

INTERNATIONAL STANDARD

NORME INTERNATIONALE



**Maritime navigation and radiocommunication equipment and systems –
Data interfaces –
Part 2: Secure communication between ship and shore (SECOM)**

**Matériels et systèmes de navigation et de radiocommunication maritimes –
Interfaces de données –
Partie 2: Communications sécurisées entre le navire et la terre (SECOM)**

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 47.020.70

ISBN 978-2-8322-3802-8

Warning! Make sure that you obtained this publication from an authorized distributor. Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.
--

CONTENTS

FOREWORD.....	13
INTRODUCTION.....	15
1 Scope.....	16
2 Normative references	16
3 Terms, definitions and abbreviated terms	17
3.1 Terms and definitions.....	17
3.2 Abbreviated terms.....	21
4 General description of SECOM	21
4.1 General.....	21
4.2 Information service interface	22
4.3 Information security	23
4.3.1 Measures.....	23
4.3.2 SECOM PKI.....	23
4.3.3 Communication channel security	24
4.3.4 Data protection	24
4.3.5 Certificate revocation status	26
4.4 Service discoverability	26
4.5 Structure of this document	27
5 SECOM information service interface	27
5.1 General.....	27
5.2 How to read descriptions of service interface definition	28
5.3 Service technology and service transportation protocol.....	29
5.4 Service interface versioning	30
5.5 Pagination	30
5.6 Common information objects and data types	30
5.6.1 General	30
5.6.2 Basic data types	31
5.6.3 SECOM_ExchangeMetadataObject.....	31
5.6.4 Transfer of public key	32
5.6.5 PaginationObject	34
5.6.6 ContainerTypeEnum	35
5.6.7 SECOM_DataProductType	35
5.6.8 SECOM_ResponseCodeEnum.....	36
5.6.9 AckRequest Enum	36
5.6.10 Common HTTP response codes.....	37
5.6.11 Well-known text – WKT.....	37
5.6.12 Universally Unique Identifier – UUID.....	38
5.6.13 UN/LOCODE	39
5.7 Service interface definitions	39
5.7.1 General	39
5.7.2 Service interface – Upload.....	40
5.7.3 Service interface – Upload Link	46
5.7.4 Service interface – Acknowledgement.....	51
5.7.5 Service interface – Get	55
5.7.6 Service interface – Get Summary	60
5.7.7 Service interface – Get By Link.....	64

5.7.8	Service interface – Access.....	66
5.7.9	Service interface – Access Notification	69
5.7.10	Service interface – Subscription	71
5.7.11	Service interface – Remove Subscription.....	76
5.7.12	Service interface – Subscription Notification	79
5.7.13	Service interface – Capability	81
5.7.14	Service interface – Ping.....	84
5.7.15	Service interface – EncryptionKey	86
5.7.16	Service interface – PublicKey	92
6	SECOM communication channel security.....	96
6.1	General.....	96
6.2	Secure transfer	96
6.2.1	Secure communication channel	96
6.2.2	Authentication procedure	97
7	SECOM data protection	97
7.1	General.....	97
7.2	Data compression and packaging	98
7.3	Data authentication and signing	98
7.3.1	General	98
7.3.2	Data formats and standards for digital signatures, keys and certificates	98
7.3.3	Creation of digital signature	99
7.3.4	Creation of envelope signature	100
7.3.5	Verification of digital signature.....	101
7.3.6	Verification of envelope signature	102
7.3.7	Example of commands for data authentication	102
7.4	Data encryption.....	103
7.4.1	General	103
7.4.2	Encryption algorithm	103
7.5	Creation and transfer of encryption key.....	103
7.5.1	General	103
7.5.2	SECOM encryption key management.....	104
7.5.3	Generate encryption key.....	105
7.5.4	Sign the protected encryption key	105
7.5.5	Transfer of the encryption key	105
7.5.6	Example	106
8	SECOM PKI.....	106
8.1	General.....	106
8.2	Scheme	107
8.2.1	General	107
8.2.2	Scheme administrator	107
8.2.3	Data servers	107
8.2.4	Data clients	107
8.2.5	Procedure.....	108
8.3	Generation of public and private key	108
8.4	Certificate signing request	109
8.5	Certificate revocation	109
8.5.1	General	109
8.5.2	CRL – Certificate revocation list.....	109
8.5.3	OCSP – Online certificate status protocol	109

8.6	SECOM PKI service interface	110
8.6.1	General	110
8.6.2	Service interface – CSR	110
8.6.3	Service interface – GetPublicKey	113
8.6.4	Service interface – CRL	115
8.6.5	Service interface – OCSP	116
8.6.6	Service interface – Revoke	119
9	SECOM service discovery service interface	121
9.1	General	121
9.2	Service interface – Search service	121
9.2.1	Specification	121
9.2.2	Data exchange model	122
9.2.3	REST design	124
10	SECOM error cases	125
10.1	Error cases	125
10.2	General	126
10.3	Message integrity	126
10.4	Data integrity	126
10.5	Transport confidentiality	126
10.6	Data protection	127
10.7	Service identity	127
10.8	Client identity	127
10.9	Client authorization	128
10.10	Bandwidth optimization	128
10.11	Large message transfer	128
10.12	Closed loop communication	129
10.13	Service discoverability	130
10.14	Information push	130
10.15	Information pull	130
10.16	Subscribe to data	131
10.17	Service information	131
10.18	Service condition	131
11	Test methods and expected results	132
11.1	General	132
11.2	Communication channel security test	132
11.3	Data protection test	133
11.3.1	Data Compression and packaging	133
11.3.2	Data authentication and signature	133
11.3.3	Encryption	133
11.3.4	Digital signature test	133
11.4	SECOM ship/shore test	133
11.4.1	General	133
11.4.2	Prerequisites SECOM ship/shore EUT	136
11.4.3	Upload data	136
11.4.4	Download data	137
11.5	SECOM Information Service test	139
11.5.1	General	139
11.5.2	Prerequisites SECOM information service EUT	140
11.5.3	Access	140

11.5.4	Access notification.....	141
11.5.5	Acknowledgement.....	141
11.5.6	Capability	142
11.5.7	EncryptionKey	143
11.5.8	EncryptionKey Notification	143
11.5.9	Get	144
11.5.10	Get By Link.....	145
11.5.11	Get Summary	146
11.5.12	Get Public Key.....	147
11.5.13	Upload Public Key	147
11.5.14	Ping.....	148
11.5.15	Subscription	148
11.5.16	Subscription Notification	149
11.5.17	Remove Subscription	149
11.5.18	Upload.....	150
11.5.19	Upload Link	151
11.6	SECOM PKI Service test.....	152
11.6.1	Prerequisites PKI EUT	152
11.6.2	CRL.....	153
11.6.3	OCSP	153
11.6.4	Revoke	154
11.6.5	CSR	154
11.6.6	GetPublicKey.....	154
11.7	SECOM Service Discovery test.....	155
11.7.1	General	155
11.7.2	Prerequisites Service Discovery EUT.....	155
11.7.3	Search service – By geometry	155
11.7.4	Search service – Without specified search criteria	156
Annex A	(normative) REST service interface definitions.....	157
A.1	Purpose	157
A.2	SECOM information service REST interface definition	157
A.3	SECOM PKI service REST interface definition	157
A.4	SECOM discovery service REST interface definition	157
Annex B	(informative) Operational use cases and profiles.....	158
B.1	Purpose	158
B.2	Use cases and service interface profiles	158
B.2.1	UC-1 Ship shares route plan with service providing enhanced monitoring	158
B.2.2	UC-2 Pilot routes	159
B.2.3	UC-3 Route optimization.....	160
B.2.4	UC-4 Enhanced monitoring service requests route plan from/for ship for monitoring	161
B.2.5	UC-5 Discover service instance to consume	162
B.2.6	UC-6 Chart (ENC) updates	163
B.2.7	UC-7 navigational warning service.....	164
B.2.8	UC-8 Updates for detailed bathymetry and tidal and water level forecasts	166
Annex C	(informative) Message exchange patterns.....	167
C.1	Purpose	167

C.2	Message exchange pattern	167
C.2.1	Generic message exchange patterns	167
C.2.2	Alternative and error sequences	170
Annex D	(informative) Guidance on implementation	171
D.1	Purpose	171
D.2	On ship	172
D.3	On shore	173
D.4	Service composition	174
D.5	Private side security	175
D.6	SECOM PKI	176
D.6.1	General	176
D.6.2	Structure and Functionality	176
D.6.3	Identity management	177
D.6.4	Public Key Infrastructure	180
D.6.5	Authentication and authorization for web services	185
D.6.6	Profile "Basic Requirements"	186
D.7	SECOM service discovery	186
D.7.1	Example 1: geometry combined with serviceType search	186
D.7.2	Example 2: Search with AND/OR condition	188
Annex E	(informative) Use of white list	190
E.1	Purpose	190
E.2	Authorization to access data	190
E.3	Access control list	191
E.4	Authorization based on predefined rules or list	191
E.5	Manually updated list	192
E.6	Rule based handling on request to information (rule based authorization)	192
E.7	Rule based request for information	192
E.8	Procedure when receiving "Not authorized"	192
Annex F	(informative) Test and simulators	193
F.1	Purpose	193
F.2	Manual testing	193
F.3	Ship and shore equipment	193
F.4	SECOM information service equipment	194
F.5	SECOM PKI equipment	194
F.6	SECOM Service Discovery equipment	195
Bibliography		196
Figure 1	– Overview of SECOM	22
Figure 2	– Secure communication channel	24
Figure 3	– Illustration of what parts of the message are protected by the two signatures	25
Figure 4	– Envelope and data validation	26
Figure 5	– Service definition model for the service interface definitions	28
Figure 6	– Example in C# of conversion from PEM format to minified public key	33
Figure 7	– Example of a public key in PEM format converted to a single line string	33
Figure 8	– Example in C# of conversion from minified public key to PEM format	34
Figure 9	– Example of a minified public key string restored to the original PEM format	34
Figure 10	– UUID version and variant	38

Figure 11 – Upload interface UML diagram	41
Figure 12 – Sequence diagram for upload signed unclassified data with acknowledgement	45
Figure 13 – Update link interface UML diagram.....	47
Figure 14 – Sequence diagram for Upload link to large data	51
Figure 15 – Acknowledgement interface UML diagram	52
Figure 16 – Sequence diagram for Acknowledgement interface	55
Figure 17 – Get interface UML diagram.....	56
Figure 18 – Sequence diagram for Get interface	59
Figure 19 – Sequence diagram for Get interface and classified data	60
Figure 20 – Get Summary interface UML diagram	61
Figure 21 – Sequence diagram for Get Summary interface	64
Figure 22 – Get By Link interface in UML	64
Figure 23 – Sequence diagram for Get By Link interface.....	66
Figure 24 – Access interface UML diagram	67
Figure 25 – Sequence diagram for Request Access and Access Notification interface	69
Figure 26 – Access Notification interface UML diagram.....	70
Figure 27 – Subscribe interface UML diagram.....	72
Figure 28 – Sequence diagram for Subscribe interface	74
Figure 29 – Operational sequence diagram for Subscription interfaces	75
Figure 30 – Sequence diagram for Subscription interfaces with external subscription request	76
Figure 31 – Remove Subscription interface UML diagram	77
Figure 32 – Sequence diagram for Remove Subscription interface.....	78
Figure 33 – Subscription Notification interface UML diagram	79
Figure 34 – Sequence diagram for Subscription Notification interface	81
Figure 35 – Capability interface UML diagram.....	82
Figure 36 – Sequence diagram for Capability interface	84
Figure 37 – Ping interface UML diagram	85
Figure 38 – Check status on service	86
Figure 39 – Encryption Key interface UML diagram.....	87
Figure 40 – Operational sequence diagram for EncryptionKey upload interface	91
Figure 41 – Operational sequence diagram for EncryptionKey notification interface	92
Figure 42 – PublicKey interface UML diagram.....	93
Figure 43 – Operational sequence diagram for PublicKey interface.....	95
Figure 44 – Principle for service authentication.....	97
Figure 45 – Sequence for SECOM encryption key management.....	104
Figure 46 – Alternative sequence for SECOM encryption key management.....	105
Figure 47 – CSR interface UML diagram	111
Figure 48 – Operational sequence diagram for CSR	112
Figure 49 – GetPublicKey interface UML diagram	113
Figure 50 – Operational sequence diagram for GetPublicKey.....	115
Figure 51 – GetCRL interface UML diagram.....	115
Figure 52 – Operational sequence diagram for CRL.....	116

Figure 53 – GetOCSP interface UML diagram	117
Figure 54 – Operational sequence diagram for OCSP	119
Figure 55 – PostRevoke interface UML diagram	119
Figure 56 – Operational sequence diagram for Revoke	121
Figure 57 – Search service UML information diagram	122
Figure C.1 – Message Exchange Pattern – ONE_WAY	167
Figure C.2 – Message Exchange Pattern – REQUEST_CALLBACK	168
Figure C.3 – Message exchange pattern – REQUEST_RESPONSE	168
Figure C.4 – Message exchange pattern – PUBLISH_SUBSCRIBE (Provider nominates)	169
Figure C.5 – Message exchange pattern – PUBLISH_SUBSCRIBE (Consumer request)	169
Figure C.6 – Error sequence; Incorrect uploaded message	170
Figure C.7 – Error sequence; Unauthorized upload of message	170
Figure C.8 – Error sequence; Unauthorized subscription request	170
Figure D.1 – Overview of SECOM	171
Figure D.2 – Overview of certificate usage	172
Figure D.3 – Deployment example for SECOM on ship	173
Figure D.4 – Deployment example for SECOM on shore	174
Figure D.5 – Service composition	175
Figure D.6 – Structure of MIR within MCP	176
Figure D.7 – Hierarchical X.509 PKI Structure	181
Figure D.8 – Request find service with geometry and query	187
Figure D.9 – Response from service registry	188
Figure D.10 – Response from service registry	189
Figure F.1 – Manual testing	193
Figure F.2 – Overview of test equipment for ship and shore equipment	194
Figure F.3 – Overview of test equipment for SECOM information service equipment	194
Figure F.4 – Overview of test equipment for SECOM PKI equipment	195
Figure F.5 – Overview of test equipment for SECOM service discovery equipment	195
Table 1 – Read instructions for tables in service interface definitions	29
Table 2 – SECOM Service interface versioning	30
Table 3 – Basic data types	31
Table 4 – SECOM_ExchangeMetadataObject	32
Table 5 – DigitalSignatureValueObject	32
Table 6 – PaginationObject	35
Table 7 – ContainerTypeEnum	35
Table 8 – SECOM_DataProductType	35
Table 9 – SECOM_ResponseCodeEnum	36
Table 10 – AckRequest Enum	36
Table 11 – Common HTTP codes	37
Table 12 – Supported WKT geometric objects	37
Table 13 – UUID variants	38

Table 14 – UUID versions	39
Table 15 – Service interfaces overview	39
Table 16 – Information input for Upload interface	42
Table 17 – Information output for Upload interface	43
Table 18 – REST implementation of Upload	43
Table 19 – HTTP Response codes and message in response object	44
Table 20 – Information input for Upload Link interface	48
Table 21 – Information output for Upload Link interface	49
Table 22 – REST implementation of Upload Link	49
Table 23 – HTTP Response codes and message in response object	49
Table 24 – Information input for Acknowledgement interface	53
Table 25 – Enumerations for not acknowledged	53
Table 26 – Information output for Acknowledgement interface	53
Table 27 – Enumerations for Acknowledgement interface	54
Table 28 – REST implementation of acknowledgement	54
Table 29 – HTTP Response codes and response message	55
Table 30 – Information input for Get interface	57
Table 31 – Information output for Get interface	57
Table 32 – REST implementation of Get	58
Table 33 – HTTP Response code and message of Get	58
Table 34 – Information input for Get Summary interface	61
Table 35 – Information output for Get Summary interface	62
Table 36 – REST implementation of Get Summary	63
Table 37 – HTTP Response codes and messages of Get Summary	63
Table 38 – Information input for Get By Link interface	64
Table 39 – Information output for Get By Link interface	65
Table 40 – REST implementation of Get By Link	65
Table 41 – HTTP Response code and message of Get By Link	65
Table 42 – Information input for Access interface	67
Table 43 – Information output for Access interface	68
Table 44 – Enumerations for Access interface	68
Table 45 – Parameter binding for the operation	68
Table 46 – HTTP Response codes	69
Table 47 – Information input for Access Notification interface	70
Table 48 – Information output for Access Notification interface	70
Table 49 – Parameter binding for the operation	71
Table 50 – HTTP response codes	71
Table 51 – Information input for Subscription interface	73
Table 52 – Information output for Subscription interface	73
Table 53 – REST implementation of Subscription	73
Table 54 – HTTP response codes and messages of Subscription	74
Table 55 – Information input for Remove Subscription interface	77
Table 56 – Information output for Remove Subscription interface	77

Table 57 – REST implementation of Remove Subscription	78
Table 58 – HTTP Response codes and messages of Remove Subscription.....	78
Table 59 – Information input for Subscription Notification interface	79
Table 60 – Information output for Subscription Notification interface	79
Table 61 – Enumerations for Subscription Notification interface	80
Table 62 – Information exchange for Subscription Notification	80
Table 63 – HTTP response codes for Subscription Notification	80
Table 64 – Capability example	81
Table 65 – Information output for Capability interface	83
Table 66 – REST implementation of Capability	84
Table 67 – HTTP response codes and messages of Capability	84
Table 68 – Information output for Ping interface.....	85
Table 69 – REST implementation of Ping	86
Table 70 – HTTP response codes of Ping	86
Table 71 – Information input for Encryption Key interface	88
Table 72 – Information input for Encryption Key Notification interface	88
Table 73 – Information output for Encryption Key interface	89
Table 74 – REST implementation of EncryptionKey upload	89
Table 75 – HTTP response codes of EncryptionKey upload	89
Table 76 – REST implementation of EncryptionKey notification.....	90
Table 77 – HTTP response codes of EncryptionKey notification.....	90
Table 78 – Information input for PublicKey interface	93
Table 79 – Information output for PublicKey interface GET and information input for PublicKey interface POST.....	93
Table 80 – REST implementation of PublicKey (GET)	94
Table 81 – HTTP response code and message of PublicKey (GET)	94
Table 82 – REST implementation of PublicKey (POST).....	95
Table 83 – HTTP response code and message of PublicKey (POST)	95
Table 84 – Conversion rules	100
Table 85 – Interfaces with envelope signature	101
Table 86 – Command examples.....	102
Table 87 – Example of commands	106
Table 88 – Creation of public and private key pairs – Example of basic commands.....	109
Table 89 – PKI interface overview.....	110
Table 90 – Information input for CSR interface.....	111
Table 91 – Information output for CSR interface	111
Table 92 – REST implementation of CSR.....	112
Table 93 – HTTP response codes and message in response object.....	112
Table 94 – Information input for GetPublicKey interface.....	113
Table 95 – Information output for GetPublicKey interface.....	113
Table 96 – REST implementation of GetPublicKey interface	114
Table 97 – HTTP Response codes and message in response object.....	114
Table 98 – REST implementation of CRL	116

Table 99 – HTTP response codes and message in response object	116
Table 100 – REST implementation of OCSP	117
Table 101 – HTTP response codes and message in response object	118
Table 102 – REST implementation of OCSP	118
Table 103 – HTTP response codes and message in response object	118
Table 104 – Information input for Revoke interface	119
Table 105 – Enumerations for Revoke interface	120
Table 106 – Information output for Revoke interface	120
Table 107 – REST implementation of Revoke	120
Table 108 – HTTP response codes and message in response object	121
Table 109 – Information input for search service interface	123
Table 110 – Information input for search parameter object.....	123
Table 111 – Information output for search service interface	124
Table 112 – REST implementation for Search Service	125
Table 113 – HTTP response codes	125
Table 114 – Test data reference	134
Table 115 – Upload test method steps	137
Table 116 – Download test method steps.....	138
Table 117 – Test data reference	139
Table 118 – Access test method steps	141
Table 119 – Access Notification test method steps	141
Table 120 – Acknowledgement test method steps	142
Table 121 – Capability test method steps.....	142
Table 122 – EncryptionKey test method steps.....	143
Table 123 – EncryptionKey notification test method steps.....	144
Table 124 – Get test method steps	145
Table 125 – Get By Link test method steps	146
Table 126 – Get Summary test method steps.....	147
Table 127 – Get Public Key test method steps	147
Table 128 – Upload Public Key test method steps.....	148
Table 129 – Ping test method steps	148
Table 130 – Subscription test method steps.....	149
Table 131 – Subscription Notification test method steps	149
Table 132 – Remove Subscription test method steps	150
Table 133 – Upload test method steps	151
Table 134 – Upload Link test method steps.....	152
Table 135 – CRL test method steps	153
Table 136 – OCSP test method steps	153
Table 137 – Revoke test method steps	154
Table 138 – CSR test method steps.....	154
Table 139 – GetPublicKey test method steps	155
Table 140 – Search service by geometry test method steps.....	156
Table 141 – Search service empty query test method steps.....	156

Table B.1 – UC-1 Ship shares route plan with service providing enhanced monitoring	159
Table B.2 – Required service interfaces in UC-3	160
Table B.3 – Required service interfaces in UC-3	161
Table B.4 – Required service interfaces in UC-4	162
Table B.5 – Required service interfaces in UC-6	164
Table B.6 – Required service interfaces in UC-7	165
Table B.7 – Required service interfaces in UC-8	166
Table D.1 – Domain parameters	183
Table D.2 – Subject distinguished name field items	183
Table D.3 – Fields and object identifiers	184
Table D.4 – MCP OpenID Connect token	186

INTERNATIONAL ELECTROTECHNICAL COMMISSION

**MARITIME NAVIGATION AND RADIOCOMMUNICATION
EQUIPMENT AND SYSTEMS –
DATA INTERFACES –****Part 2: Secure communication between ship and shore (SECOM)**

FOREWORD

- 1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
- 2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
- 3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
- 4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
- 5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
- 6) All users should ensure that they have the latest edition of this publication.
- 7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
- 8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
- 9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

IEC 63173-2 has been prepared by IEC technical committee 80: Maritime navigation and radiocommunication equipment and systems. It is an International Standard.

The text of this International Standard is based on the following documents:

Draft	Report on voting
80/1030/FDIS	80/1039/RVD

Full information on the voting for its approval can be found in the report on voting indicated in the above table.

The language used for the development of this International Standard is English.

This document was drafted in accordance with ISO/IEC Directives, Part 2, and developed in accordance with ISO/IEC Directives, Part 1 and ISO/IEC Directives, IEC Supplement, available at www.iec.ch/members_experts/refdocs. The main document types developed by IEC are described in greater detail at www.iec.ch/standardsdev/publications.

A list of all parts in the IEC 63173 series, published under the general *Maritime navigation and radiocommunication equipment and systems – Data interfaces*, can be found on the IEC website.

The committee has decided that the contents of this document will remain unchanged until the stability date indicated on the IEC website under webstore.iec.ch in the data related to the specific document. At this date, the document will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

E-navigation has been defined as the means of providing electronic information in a harmonized way, and maritime services have been specified by the International Maritime Organization (IMO). The maritime services are operational services for actors both ashore and onboard. To make the maritime services interoperable between different actors and systems from different manufactures standards, specifications and guidelines in several layers are required, for example technical services and data/product formats. Technical services comprises a set of technical solutions and communications means to provide a maritime service. IMO's e-navigation strategy implementation plan (SIP) requires that all maritime services are IHO S-100 conformant as a baseline. Further, IEC is expected to implement the details as outlined in the SIP.

Secure communication between ship and shore (SECOM) provides standards for secure data exchange with technical services. Further, it contains a technical service interface design that is in accordance with the service guidelines and templates defined by IALA and partly included in IHO S-100.

SECOM specifies service interfaces (APIs) for data exchange, data protection measures to enable secure communication and interfaces for service discoverability. SECOM is applicable for IHO S-100 based products but also other data (payload) formats are supported, i.e. SECOM is generally independent of which data type is exchanged.

The standardisation of a common service interface for data exchange will enable wider technical interoperability where the same service interface can be used for exchanging information regardless of its operational use.

Accordingly, the purpose of SECOM is to:

- facilitate standardized information exchange of, for example, IHO S-100 based products part of maritime services such as route plans, nautical chart updates and navigational warnings;
- facilitate interoperability between maritime IT systems;
- reduce the need to support many different (proprietary) service designs;
- utilize the benefits of service oriented architecture in maritime communication, for example to enable ship systems to interact with port systems on the first call to a specific port.

MARITIME NAVIGATION AND RADIOCOMMUNICATION EQUIPMENT AND SYSTEMS – DATA INTERFACES –

Part 2: Secure communication between ship and shore (SECOM)

1 Scope

The scope of SECOM includes interfaces (APIs) for data exchange (information services), information security measures to enable secure communication and interfaces for service discoverability. SECOM provides technical interoperability, where the same service interface is used for exchanging the information regardless of its operational use, up to the level of exchanging information securely online. Although designed for IHO S-100 based products, SECOM is technically payload agnostic and applicable also for other types of data.

Communication between SECOM information services for data exchange relies on IP based web services. The "last mile" links between a SECOM information service and the end-user application is not defined in this document, thus the communication technology between the vendor API and a ship/shore system can be non-IP based as well as IP based. The informative Annex D describes one such implementation of this. This allows different solutions between the service and shore/ship's system/applications.

SECOM does not define physical layer or link layer for transport of data between SECOM information services, but requires that the transport supports IP communication. SECOM is applicable for both public (governmental) and private (business) services. SECOM is applicable for ship-shore and shore-ship communication, and can be used for ship-ship communication.

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.

IHO S-100:2018, *IHO Universal Hydrographic Data Model*, ed. 4.0.0

RFC 2315, *PKCS #7: Cryptographic Message Syntax*

RFC 2459, *Internet X.509 Public-key infrastructure and attribute certificate frameworks*

RFC 2818, *HTTP Over TLS (2000)*

RFC 2986, *PKCS #10: Certification Request Syntax Specification*

RFC 4122, *A Universally Unique Identifier (UUID) URN Namespace*

RFC 5246, *TLS version 1.2 (2008)*

RFC 5280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*

RFC 6960, *X.509 Internet Public Key Infrastructure, Online Certificate Status Protocol – OCSP*

RFC 7231, *Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content*

RFC 8446, *TLS version 1.3 (2018)*

SOMMAIRE

AVANT-PROPOS	209
INTRODUCTION.....	211
1 Domaine d'application	212
2 Références normatives	212
3 Termes, définitions et termes abrégés	213
3.1 Termes et définitions	213
3.2 Termes abrégés	217
4 Description générale du SECOM	218
4.1 Généralités	218
4.2 Interface des services d'information	219
4.3 Sécurité des informations.....	219
4.3.1 Mesures	219
4.3.2 PKI SECOM.....	220
4.3.3 Sécurité des canaux de communication	220
4.3.4 Protection des données	221
4.3.5 Etat de révocation du certificat	223
4.4 Découvrabilité des services	223
4.5 Structure du présent document	223
5 Interface des services d'information SECOM	223
5.1 Généralités	223
5.2 Comment lire les descriptions de la définition des interfaces de service	224
5.3 Technologie des services et protocole de transport des services	226
5.4 Versions de l'interface de service.....	226
5.5 Pagination	227
5.6 Objets d'information communs et types de données.....	227
5.6.1 Généralités	227
5.6.2 Types de données de base	227
5.6.3 SECOM_ExchangeMetadataObject.....	228
5.6.4 Transfert de clé publique	229
5.6.5 PaginationObject	232
5.6.6 ContainerTypeEnum	232
5.6.7 SECOM_DataProductType	233
5.6.8 SECOM_ResponseCodeEnum.....	233
5.6.9 AckRequest Enum	234
5.6.10 Codes de réponse HTTP communs.....	234
5.6.11 Représentation textuelle connue (WKT).....	234
5.6.12 Identificateur unique universel (UUID)	235
5.6.13 UN/LOCODE	237
5.7 Définitions des interfaces de service	237
5.7.1 Généralités	237
5.7.2 Interface de service – Upload	238
5.7.3 Interface de service – Upload Link	244
5.7.4 Interface de service – Acknowledgement	249
5.7.5 Interface de service – Get.....	253
5.7.6 Interface de service – Get Summary	258
5.7.7 Interface de service – Get By Link	262

5.7.8	Interface de service – Access	264
5.7.9	Interface de service – Access Notification.....	267
5.7.10	Interface de service – Subscription	269
5.7.11	Interface de service – Remove Subscription	274
5.7.12	Interface de service – Subscription Notification.....	277
5.7.13	Interface de service – Capability	279
5.7.14	Interface de service – Ping	282
5.7.15	Interface de service – EncryptionKey	284
5.7.16	Interface de service – PublicKey	290
6	Sécurité des canaux de communication SECOM.....	293
6.1	Généralités	293
6.2	Transfert sécurisé	294
6.2.1	Canaux de communication sécurisés	294
6.2.2	Procédure d'authentification	294
7	Protection des données SECOM.....	295
7.1	Généralités	295
7.2	Compression et emballage des données	295
7.3	Authentification et signature des données	296
7.3.1	Généralités	296
7.3.2	Formats de données et normes pour les signatures numériques, les clés et les certificats	296
7.3.3	Création d'une signature numérique	297
7.3.4	Création d'une signature d'enveloppe	298
7.3.5	Vérification de la signature numérique	300
7.3.6	Vérification d'une signature d'enveloppe.....	300
7.3.7	Exemple de commandes d'authentification des données.....	301
7.4	Chiffrement des données	301
7.4.1	Généralités	301
7.4.2	Algorithme de chiffrement	301
7.5	Création et transfert de clé de chiffrement	302
7.5.1	Généralités	302
7.5.2	Gestion des clés de chiffrement SECOM	302
7.5.3	Génération de la clé de chiffrement.	304
7.5.4	Signature de la clé de chiffrement protégée.....	304
7.5.5	Transfert de la clé de chiffrement.	305
7.5.6	Exemple	305
8	PKI SECOM.....	305
8.1	Généralités	305
8.2	Schéma	306
8.2.1	Généralités	306
8.2.2	Administrateur de schéma	306
8.2.3	Serveurs de données.....	306
8.2.4	Clients de données	307
8.2.5	Procédure.....	307
8.3	Génération des clés publique et privée	307
8.4	Demande de signature de certificat.....	308
8.5	Révocation de certificats	308
8.5.1	Généralités	308
8.5.2	CRL Liste de révocation de certificats.....	308

8.5.3	OCSP Protocole de statut de certificat en ligne	308
8.6	Interface des services PKI SECOM	309
8.6.1	Généralités	309
8.6.2	Interface de service – CSR	310
8.6.3	Interface de service – GetPublicKey	312
8.6.4	Interface de service – CRL	314
8.6.5	Interface de service – OCSP	316
8.6.6	Interface de service – Revoke	318
9	Interface du service de découverte de services SECOM	321
9.1	Généralités	321
9.2	Interface de service – Search Service	322
9.2.1	Spécification	322
9.2.2	Modèle d'échange de données	323
9.2.3	Conception REST	324
10	Cas d'erreur SECOM	325
10.1	Cas d'erreur	325
10.2	Généralités	326
10.3	Intégrité des messages	326
10.4	Intégrité des données	326
10.5	Confidentialité des transports	327
10.6	Protection des données	327
10.7	Identité du service	328
10.8	Identité du client	328
10.9	Autorisation du client	328
10.10	Optimisation de la bande passante	328
10.11	Transfert de longs messages	328
10.12	Communication en boucle fermée	329
10.13	Découvrabilité des services	330
10.14	Envoi d'informations (push)	330
10.15	Extraction d'informations (pull)	331
10.16	Abonnement aux données	331
10.17	Informations sur le service	332
10.18	Conditions du service	332
11	Méthodes d'essai et résultats escomptés	332
11.1	Généralités	332
11.2	Essai de sécurité des canaux de communication	333
11.3	Essai de protection des données	333
11.3.1	Compression et empaquetage des données	333
11.3.2	Authentification et signature des données	333
11.3.3	Chiffrement	333
11.3.4	Essai de signature numérique	333
11.4	Essai SECOM navire/terre	334
11.4.1	Généralités	334
11.4.2	Conditions préalables SECOM pour un EUT navire/terre	337
11.4.3	Données pour le téléchargement montant	337
11.4.4	Données pour le téléchargement descendant	338
11.5	Essai de service d'information SECOM	340
11.5.1	Généralités	340

11.5.2	Conditions préalables relatives au service d'informations SECOM des EUT	341
11.5.3	Access.....	341
11.5.4	Access Notification	342
11.5.5	Acknowledgement.....	342
11.5.6	Capability	343
11.5.7	EncryptionKey	344
11.5.8	EncryptionKey Notification	345
11.5.9	Get	346
11.5.10	Get By Link.....	347
11.5.11	Get Summary	348
11.5.12	Get Public Key.....	349
11.5.13	Upload Public Key	349
11.5.14	Ping.....	350
11.5.15	Subscription	350
11.5.16	Subscription Notification	351
11.5.17	Remove Subscription.....	351
11.5.18	Upload.....	352
11.5.19	Upload Link	353
11.6	Essai relatif au service PKI SECOM.....	354
11.6.1	Conditions préalables relatives à la PKI des EUT	354
11.6.2	CRL.....	355
11.6.3	OCSP	355
11.6.4	Revoke	356
11.6.5	CSR	356
11.6.6	GetPublicKey.....	357
11.7	Essai relatif à la fonction de découverte des services SECOM.....	357
11.7.1	Généralités.....	357
11.7.2	Conditions préalables pour les EUT de découverte des services.....	357
11.7.3	Search service – par géométrie	358
11.7.4	Search service – sans critère de recherche spécifique.....	358
Annexe A (normative)	Définitions relatives à l'interface de service REST.....	360
A.1	Objectif.....	360
A.2	Définition de l'interface REST des services d'informations SECOM.....	360
A.3	Définition de l'interface REST du service PKI SECOM	360
A.4	Définition de l'interface REST du service de découverte des services SECOM.....	360
Annexe B (informative)	Cas d'utilisation (UC) et profils opérationnels	361
B.1	Objectif.....	361
B.2	Cas d'utilisation et profils d'interface de service.....	361
B.2.1	UC-1 Le navire partage son plan de route avec un service assurant une surveillance renforcée	361
B.2.2	UC-2 Routes pilotes.....	363
B.2.3	UC-3 Optimisation des routes	364
B.2.4	UC-4 Le service de surveillance renforcée demande un plan de route au/pour le navire pour la surveillance	365
B.2.5	UC-5 Instance de service de découverte à utiliser	366
B.2.6	UC-6 Mises à jour de cartes (ENC).....	367
B.2.7	UC-7 Service d'avertissements de navigation	368

B.2.8	UC-8 Mises à jour pour la bathymétrie détaillée et les prévisions de marées et de hauteur d'eau	369
Annexe C (informative)	Schémas d'échange de messages	371
C.1	Objectif	371
C.2	Schéma d'échange de messages	371
C.2.1	Schémas d'échange de messages génériques	371
C.2.2	Options et séquences d'erreur	374
Annexe D (informative)	Recommandations relatives à la mise en œuvre	375
D.1	Objectif	375
D.2	A bord du navire	376
D.3	A terre	377
D.4	Composition du service	378
D.5	Sécurité du côté privé	379
D.6	PKI SECOM	379
D.6.1	Généralités	379
D.6.2	Structure et fonctionnalité	379
D.6.3	Gestion des identités	381
D.6.4	Infrastructure de clé publique	383
D.6.5	Authentification et autorisation pour les services Web	390
D.6.6	"Exigences de base" de profil	391
D.7	Découverte des services SECOM	391
D.7.1	Exemple 1: géométrie associée à la recherche serviceType	391
D.7.2	Exemple 2: Recherche avec condition ET/OU	393
Annexe E (informative)	Utilisation de la liste blanche	395
E.1	Objectif	395
E.2	Autorisation d'accéder aux données	395
E.3	Liste de contrôle d'accès	396
E.4	Autorisation basée sur des règles ou une liste prédéfinies	397
E.5	Liste mise à jour manuellement	397
E.6	Gestion basée sur des règles pour les demandes d'informations (autorisation en fonction de règles)	397
E.7	Demande d'informations basée sur des règles	397
E.8	Procédure en cas de réponse "Non autorisé"	397
Annexe F (informative)	Essai et simulateurs	398
F.1	Objectif	398
F.2	Essai manuel	398
F.3	Matériel du navire et à terre	398
F.4	Matériel des services d'information SECOM	399
F.5	Matériel de PKI SECOM	399
F.6	Matériel de découverte des services SECOM	400
Bibliographie		401
Figure 1	– Vue d'ensemble de SECOM	218
Figure 2	– Canaux de communication sécurisés	220
Figure 3	– Représentation des parties du message qui sont protégées par les deux signatures	222
Figure 4	– Validation de l'enveloppe et des données	222
Figure 5	– Modèle de définition de service pour les définitions d'interface de service	225

Figure 6 – Exemple en C# de conversion du format PEM en clé publique minimisée.....	230
Figure 7 – Exemple de clé publique au format PEM convertie en chaîne d'une seule ligne	230
Figure 8 – Exemple en C# de conversion de clé publique minimisée au format PEM.....	231
Figure 9 – Exemple de chaîne de clé publique minimisée restaurée au format PEM original	232
Figure 10 – Version UUID et variante.....	236
Figure 11 – Diagramme UML de l'interface Upload	239
Figure 12 – Diagramme de séquence pour le téléchargement montant de données non classifiées signées avec acceptation.....	243
Figure 13 – Diagramme UML de l'interface de lien de téléchargement	245
Figure 14 – Diagramme de séquence pour Upload Link vers des données volumineuses.....	249
Figure 15 – Diagramme UML de l'interface Acknowledgement	250
Figure 16 – Diagramme de séquence pour l'interface Acknowledgement	253
Figure 17 – Diagramme UML de l'interface Get.....	254
Figure 18 – Diagramme de séquence de l'interface Get	257
Figure 19 – Diagramme de séquence de l'interface Get et de données classifiées	258
Figure 20 – Diagramme UML de l'interface Get Summary	259
Figure 21 – Diagramme de séquence de l'interface Get Summary	262
Figure 22 – Interface Get By Link en UML.....	262
Figure 23 – Diagramme de séquence de l'interface Get By Link.....	264
Figure 24 – Diagramme UML de l'interface Access	265
Figure 25 – Diagramme de séquence des interfaces Request Access et Access Notification	267
Figure 26 – Diagramme UML de l'interface Access Notification.....	268
Figure 27 – Diagramme UML de l'interface Subscribe	270
Figure 28—Diagramme de séquence de l'interface Subscribe	272
Figure 29 – Diagramme de séquence opérationnelle des interfaces Subscription.....	273
Figure 30 – Diagramme de séquence des interfaces Subscription avec demande d'abonnement externe	274
Figure 31 – Diagramme UML de l'interface Remove Subscription	275
Figure 32 – Diagramme de séquence de l'interface Remove Subscription.....	276
Figure 33 – Diagramme UML de l'interface Subscription Notification.....	277
Figure 34 – Diagramme de séquence de l'interface Subscription Notification	279
Figure 35 – Diagramme UML de l'interface Capability	280
Figure 36 – Diagramme de séquence de l'interface Capability	282
Figure 37 – Diagramme UML de l'interface Ping	283
Figure 38 – Vérification de l'état du service	284
Figure 39 – Diagramme UML de l'interface Encryption Key.....	285
Figure 40 – Diagramme de séquence opérationnelle de l'interface de téléchargement montant EncryptionKey	289
Figure 41 – Diagramme de séquence opérationnelle de l'interface EncryptionKey notification.....	289
Figure 42 – Diagramme UML de l'interface PublicKey	290
Figure 43 – Diagramme de séquence opérationnelle de l'interface PublicKey	293

Figure 44 – Principe d'authentification des services	295
Figure 45 – Séquence de gestion des clés de chiffrement SECOM	303
Figure 46 – Autre séquence de gestion des clés de chiffrement SECOM.....	304
Figure 47 – Diagramme UML de l'interface CSR	310
Figure 48 – Diagramme de séquence opérationnelle de CSR.....	312
Figure 49 – Diagramme UML de l'interface GetPublicKey	312
Figure 50 – Diagramme de séquence opérationnelle de GetPublicKey	314
Figure 51 – Diagramme UML de l'interface GetCRL	314
Figure 52 – Diagramme de séquence opérationnelle de CRL	316
Figure 53 – Diagramme UML de l'interface GetOCSP	316
Figure 54 – Diagramme de séquence opérationnelle de OCSP	318
Figure 55 – Diagramme UML de l'interface PostRevoke.....	319
Figure 56 – Diagramme de séquence opérationnelle de Revoke	321
Figure 57 – Diagramme d'information UML de Search Service.....	322
Figure C.1 – Schéma d'échange de messages – ONE_WAY.....	371
Figure C.2 – Schéma d'échange de messages – REQUEST_CALLBACK.....	372
Figure C.3 – Schéma d'échange de messages – REQUEST_RESPONSE.....	372
Figure C.4 – Schéma d'échange de messages -- PUBLISH_SUBSCRIBE (le fournisseur désigne)	373
Figure C.5 – Schéma d'échange de messages – PUBLISH_SUBSCRIBE (l'utilisateur demande)	373
Figure C.6 – Séquence d'erreur: Message chargé incorrect	374
Figure C.7 – Séquence d'erreur: Message chargé non autorisé	374
Figure C.8 – Séquence d'erreur: Demande d'abonnement non autorisée	374
Figure D.1 – Vue d'ensemble des services SECOM	375
Figure D.2 – Vue d'ensemble de l'utilisation des certificats	376
Figure D.3 – Exemple de déploiement de service SECOM sur un navire	377
Figure D.4 – Exemple de déploiement d'un service SECOM à terre	377
Figure D.5 – Composition du service.....	378
Figure D.6 – Structure du MIR au sein de la MCP	380
Figure D.7 – Structure hiérarchique de la PKI X.509	385
Figure D.8 – Service de recherche d'une demande à l'aide de la géométrie et d'une requête	392
Figure D.9 – Réponse du registre de services.....	393
Figure D.10 – Réponse du registre de services.....	394
Figure F.1 – Essai manuel	398
Figure F.2 – Vue d'ensemble du matériel d'essai pour les matériels du navire et à terre	399
Figure F.3 – Vue d'ensemble du matériel d'essai pour le matériel des services d'information SECOM	399
Figure F.4 – Vue d'ensemble du matériel d'essai pour le matériel PKI SECOM	400
Figure F.5 – Vue d'ensemble du matériel d'essai pour le matériel de découverte des services SECOM.....	400

Tableau 1 – Lire les instructions pour les tableaux dans les définitions des interfaces de service	225
--	-----

Tableau 2 – Versions de l'interface de service SECOM	226
Tableau 3 – Types de données de base	227
Tableau 4 – SECOM_ExchangeMetadataObject	229
Tableau 5 – DigitalSignatureValueObject	229
Tableau 6 – PaginationObject	232
Tableau 7 – ContainerTypeEnum	232
Tableau 8 – SECOM_DataProductType	233
Tableau 9 – SECOM_ResponseCodeEnum	234
Tableau 10 – AckRequest Enum	234
Tableau 11 – Codes HTTP communs	234
Tableau 12 – Objets géométriques WKT pris en charge	235
Tableau 13 – Variantes d'UUID	236
Tableau 14 – Versions d'UUID	236
Tableau 15 – Vue d'ensemble des interfaces de service	237
Tableau 16 – Entrée d'informations pour l'interface Upload	240
Tableau 17 – Sortie d'informations pour l'interface Upload	241
Tableau 18 – Mise en œuvre REST de Upload	241
Tableau 19 – Codes de réponse et messages HTTP dans l'objet réponse	242
Tableau 20 – Entrée d'informations pour l'interface Upload Link	246
Tableau 21 – Sortie d'informations pour l'interface Upload Link	247
Tableau 22 – Mise en œuvre REST de Upload Link	247
Tableau 23 – Codes de réponse et messages HTTP dans l'objet réponse	247
Tableau 24 – Entrée d'informations pour l'interface Acknowledgement	251
Tableau 25 – Enumérations pour non accepté	251
Tableau 26 – Sortie d'informations pour l'interface Acknowledgement	251
Tableau 27 – Enumérations pour l'interface Acknowledgement	252
Tableau 28 – Mise en œuvre REST de Acknowledgement	252
Tableau 29 – Codes et messages de réponse HTTP	253
Tableau 30 – Entrée d'informations pour l'interface Get	255
Tableau 31 – Sortie d'informations pour l'interface Get	255
Tableau 32 – Mise en œuvre REST de Get	256
Tableau 33 – Codes et messages de réponse HTTP de Get	257
Tableau 34 – Entrée d'informations pour l'interface Get Summary	259
Tableau 35 – Sortie d'informations pour l'interface Get Summary	260
Tableau 36 – Mise en œuvre REST de Get Summary	261
Tableau 37 – Codes et messages de réponse HTTP de Get Summary	261
Tableau 38 – Entrée d'informations pour l'interface Get By Link	263
Tableau 39 – Sortie d'informations pour l'interface Get By Link	263
Tableau 40 – Mise en œuvre REST de Get By Link	263
Tableau 41 – Codes et messages de réponse HTTP de Get By link	264
Tableau 42 – Entrée d'informations pour l'interface Access	265
Tableau 43 – Sortie d'informations pour l'interface Access	266
Tableau 44 – Enumérations pour l'interface Access	266

Tableau 45 – Liens avec les paramètres de l'opération	266
Tableau 46 – Codes de réponse HTTP	267
Tableau 47 – Entrée d'informations pour l'interface Access Notification	268
Tableau 48 – Sortie d'informations pour l'interface Access Notification	268
Tableau 49 – Liens avec les paramètres de l'opération	269
Tableau 50 – Codes de réponse HTTP	269
Tableau 51 – Entrée d'informations pour l'interface Subscription	271
Tableau 52 – Sortie d'informations pour l'interface Subscription	271
Tableau 53 – Mise en œuvre REST de Subscription	271
Tableau 54 – Codes et messages de réponse HTTP de Subscription	272
Tableau 55 – Entrée d'informations pour l'interface Remove Subscription	275
Tableau 56 – Sortie d'informations pour l'interface Remove Subscription	275
Tableau 57 – Mise en œuvre REST de Remove Subscription	276
Tableau 58 – Codes et messages de réponse HTTP de Remove Subscription	276
Tableau 59 – Entrée d'informations pour l'interface Subscription Notification	277
Tableau 60 – Sortie d'informations pour l'interface Subscription Notification	277
Tableau 61 – Enumérations pour l'interface Subscription Notification	278
Tableau 62 – Echange d'informations pour Subscription Notification	278
Tableau 63 – Codes de réponse HTTP pour Subscription Notification	278
Tableau 64 – Exemple de capacité	279
Tableau 65 – Sortie d'informations pour l'interface Capability	281
Tableau 66 – Mise en œuvre REST de Capability	282
Tableau 67 – Codes et messages de réponse HTTP de Capability	282
Tableau 68 – Sortie d'informations pour l'interface Ping	283
Tableau 69 – Mise en œuvre REST de Ping	284
Tableau 70 – Codes de réponse HTTP Ping	284
Tableau 71 – Entrée d'informations pour l'interface Encryption Key	286
Tableau 72 – Entrée d'informations pour l'interface Encryption Key Notification	286
Tableau 73 – Sortie d'informations pour l'interface Encryption Key	287
Tableau 74 – Mise en œuvre REST du téléchargement montant EncryptionKey	287
Tableau 75 – Codes de réponse HTTP du téléchargement montant EncryptionKey	287
Tableau 76 – Mise en œuvre REST de EncryptionKey notification	288
Tableau 77 – Codes de réponse HTTP de EncryptionKey notification	288
Tableau 78 – Entrée d'informations pour l'interface PublicKey	291
Tableau 79 – Sortie d'information pour l'interface PublicKey GET et entrée d'informations pour l'interface PublicKey POST	291
Tableau 80 – Mise en œuvre REST de PublicKey (GET)	292
Tableau 81 – Codes et messages de réponse HTTP de PublicKey (GET)	292
Tableau 82 – Mise en œuvre REST de PublicKey (POST)	292
Tableau 83 – Codes et messages de réponse HTTP de PublicKey (POST)	293
Tableau 84 – Règles de conversion	299
Tableau 85 – Interfaces avec signature d'enveloppe	299
Tableau 86 – Exemples de commandes	301

Tableau 87 – Exemple de commandes.....	305
Tableau 88 – Création de paires de clés publiques et privées – exemple de commandes de base.....	308
Tableau 89 – Vue d'ensemble des interfaces PKI	309
Tableau 90 – Entrée d'informations pour l'interface CSR	310
Tableau 91 – Sortie d'informations pour l'interface CSR	310
Tableau 92 – Mise en œuvre REST de CSR	311
Tableau 93 – Codes de réponse et messages HTTP dans l'objet réponse.....	311
Tableau 94 – Entrée d'informations pour l'interface GetPublicKey.....	313
Tableau 95 – Sortie d'informations pour l'interface GetPublicKey.....	313
Tableau 96 – Mise en œuvre REST de l'interface GetPublicKey	313
Tableau 97 – Codes de réponse et messages HTTP dans l'objet réponse.....	314
Tableau 98 – Mise en œuvre REST de CRL.....	315
Tableau 99 – Codes de réponse et messages HTTP dans l'objet réponse.....	315
Tableau 100 – Mise en œuvre REST de OCSP	317
Tableau 101 – Codes de réponse et messages HTTP dans l'objet réponse.....	317
Tableau 102 – Mise en œuvre REST de OCSP	317
Tableau 103 – Codes de réponse et messages HTTP dans l'objet réponse.....	318
Tableau 104 – Entrée d'informations pour l'interface Revoke.....	319
Tableau 105 – Enumérations pour l'interface Revoke.....	319
Tableau 106 – Sortie d'informations pour l'interface Revoke	319
Tableau 107 – Mise en œuvre REST de Revoke	320
Tableau 108 – Codes de réponse et messages HTTP dans l'objet réponse.....	320
Tableau 109 – Entrée d'informations pour l'interface Search Service	323
Tableau 110 – Entrée d'informations pour l'objet Search parameter.....	323
Tableau 111 – Sortie d'informations pour l'interface Search Service	324
Tableau 112 – Mise en œuvre REST de Search Service	325
Tableau 113 – Codes de réponse HTTP	325
Tableau 114 – Référence des données d'essai	334
Tableau 115 – Etapes de la méthode d'essai relative à l'interface Upload.....	338
Tableau 116 – Etapes de la méthode d'essai de téléchargement descendant	339
Tableau 117 – Référence des données d'essai	340
Tableau 118 – Etapes de la méthode d'essai relative à l'interface Access	342
Tableau 119 – Etapes de la méthode d'essai relative à l'interface Access Notification	342
Tableau 120 – Etapes de la méthode d'essai relative à l'interface Acknowledgement	343
Tableau 121 – Etapes de la méthode d'essai relative à l'interface Capability	344
Tableau 122 – Etapes de la méthode d'essai relative à l'interface EncryptionKey	345
Tableau 123 – Etapes de la méthode d'essai relative à l'interface EncryptionKey notification	346
Tableau 124 – Etapes de la méthode d'essai relative à l'interface Get.....	347
Tableau 125 – Etapes de la méthode d'essai relative à l'interface Get By Link.....	348
Tableau 126 – Etapes de la méthode d'essai relative à l'interface Get Summary	349
Tableau 127 – Etapes de la méthode d'essai relative à l'interface Get Public Key.....	349
Tableau 128 – Etapes de la méthode d'essai relative à l'interface Upload Public Key	350

Tableau 129 – Etapes de la méthode d’essai relative à l’interface Ping.....	350
Tableau 130 – Etapes de la méthode d’essai relative à l’interface Subscription	351
Tableau 131 – Etapes de la méthode d’essai relative à l’interface Subscription Notification	351
Tableau 132 – Etapes de la méthode d’essai relative à l’interface Remove Subscription.....	352
Tableau 133 – Etapes de la méthode d’essai relative à l’interface Upload.....	353
Tableau 134 – Etapes de la méthode d’essai relative à l’interface Upload Link	354
Tableau 135 – Etapes de la méthode d’essai relative à l’interface CRL.....	355
Tableau 136 – Etapes de la méthode d’essai relative à l’interface OCSP	355
Tableau 137 – Etapes de la méthode d’essai relative à l’interface Revoke	356
Tableau 138 – Etapes de la méthode d’essai relative à l’interface CSR	356
Tableau 139 – Etapes de la méthode d’essai relative à l’interface GetPublicKey.....	357
Tableau 140 – Etapes de la méthode d’essai relative à l’interface Search service par géométrie	358
Tableau 141 – Etapes de la méthode d’essai relative à l’interface Search service sans requête	359
Tableau B.1 – UC-1 Le navire partage son plan de route avec un service de surveillance renforcée.....	363
Tableau B.2 – Interfaces de service exigées dans l’UC-3.....	364
Tableau B.3 – Interfaces de service exigées dans l’UC-3.....	365
Tableau B.4 – Interfaces de service exigées dans l’UC-4.....	366
Tableau B.5 – Interfaces de service exigées dans l’UC-6.....	368
Tableau B.6 – Interfaces de service exigées dans l’UC-7	369
Tableau B.7 – Interfaces de service exigées dans l’UC-8.....	370
Tableau D.1 – Paramètres de domaine	387
Tableau D.2 – Eléments du champ dédié au nom différencié du sujet	388
Tableau D.3 – Champs et identificateurs d’objet	389
Tableau D.4 – Jeton OpenID Connect de la MCP	391

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

**MATÉRIELS ET SYSTÈMES DE NAVIGATION
ET DE RADIOCOMMUNICATION MARITIMES –
INTERFACES DE DONNÉES –****Partie 2: Communications sécurisées entre le navire et la terre (SECOM)****AVANT-PROPOS**

- 1) La Commission Electrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, l'IEC – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de l'IEC"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'IEC, participent également aux travaux. L'IEC collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
- 2) Les décisions ou accords officiels de l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
- 3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
- 4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
- 5) L'IEC elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de l'IEC. L'IEC n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
- 6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
- 7) Aucune responsabilité ne doit être imputée à l'IEC, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de l'IEC, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de l'IEC ou de toute autre Publication de l'IEC, ou au crédit qui lui est accordé.
- 8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
- 9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de l'IEC peuvent faire l'objet de droits de brevet. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets.

L'IEC 63173-2 a été établie par le comité d'études 80 de l'IEC: Matériels et systèmes de navigation et de radiocommunication maritimes. Il s'agit d'une Norme internationale.

Le texte de cette Norme internationale est issu des documents suivants:

Projet	Rapport de vote
80/1030/FDIS	80/1039/RVD

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à son approbation.

La langue employée pour l'élaboration de cette Norme internationale est l'anglais.

Le présent document a été rédigé selon les Directives ISO/IEC, Partie 2, il a été développé selon les Directives ISO/IEC, Partie 1 et les Directives ISO/IEC, Supplément IEC, disponibles sous www.iec.ch/members_experts/refdocs. Les principaux types de documents développés par l'IEC sont décrits plus en détail sous www.iec.ch/standardsdev/publications.

Une liste de toutes les parties de la série IEC 63173, publiées sous le titre général *Matériels et systèmes de navigation et de radiocommunication maritimes – Interfaces de données*, se trouve sur le site web de l'IEC.

Le comité a décidé que le contenu du présent document ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous webstore.iec.ch dans les données relatives au document recherché. A cette date, le document sera

- reconduit,
- supprimé,
- remplacé par une édition révisée, ou
- amendé.

IMPORTANT – Le logo "colour inside" qui se trouve sur la page de couverture de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une imprimante couleur.

INTRODUCTION

L'e-navigation a été définie comme le moyen de fournir des informations électroniques de manière harmonisée et les services maritimes ont été spécifiés par l'Organisation maritime internationale (OMI). Les services maritimes sont des services opérationnels pour les acteurs à terre et à bord. Pour rendre les services maritimes interopérables entre différents acteurs et systèmes de différents fabricants, des normes, des spécifications et des lignes directrices sur plusieurs niveaux sont exigées, par exemple pour les services techniques et les formats de données/produits. Les services techniques comprennent un ensemble de solutions techniques et de moyens de communication permettant de fournir un service maritime. Le Plan de mise en œuvre de la stratégie en matière d'e-navigation (SIP) de l'OMI exige que tous les services maritimes soient conformes à la S-100 de l'OHI comme base de référence. En outre, il est attendu de l'IEC qu'elle mette en œuvre les détails décrits dans le SIP.

Le standard de communications sécurisées (SECOM, SEcure COMMunications) entre le navire et la terre fournit des normes pour l'échange sécurisé de données avec les services techniques. En outre, il comporte une conception d'interface de service technique conforme aux lignes directrices et aux modèles de service définis par l'AIMS et partiellement inclus dans la S-100 de l'OHI.

Le SECOM spécifie des interfaces de service (API) pour l'échange de données, les mesures de protection des données pour permettre des communications sécurisées et des interfaces pour la découvrabilité des services. Le SECOM est applicable aux produits basés sur la S-100 de l'OHI, mais aussi à d'autres formats de données (données utiles), c'est-à-dire qu'il est généralement indépendant du type de données échangées.

La normalisation d'une interface de service commune pour l'échange de données permet une interopérabilité technique plus étendue, la même interface de service pouvant être utilisée pour échanger des informations indépendamment de leur utilisation opérationnelle.

En conséquence, l'objectif du SECOM est le suivant:

- faciliter l'échange d'informations normalisées, par exemple pour les produits basés sur la S-100 de l'OHI qui font partie des services maritimes, tels que les plans de route, les mises à jour des cartes nautiques et les avertissements de navigation;
- faciliter l'interopérabilité entre les systèmes TI maritimes;
- réduire la nécessité de prendre en charge de nombreuses conceptions de services différentes (propriétaires);
- tirer parti des avantages de l'architecture orientée services dans les communications maritimes, par exemple pour permettre aux systèmes des navires d'interagir avec les systèmes portuaires lors du premier appel à un port spécifique.

MATÉRIELS ET SYSTÈMES DE NAVIGATION ET DE RADIOCOMMUNICATION MARITIMES – INTERFACES DE DONNÉES –

Partie 2: Communications sécurisées entre le navire et la terre (SECOM)

1 Domaine d'application

Le domaine d'application du SECOM comprend des interfaces (API) pour l'échange de données (services d'information), des mesures de sécurité de l'information pour permettre des communications sécurisées et des interfaces pour la découvrabilité des services. Le SECOM assure l'interopérabilité technique, où la même interface de service est utilisée pour l'échange d'informations indépendamment de son utilisation opérationnelle, jusqu'au niveau de l'échange d'informations en ligne sécurisé. Bien que conçu pour les produits basés sur la S-100 de l'OHI, le SECOM ne dépend pas techniquement des données utiles et est également applicable à d'autres types de données.

Les communications entre services d'information SECOM pour l'échange de données sont basées sur des services web sur IP. Les liens du "dernier kilomètre" entre un service d'information SECOM et l'application d'utilisateur ne sont pas définis dans le présent document et, par conséquent, la technologie de communication entre l'API du fournisseur et un système navire/terre peut être aussi bien basée sur IP que non basée sur IP. L'Annexe D informative décrit une mise en œuvre de celles-ci. Elle permet différentes solutions entre le service et les systèmes/applications à terre/du navire.

Le SECOM ne définit pas la couche physique ou la couche de liaison pour le transport des données entre services d'information SECOM, mais exige que le transport prenne en charge la communication IP. Le SECOM est applicable aux services publics (gouvernementaux) et privés (entreprises). Le SECOM est applicable aux communications navire-terre et terre-navire, et peut être utilisé pour les communications navire-navire.

2 Références normatives

Les documents suivants sont cités dans le texte de sorte qu'ils constituent, pour tout ou partie de leur contenu, des exigences du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

OHI, S-100:2018, *Modèle universel de données hydrographiques*, éd. 4.0.0

RFC 2315, *PKCS #7: Cryptographic Message Syntax* (disponible en anglais seulement)

RFC 2459, *Internet X.509 Public-key infrastructure and attribute certificate frameworks* (disponible en anglais seulement)

RFC 2818, *HTTP Over TLS (2000)* (disponible en anglais seulement)

RFC 2986, *PKCS #10: Certification Request Syntax Specification* (disponible en anglais seulement)

RFC 4122, *A Universally Unique IDentifier (UUID) URN Namespace* (disponible en anglais seulement)

RFC 5246, *TLS version 1.2 (2008)* (disponible en anglais seulement)

RFC 5280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile* (disponible en anglais seulement)

RFC 6960, *X.509 Internet Public Key Infrastructure, Online Certificate Status Protocol – OCSP* (disponible en anglais seulement)

RFC 7231, *Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content* (disponible en anglais seulement)

RFC 8446, *TLS version 1.3 (2018)* (disponible en anglais seulement)