

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)**



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2022 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester. If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de l'IEC ou du Comité national de l'IEC du pays du demandeur. Si vous avez des questions sur le copyright de l'IEC ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de l'IEC de votre pays de résidence.

IEC Secretariat
3, rue de Varembe
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
info@iec.ch
www.iec.ch

About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigendum or an amendment might have been published.

IEC publications search - webstore.iec.ch/advsearchform

The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee, ...). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished

Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and once a month by email.

IEC Customer Service Centre - webstore.iec.ch/csc

If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: sales@iec.ch.

IEC Products & Services Portal - products.iec.ch

Discover our powerful search engine and read freely all the publications previews. With a subscription you will always have access to up to date content tailored to your needs.

Electropedia - www.electropedia.org

The world's leading online dictionary on electrotechnology, containing more than 22 300 terminological entries in English and French, with equivalent terms in 19 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

A propos de l'IEC

La Commission Electrotechnique Internationale (IEC) est la première organisation mondiale qui élabore et publie des Normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications IEC

Le contenu technique des publications IEC est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

Recherche de publications IEC - webstore.iec.ch/advsearchform

La recherche avancée permet de trouver des publications IEC en utilisant différents critères (numéro de référence, texte, comité d'études, ...). Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

IEC Just Published - webstore.iec.ch/justpublished

Restez informé sur les nouvelles publications IEC. Just Published détaille les nouvelles publications parues. Disponible en ligne et une fois par mois par email.

Service Clients - webstore.iec.ch/csc

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: sales@iec.ch.

IEC Products & Services Portal - products.iec.ch

Découvrez notre puissant moteur de recherche et consultez gratuitement tous les aperçus des publications. Avec un abonnement, vous aurez toujours accès à un contenu à jour adapté à vos besoins.

Electropedia - www.electropedia.org

Le premier dictionnaire d'électrotechnologie en ligne au monde, avec plus de 22 300 articles terminologiques en anglais et en français, ainsi que les termes équivalents dans 19 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

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.....	22
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 Pagination Object.....	34
5.6.6 Content typeEnum	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 signature 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 KI.....	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 conditions	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 simulations	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 F11 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*