message shall contain exactly one message body. The header structure is defined in ISO 28005-2, but with the following additional requirements.

a) JournalNumber: this is mandatory in accordance with this part of ISO 28005. If the journal number is not known, e.g. as in a first request, the data portion of the tag shall be empty (no data) or an empty string.

b) Messagetype: for a port clearance request message, the message type shall be "FAL". For other service requests, various codes may be used, depending on data content. The code "Receipt" is used for an acknowledgement message and the code "ACK" is used for an acknowledgement message. The new code "CANCEL" shall be used for a cancellation message (see 7.2).

c) ReportingSystem: not used for the types of message described in this part of ISO 28005 and shall be ignored by ship and SW in this context. The code may be used for other services, such as entering or leaving named ship reporting area or for advanced notifications.

d) Version: for this version of this part of ISO 28005, the first code (M) shall be "1". The SW and the ship are required to accept all messages with this version code. Higher version code messages may be rejected through a negative receipt. Other codes (N, P) may be used by ship or SW to signal versions in internal software or for other purposes.

e) ReplyURI: this is the (copy-to) list of parties to be copied and those who shall get receipt or acknowledgement messages. A minimum of one party needs to be specified and a SW limited number of parties may be specified.

6.4 Structure of request data block

The request data block is descibed in Table 4. This is a general compilation of the information elements defined in ISO 28005-2 and presented in the same order, except the first element, which is the general service request that can be used for non-clearance related requests, when the SW supports such. All elements are optional, but with different cardinality. The ship is responsible for including the information elements which are required for clearance.

Table 4 — Data type: EPCRequestBody

Tag	Type	Card.	Description
OtherServiceRequest	epc:OtherServiceRequestType	0..n	Additional service request
Agent	epc:Agent Type	0..1	The ship's agent
Company	epc:CompanyType	0..1	The ship's operating company
InmarsatCallNumber	epc:InmarsatCallNumberType	0..1	Inmarsat call number to ship
NameOfMaster	epc:NameOfMasterType	0..1	Name of master
RegistrationPort	epc:RegistrationPortType	0..1	Port of registration
ShipID	epc:ShipIDType	0..1	Ship identity
CargoData	epc:CargoDataType	0..1	Detailed description of cargo
CargoOverview	epc:CargoOverviewType	0..1	Brief description of onboard cargo
CargoType	epc:CargoTypeContentType	0..1	Type of cargo
DGSafetyDataSheet	epc:DGSafetyDataSheetType	0..n	Safety data related to dangerous goods
DutiableCrewEffects	epc:DutiableCrewEffectsType	0..1	List of crew effects that may be dutiable
GeneralDescriptionOfDG	epc:GeneralDescriptionOfDGType	0..1	General description of dangerous cargo
ShipStore	epc:ShipStoreType	0..1	Description of ship's dutiable stores
CrewList	epc:CrewListType	0..1	Information about all crew on board
PassengerList	epc:PassengerListType	0..1	Information about passengers
PersonsOnboard	epc:PersonsOnboardType	0..1	Number of persons onboard
Certificate	epc:CertificateType	0..n	Certificate description
ShipClass	epc:ShipClassType	0..1	Class notation for ship
INFClassContent	epc:INFClassContentType	0..1	Irradiated nuclear fuel class
CurrentShipSecurityLevel	epc:CurrentShipSecurityLevelType	0..1	Current security level in port
PortCallList	epc:PortCallListType	0..1	Last ten port calls
ShipToShipActivityList	epc:ShipToShipActivityListType	0..1	Ship-to-ship activities
HasSecurityPlan	epc:HasSecurityPlanType	0..1	Approved security plan
Beam	epc:BeamType	0..1	Beam of vessel
DeadWeight	epc:DeadWeightType	0..1	Dead weight

Table 4 *(continued)*

Tag	Type	Card.	Description
DoubleBottomContent	epc:DoubleBottomContentType	0..1	Double bottom or sides indicator
GrossTonnage	epc:GrossTonnageType	0..1	Gross tonnage
IceClass	epc:IceClassType	0..1	Ship ice class
LengthOverall	epc:LengthOverallType	0..1	Length overall
NetTonnage	epc:NetTonnageType	0..1	Net tonnage
SummerDraught	epc:SummerDraughtType	0..1	Summer draught
ShipTypeContent	epc:ShipTypeContentType	0..1	Ship type code
AirDraught	epc:AirDraughtType	0..1	Air draught
ArrivalDraught	epc:ArrivalDraughtType	0..1	Arrival draught
ATA	epc:ATAType	0..1	Actual time of arrival
ATD	epc:ATDType	0..1	Actual time of departure
ATP	epc:ATPType	0..1	Actual time of passage
BulkLoadUnloadData	epc:BulkLoadUnloadDataType	0..1	Data required for safe loading and unloading
CallPurpose	epc:CallPurposeType	0..1	Purpose of call
DepartureDraught	epc:DepartureDraughtType	0..1	Departure draught
EntryPosition	epc:EntryPositionType	0..1	Time and position for entry to ship reporting
ETA	epc:ETAType	0..1	Estimated time of arrival
ETD	epc:ETDType	0..1	Estimated time of departure
ETP	epc:ETPType	0..1	Estimated time of passage
ExitPosition	epc:ExitPositionType	0..1	Time and position for exit from ship reporting
LastPortOfCall	epc:LastPortOfCallType	0..1	Last port of call
Location	epc:LocationType	0..1	Identification of a location
NavigationalStatusContents	epc:NavigationalStatusContentsType	0..1	Navigational status
NextPortOfCall	epc:NextPortOfCallType	0..1	Next port of call
NextReportTime	epc:NextReportTimeType	0..1	Time of next report
OBOLoadUnloadData	epc:OBOLoadUnloadDataType	0..1	Data required for safe loading and unloading of OBO
PeriodOfStay	epc:PeriodOfStayType	0..1	Period of stay
PortOfArrival	epc:PortOfArrivalType	0..1	Arrival port
PortOfDeparture	epc:PortOfDepartureType	0..1	Departure port
RadioCommunications	epc:RadioCommunicationsType	0..1	Radiocommunication active
ROBBunkers	epc:ROBBunkersType	0..1	Bunkers remaining onboard
ShipDefects	epc:ShipDefectsType	0..1	Any defects of important ship equipment
ShipStatus	epc:ShipStatusType	0..1	Vessel status information
VoyageNumber	epc:VoyageNumberType	0..1	Voyage identification code
VoyageDescription	epc:VoyageDescriptionType	0..1	Brief description of voyage
WayPointList	epc:WayPointListType	0..1	Way-point list
WeatherInformation	epc:WeatherInformationType	0..1	Weather information as observed
BallastStatus	epc:BallastStatusType	0..1	Status of ship's ballast water when in port
WasteDisposalRequirements	epc:WasteDisposalRequirementsType	0..1	Ship's requirements for waste disposal
WasteInformation	epc:WasteInformationType	0..1	Waste information

6.5 Structure of cancel data block

Table 5 defines the contents of the cancel data block. It only contains a boolean flag that needs to be true for the cancellation to be effected.

Table 5 — Data type: EPCCancelBody

Tag	Type	Card.	Description
Cancel	epc:boolean	1..1	Confirm cancellation

6.6 Structure of receiptdata block

Table 6 defines the content of the receipt data block. The first element is a flag specifying whether or not the request will be processed. If it is not processed, the comment field in the message gives a human readable explanation of the reason. The RequestErrorCode will give an error code as defined in 7.3. The port security level shall always be returned according to the ISPS code and the request status codes gives the list of authorities that may return acknowledgements as well as the status of other service requests if these were included.

Table 6 — Data type: EPCReceiptBody

Tag	Type	Card.	Description
RequestProcessed	epc:boolean	1..1	Flag specifying if request will be processed (true)
RequestErrorCode	epc:token	1..1	Error code
CurrentPortSecurityLevel	epc:CurrentPortSecurityLevelType	1..1	Current security level in port
EPCClearanceStatus	EPCClearanceStatusType	1..n	Status of the different authorities' authorization
RequestStatus	epc:RequestStatusTypeContentType	0..n	Status of a service request

6.7 Structure of acknowledgement data block

The acknowledgement data block only lists (normally only one) acknowledgement status from one authority (see Table 7). The ship shall compare this with the list given in the receipt message.

Table 7 — Data type: EPCAcknowledgeBody

Tag	Type	Card.	Description
EPCClearanceStatus	EPCClearanceStatusType	1..n	Status of the different authorities' authorization (normally only one).

7 New data types

7.1 New data types — General

This clause contains definitions of new or modified data types with ISO 28005-2 as a baseline. Each subclause defines a new or modified data type. The syntax is the same as in ISO 28005-2.

7.2 epc:MessageTypeContentType — New code values

This code shall get one addition value (see Table 8).

Table 8 — New message types

Message code	Content of message	Normative reference
CANCEL	Cancellation of a previous request	

7.3 RequestErrorCode — Request error codes

This data element is a numeric token and may have one of the following codes (see Table 9).

Table 9 — Error codes

Message code	Content of message
0	Request is accepted and will be processed
1	SW does not accept multiple request updates. This request will be ignored and the original request will continue to be processed.
2	Too many copy-to entries.
3	The request did not contain enough information to continue processing. The request will be ignored.

7.4 EPCClearanceStatusType — Data type for clearance status

This data type is used to list authorities, which need to clear a ship and from which the ship needs to receive a clearance acknowledgement.

```
<xs:complexType name="EPCClearanceStatusType">
   <xs:sequence>
      <xs:element name="Authority" type="epc:token"/>
      <xs:element name="UsesSW" type="epc:boolean"/>
      <xs:element name="RequestStatus" type="epc:RequestStatusType"/>
      <xs:element name "MissingTag" type="epc:string"
                  minOccur="0" maxOccur="unbounded"/>
   </xs:sequence>
</xs:complexType>
```

The authority code is assigned by the SW and is a general token, which is used consequently for this authority. The UsesSW flag is a boolean that is true if the acknowledgement will be sent through the SW. If false, the acknowledgement may be given by other means, normally described in the comment field of the next tag. The RequestStatus gives the current status of the request with a possibility to give a comment. The status codes used are:

— Discarded: not enough information to send the request to this authority. More information is needed;

— Pending: the request has been forwarded to this authority. The ship needs to await an acknowledgement from authority;

— Accepted: the request has been processed and is accepted. No further acknowledgement will be received;

— NotAccepted: the request has been processed and was not accepted. The comment field describes a reason. A new request needs to be sent.

— AcceptedWithConditions: the request was accepted, but with conditions as explained in comments. No further acknowledgement will be sent.

— MissingTag: this is an optional list of missing infromation elements for a certain type of clearance. Some SW systems may be able to return this for clearances that have not been granted. Each element will list one missing tag in xpath format, always starting with "EPCRequestBody/".

Annex A
(informative)

Implementation advice for single window

A.1 Service-oriented architecture(SOA)

In service-oriented architecture (SOA), the concept of service can be understood as a software component that executes a business process from a business point of view. In SOA, services are loosely coupled, platform independent and neutral interface. Therefore, the effects on other services are minimized when any particular service is changed. Because of this, a system based on SOA is agile in dealing with business changes and its components can be reused in many different combinations. The main features of SOA include:

a) Model-driven Development Methodology:

   — developing a software system is an abstraction of complicated business;

   — process of making abstract business implementable;

   — use of UML (Unified Modelling Language) as a modelling language.

b) Service-oriented Development Methodology:

   — "service orientation" is based on the "separate of concerns" in software engineering theory. It is based on the concept of dividing and classifying a big problem into individual areas of interest;

   — services are platform independent and accessed by applications in a standardized way;

   — services are reusable and loosely coupled;

   — services can be combined.

Figure A.1 shows the conceptual configuration of SOA. SOA is based on a traditional request/response mechanism. The service consumer calls service providers through a common service bus called ESB. Consumers request specific services through a standard set of "request" communication protocols across the ESB. When the services complete, the results are communicated to the consumer using another set of standard "response" protocols. More explanation of Figure A.1 is given below.

— Access service is a component supporting the connection between a SW system and users or external organizations. This service is based on a standard communication protocol.

— Interaction service is a service for transactions among unit modules or between unit modules and the service repository within a SW system.

— Business application service is the execution of service modules implemented within a SW system. Examples in a SW for maritime transport business include port arrival/departure, application/approval, cargo report/approval and dangerous cargo report/approval.

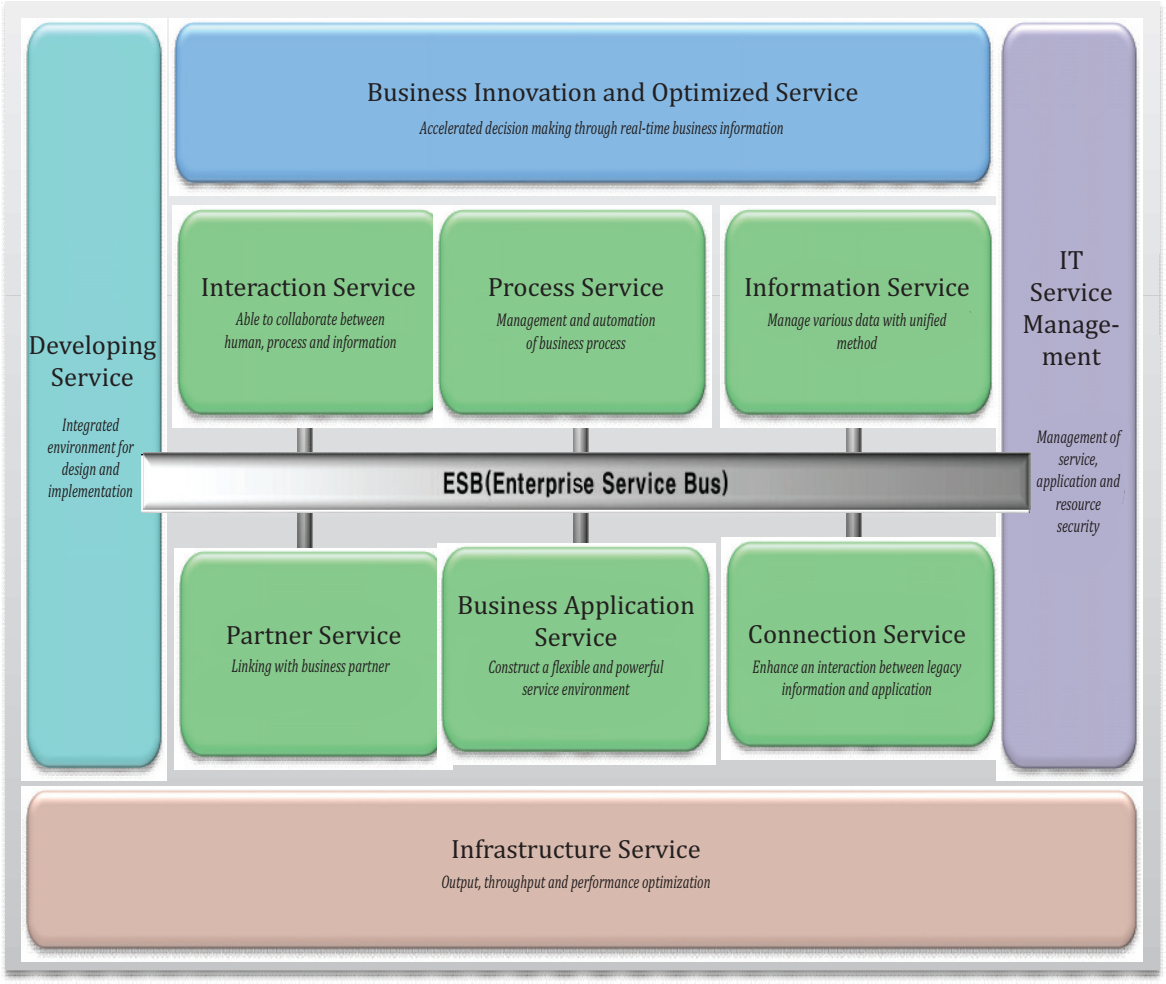

Figure A.1 — SOA conceptual configuration

A.2 Web service

See Figure A.2.

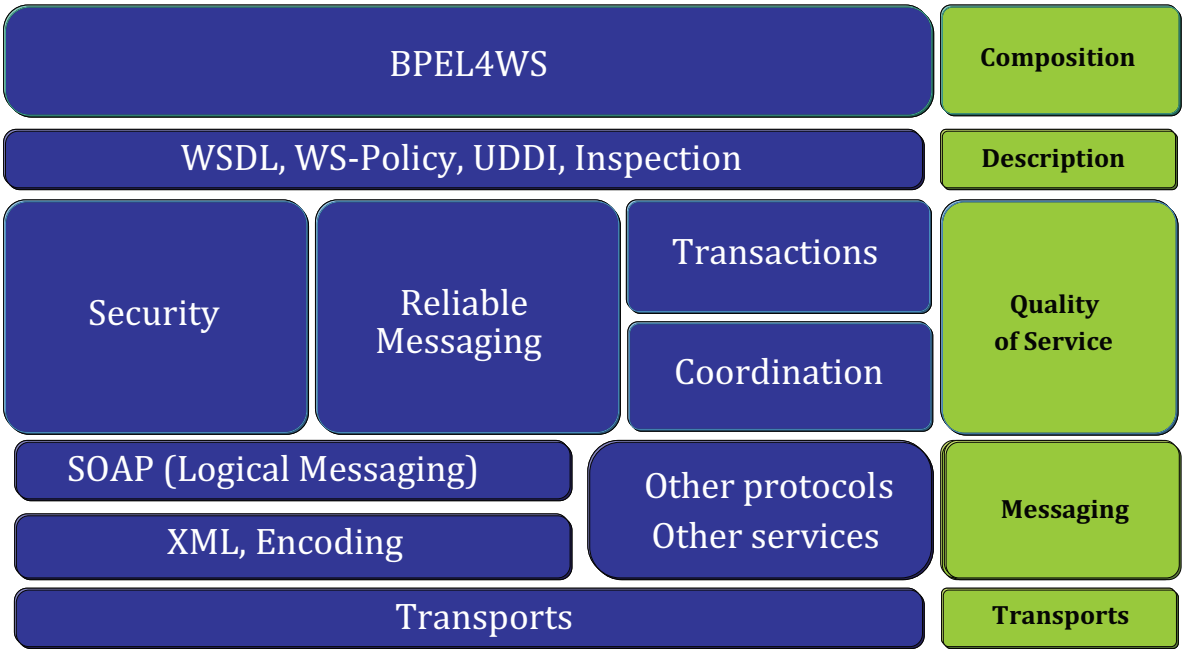

Figure A.2 — Web service standard

a) WSDL (WEB Service Description Language)

— Entry Point for service provider;

— used as a Service Endpoint or End Point;

— provision of End Point Interface definition, physical service location (address) definition.

e) SOAP (Simple Object Access Protocol)

— XML-based protocol for systematic information exchange in a distributed environment;

— transport-independent, can be combined to such protocols as HTTP, JMS, SMTP, FTP;

— designed for communication among applications and on the Internet;

— based on the Internet and HTTP, and can be used in combination with security policies.

A.3 JAVA

A.3.1 Overview

Java is an Object Oriented Language developed in the USA in 1990. JAVA gained prominent attention with the emergence of the Internet and the Web.

A.3.2 Features

a) Java was developed based on C++, but removed the difficult concepts and constructs from that language.

b) Object-oriented: in object orientation, the focus is on object and functions manipulating objects rather than steps.

c) Operable in a distributed environment: Java has a library that supports many protocols operating in a TCP/IP network environment, such as HTTP. As a result, it can control objects in a remote computer using URL (Uniform Resource Locator).

d) Platform independent: if there is a Java virtual machine, Java can be executed anywhere regardless of a system.

e) Supporting multi threads: JAVA can support multiple, simultaneous threads within a single program. In other words, a single Java program can be composed of multiple thread programs, and each thread can independently perform another task.

A.3.3 MVC pattern

MVC is the abbreviated term for Model-View-Control. MVC means to develop an application in a division of View, Model and Control. Hereby, View for presentation to users, Model for processing business logic and Control for managing Model and View. The MVC pattern is used to avoid difficulties in development and maintenance of complicated source codes resulting from the effort to write all the functions within an application. The advantage of the MVC pattern is to realize object-oriented and component-based methodologies.

A.3.4 EJB (Enterprise JavaBeans)

Enterprise JavaBeans is a component architecture for developing and sharing distributed and object-oriented Java applications. By providing various services supporting extensible application server components, it enables developers to write business applications as components.

A.4 Spring framework

A.4.1 Overview

Spring framework provides functions needed in enterprise applications. Because it supports multiple functions provided by J2EE, Spring framework is becoming popular as a replacement for J2EE.

A.4.2 Features

a) It is a lightweight container. It is a container having Java objects. It manages the lifecycle of these Java objects from creation to disposal and can bring necessary objects for use.

b) It supports DI (Dependency Injection) pattern. It can configure dependency among objects using configuration files. Therefore, objects do not need to create or search dependent objects by themselves.

c) It supports AOP (Aspect Oriented Programming). Because it supports AOP by itself, Spring framework can divide and apply functions that are commonly needed in various modules. Examples include transaction, logging and security

d) It supports POJO (Plain Old Java Object). Java objects stored in Spring framework do not need to implement specific interfaces or inherit particular classes. Therefore, existing codes can be used without modification.

e) It provides a consistent method for processing transactions. Because it inputs transaction-related information through a configuration file, Spring framework can use the same code in multiple environments regardless of transaction implementation.

f) It supports various API that are related to continuity. It supports interoperation with widely used libraries related to database such as JDBC, iBATIS, Hibernate, JPA, JDO.

g) It supports interoperability with various APIs. Spring framework enables developers to use various APIs needed in developing enterprise applications (such as JMS, mail and scheduling) through a configuration file

A.5 Ajax (Asynchronous JavaScript +XML)

A.5.1 Overview

It is an asynchronous communication technology for exchanging XML data between client and server using Asynchronous JavaScript and XML. In traditional web applications, users can see the result on a browser only after a response is sent from the server. With AJAX a user can see the result on a browser in the process of sending a request and can check the result without page shift upon receiving a response from a server.

A.5.2 Features

a) It can get data simply without page shift, therefore can improve user interface. For example, in a certain web mapping service application, it can display location information on a screen through a mouse drag without page shift.

b) Using AJAX, office programs or calendar programs can be developed on the Web.

c) It does not work in a browser that supports JavaScript because it is composed of JavaScript.

A.6 C#

A.6.1 Overview

C# is a programming language developed to strategically support .NET platform. It is based on C++ and further developed from C++ by standardizing C++ syntax. Therefore, it completely covers C and C++, and can use existing COM components easily.

A.7 Net framework

A.7.1 Overview

".NET" refers to an ideal development environment that supports everything needed in developing programs. For example, in developing a program using C language, various necessary components should be collected individually. However, .NET provides a language, development tools, a library, number relevant technologies, etc. which are needed in development. In short, it refers to a type of environment for easier development.

A.7.2 Features

a) Usually, codes written in each programming language are translated into machine language at "compile" time. In .NET, they are translated into an intermediate language. That language can be considered a pre-machine language that can be translated into machine language easily. The resulting file compiled with intermediate language in .NET is called Assembly. In C#, they are equivalent to .exe files or .dll files.

b) Assembly is composed of: a) metadata that have all the information on intermediate language and class, b) a manifest that has information on Assembly itself, and c) resources that are data used by programs. The assembly used can be classified into private assembly and public assembly. Private assembly refers to a simple library that is used when needed. Public assembly refers to a library commonly shared by a system by registering it to a directory in a system

c) Because .NET programs can be operated in any operating system as long as .NET Framework is provided, it can be platform independent. As long as there is a compiler for translating intermediate language into machine language, it can be executed in any platform and is called JIT (Just In Time Compiler).

A.7.3 .Net framework component

a) Class Library: .NET Framework supports various libraries necessary in development and execution. It supports the environment needed for developing databases, Web Application, Graphic, XML, Web Services.

b) Common Language Runtime (CLR): CLR provides an execution environment. It is a virtual operating system that loads, dynamically compiles, and executes programs developed by languages supporting .NET, such as VB.NET, C#, C++, Jscript.NET, and manages memories.

Annex B
(informative)

Development of a single window

B.1 Development procedure

The ultimate goal of this part of ISO 28005 is to facilitate efforts by IMO member states to implement SW systems.

B.2 Caution

There are certain areas that need cautious attention in implementing a SW. They are identified as follows:

a) Unified standard electronic document

Processes relevant to SWs include general declaration, cargo declaration and crew/passenger list. All electronic and paper documents used in the government agencies participating in SW should be analysed and listed by agencies. Only essential data elements will be collected in consideration of usage frequency, importance and connectivity. All government agencies participating in SW should be able to agree on the collected data elements at this stage.

b) Simplified work processing

Government agencies participating in SW should define their work processes related to SW. Each agency should describe its work processes in the form of a graphical diagram. By analysing the work processes, redundant or unnecessary processes may be identified and removed. In addition, by redefining works, work processes of each agency are modified. In this stage, it is highly likely that work processes of each agency are changed with possible amendments to relevant regulations.

c) Migration to existing information system

Some government agencies might have information systems for processing whole or part of SW services electronically. As electronic documents and work processes possibly change, the existing information systems can need to be modified with a possible burden of financial costs. Therefore, migration to an existing information system should be considered when electronic documents and work processes are redefined.

d) Minimization of user interface change

It is possible that users can be confused when work processes are transitioned to a SW. In case electronic documents or communication protocols are changed, a relevant adapter should be developed and distributed; otherwise, relevant information needed for the development of an adapter should be prepared and distributed to the users. Another alternative would be the development of a web-based system for easy use by users.

B.3 Single window methodology

Since the SW system is a software system, this part of ISO 28005 recommends a methodology based on a well-known development process. That process has five phases: plan (planning), analysis, design, implementation, test and delivery. These phases are shown in Figure B.1, which also shows the detailed tasks for each of the five phases. The five phases are presented in Tables B.1 to B.5.

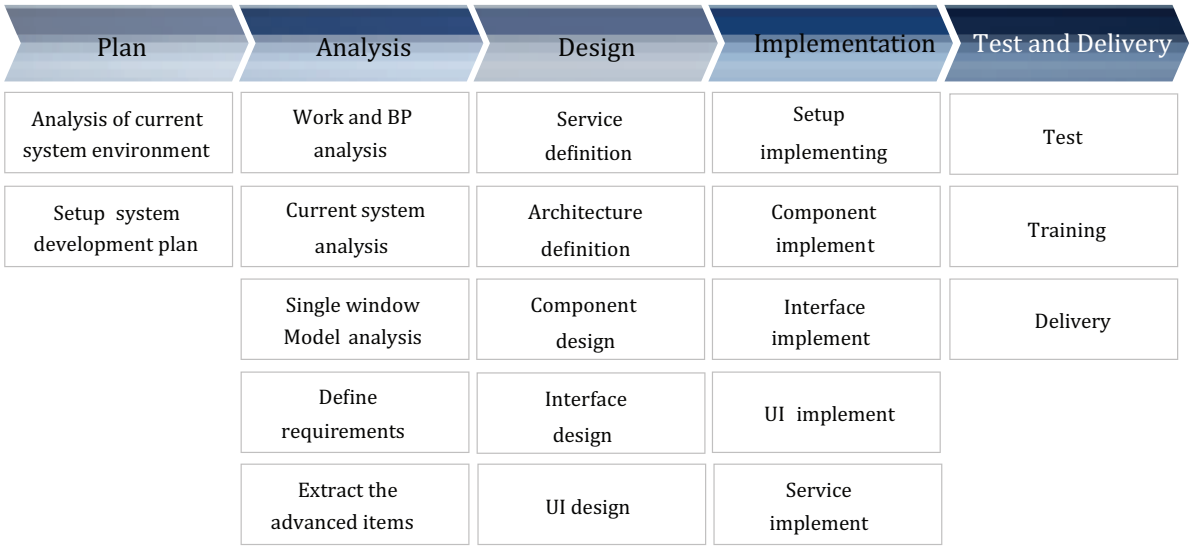

Figure B.1 — SW service development and implementation methodology

B.3.1 Development methodology detailed

Table B.1 — Planning

No.	Phase	Task	Remarks
1	Understand system environment	— Understand environment related to system development — identify functions, interests and issues of each entity	
2	Establish development plan	— Establish development schedule — Form a project team — Define roles of team members	

Table B.2 — Analysis

No.	Phase	Task	Remarks
1	Analyse business and business process	— Analyse existing target business and business process — Conduct UseCase modelling — Derive services and processes to be implemented — Identify functions, interests and issues of each entity	Analyse and list business flows occurring in maritime transport, such as customs, inspection, transport, storage and port arrival/departure
2	Analyse current system	— Analyse existing information systems — Analyse their functions and interests	— Analyse current information system by entities and points — Understand issues and requirements — Define information improvement tasks
3	Analyse SW model	— Analyse SW model — Analyse best-practice cases	— Set application scope based on country's environment (business, law, informatization, etc.)
4	Define requirements	— Collect requirements: stakeholder interview — Derive system requirements	— Survey government agencies and users — Define by dividing by business areas
5	Derive improvement measures	— Derive issues and improvement points for current processes — Derive major issues through the analysis of requirements — Derive improvement measures and tasks	— Target model is a SW system — Analyse gap with target model — Identify measures to minimize the gap

Table B.3 — Design

No.	Phase	Task	Remarks
1	Define services	— Define business processes as services — Design services to be implemented	— Business services such as port arrival/departure, cargo report exist — Application services such as document relay, document conversion and document retrieval for business services exist
2	Define architecture	— Design software architecture — Select base framework — Design overall system architecture, components, modules and database	— Measure to encapsulate components — Measure to reuse components — Selection of programming language
3	Design component	— Design components by independent functions — Define relevant component specification — Define in details up to class level	
4	Design interface	— Define parameters exchanged between components — Define and design interchange interface	— Need to define interface among internal modules or with external organizations
5	Design UI	— Define and design user interface — Design in a Web-based environment	— The goal is to maximize user convenience and accessibility — Guarantee scalability by applying advanced Web technologies

Table B.4 — Implementation

No.	Phase	Task	Remarks
1	Establish development environment	— Select development environment and tools — Configure database, Web environment — Define development methodology for shared work	— Development methodology: Define program Naming, parameter Naming, annotation processing method
2	Implement component	— Implement component by unit function — Implement Web in a way to interoperate with server component	— Correct syntactic errors on source codes and compile errors — Runtime errors are corrected at the time of unit test.
3	Implement interface	— Implement according to interface design specification — Interconnect relevant components	—
4	Implement User Interface	— Design screen and interconnect with components after implementation	
5	Implement service	— Assemble business components and data modules — Service assembly and implementation according to business requirements	— The goal is to maximize user convenience and accessibility — Guarantee scalability by applying advanced Web technologies

Table B.5 — Test and delivery

No.	Phase	Task	Remarks
1	Test	— Establish test plan — Conduct unit test — Conduct combined test	— Correct unit module errors through unit test — Measure requirements fulfilment and performance through combined test
2	Training	— Develop a guide for system user and operator — Train users and operators	
3	Operation	— Install in a running system	

B.3.2 Methodology deliverables

See Table B.6.

Table B.6 — Methodology deliverables

No.	Phase	Activity	Task	Deliverables
1	Plan	Understand system environment	Identify relevant systems	Analysis of existing systems
		Establish development plan	Team formation, division of labor and development schedule	Development plan
2	Analysis	Analyse business and business process	Analyse current businesses Business modeling	Business analysis report Definition of business
		Analyse current system	System analysis	System analysis report
		Analyse SW model	Analysis of SW model Analysis of best-practice cases	Report on the analysis of SW model Report on benchmarking cases
		Define requirements	Stakeholder survey Stakeholder interview Requirements specification	Survey result Analysis report on interview Requirements specification
		Derive improvement measures	Define future model	Definition of future model
3	Design	Define services	Service specification Service design	Service specification Service design
		Define architecture	Architecture specification Architecture design Database design	Architecture specification Architecture design Database design
		Design component	Component specification Component design	Component specification Component design
		Design interface	Interface specification Interface design	Interface specification Interface design
		Design User Interface	UI design UI design	UI design UI design
4	Implementation	Establish development environment	Define development environment	Definition of development environment
		Implement component	Implement components	Components codes
		Implement interface	Implement interface	Interface codes
		Implement User Interface	Implement UI	UI codes
		Implement services	Implement services	Services implementation codes

Table B.6 *(continued)*

No.	Phase	Activity	Task	Deliverables
5	Test and operation	Test	Prepare test cases	Test cases
			Conduct unit test	Result of unit test
			Design combined test	Combined test specification
			Conduct combined test	Result of combined test
		Training	Prepare user manual	User manual
			Prepare operator manual	operator manual
			Train users	Report on user training
			Train operators	Report on operator training
		Operation	Takeover test	Result of takeover test
			System release	Report on system release

B.4 System architecture

In principle, a SW system for maritime transport business should be independent of the hardware system, scalable in its structure, and, to the extent possible, reusable. It shall also define all the necessary business processes and low-level functions as simple service components. These components are stored in a service repository. They can be used as is, or composed (assembled) into more complex services as needed. Users and other organizations can access this repository using standard communication protocols, such as TCP/IP, HTTP, WEB Service and SMTP. If the SW system is developed as a Web-based system, which is the recommendation of this part of ISO 28005, it will contain a Web server. To process the data transmitted to a SW system from this server, this part of ISO 28005 recommends an Enterprise Service Bus (ESB). The set of services needed to process that data, and the sequence in which they are executed, are determined by additional external logic typically written in Java or any other object-oriented language.

Bibliography

[1] ISO 6422-1, *Layout key for trade documents — Part 1: Paper-based documents*

[2] ISO 8440, *Location of codes in trade documents*

[3] ISO 8601, *Data elements and interchange formats — Information interchange — Representation of dates and times*

[4] ISO 7372, *Trade data interchange — Trade data elements directory*

[5] ISO 9735 (all parts), *Electronic data interchange for administration, commerce and transport (EDIFACT) — Application level syntax rules (Syntax version number: 4, Syntax release number: 1)*

[6] ISO/TS 20625, *Electronic data interchange for administration, commerce and transport (EDIFACT) — Rules for generation of XML scheme files (XSD) on the basis of EDI(FACT) implementation guidelines*

[7] ISO/TS 15000-5, *Electronic Business Extensible Markup Language (ebXML) — Part 5: ebXML Core Components Technical Specification, Version 2.01(ebCCTS)*

[8] ISO 14533-1, *Processes, data elements and documents in commerce, industry and administration — Long term signature profiles — Part 1: Long term signature profiles for CMS Advanced Electronic Signatures (CAdES)*

[8] ISO 14533-2, *Processes, data elements and documents in commerce, industry and administration — Long term signature profiles — Part 2: Long term signature profiles for XML Advanced Electronic Signatures (XAdES)*

[9] ISO 17369, *Statistical data and metadata exchange (SDMX)*

[10] IMO, *Convention on Facilitation of International Maritime Traffic (FAL)*, Adoption: 9 April 1965, Entry into force: 5 March 1967

[11] IMO FAL 36/5/2, *Justification for Single Window Guidelines for Maritime Transport*

[12] IMO FAL 37/5/2, *Proposals for Single Window Guideline for Maritime Transport in Terms of Technical Aspects*

[13] FAL.5/Circ.35, *Revised IMO Compendium on facilitation and electronic business*, 9 September 2011

[14] UN/CEFACT Recommendation No. 33, *Recommendation and Guidelines on Establishing a Single Window*

[15] IMO Circular FAL.5/Circ.36, *Guidelines for Setting up a Single Window System in Maritime Transport*, 9 November 2011

[16] ISOC RFC 3986:2005, *Uniform Resource Identifier (URI): Generic Syntax*

[17] ISOC RFC 3305, *Report from the Joint W3C/IETF URI Planning Interest Group: Uniform Resource Identifiers (URIs), URLs, and Uniform Resource Names (URNs): Clarifications and Recommendations*

[18] *International Ship and Port Facility Security Code (ISPS)*, 2004, implemented through the *International Convention for the Safety of Life at Sea (SOLAS), Chapter XI-2 Special measures to enhance maritime security*

ICS 47.020.99,35.240.60

Price based on 28 pages

This page deliberately left blank

British Standards Institution (BSI)

BSI is the independent national body responsible for preparing British Standards and other standards-related publications, information and services. It presents the UK view on standards in Europe and at the international level.

BSI is incorporated by Royal Charter. British Standards and other standardisation products are published by BSI Standards Limited.

Revisions

British Standards and PASs are periodically updated by amendment or revision. Users of British Standards and PASs should make sure that they possess the latest amendments or editions.

It is the constant aim of BSI to improve the quality of our products and services. We would be grateful if anyone finding an inaccuracy or ambiguity while using British Standards would inform the Secretary of the technical committee responsible, the identity of which can be found on the inside front cover. Similary for PASs, please notify BSI Customer Services.

Tel: +44 (0)20 8996 9001 Fax: +44 (0)20 8996 7001

BSI offers BSI Subscribing Members an individual updating service called PLUS which ensures that subscribers automatically receive the latest editions of British Standards and PASs.

Tel: +44 (0)20 8996 7669 Fax: +44 (0)20 8996 7001
Email: plus@bsigroup.com

Buying standards

You may buy PDF and hard copy versions of standards directly using a credit card from the BSI Shop on the website **www.bsigroup.com/shop.** In addition all orders for BSI, international and foreign standards publications can be addressed to BSI Customer Services.

Tel: +44 (0)20 8996 9001 Fax: +44 (0)20 8996 7001
Email: orders@bsigroup.com

In response to orders for international standards, BSI will supply the British Standard implementation of the relevant international standard, unless otherwise requested.

Information on standards

BSI provides a wide range of information on national, European and international standards through its Knowledge Centre.

Tel: +44 (0)20 8996 7004 Fax: +44 (0)20 8996 7005
Email: knowledgecentre@bsigroup.com

BSI Subscribing Members are kept up to date with standards developments and receive substantial discounts on the purchase price of standards. For details of these and other benefits contact Membership Administration.

Tel: +44 (0)20 8996 7002 Fax: +44 (0)20 8996 7001
Email: membership@bsigroup.com

Information regarding online access to British Standards and PASs via British Standards Online can be found at **www.bsigroup.com/BSOL**

Further information about British Standards is available on the BSI website at **www.bsi-group.com/standards**

Copyright

BSI

389 Chiswick High Road London W4 4AL UK

Tel +44 (0)20 8996 9001
Fax +44 (0)20 8996 7001
www.bsigroup.com/standards

raising standards worldwide™