ISO/IEC 9594-11:2020-12 (E)

Information technology - Open systems interconnection directory - Part 11: Protocol specifications for secure operations

Contents

		Page
SECTION 1 – GENERAL		1
1	Scope	1
2	Normative references	1
	2.1 Identical Recommendations | International Standards	1
	2.2 Other references	1
3	Definitions	2
	3.1 OSI Reference Model definitions	2
	3.2 Directory model definitions	2
	3.3 Public-key and attribute certificate definitions	2
	3.4 Terms specified by this Recommendation | International Standard	2
4	Abbreviations	3
5	Conventions	4
6	Common data types and special cryptographic algorithms	4
	6.1 Introduction	4
	6.2 ASN.1 information object class specification tool	4
	6.3 Multiple-cryptographic algorithm specifications	6
	6.4 Key establishment algorithms	7
	6.5 Multiple-cryptographic algorithm-value pairs	9
	6.6 Formal specification of encipherment	11
7	General concepts for securing protocols	11
	7.1 Introduction	11
	7.2 Protected protocol plug-in concept	12
	7.3 Communications structure	12
	7.4 Another view of the relationship between the wrapper protocol and the protected protocol	12
	7.5 Structure of application protocol data unit	13
	7.6 Exception conditions	13
SECTION 2 – THE WRAPPER PROTOCOL		14
8	Wrapper protocol general concepts	14
	8.1 Introduction	14
	8.2 UTC time specification	14
	8.3 Use of alternative cryptographic algorithms	14
	8.4 General on establishing shared keys	14
	8.5 Sequence numbers	15
	8.6 Use of invocation identification in the wrapper protocol	15
	8.7 Mapping to underlying services	15
	8.8 Definition of protected protocols	15
	8.9 Overview of wrapper protocol data units	15
9	Association management	16
	9.1 Introduction to association management	16
	9.2 Association handshake request	16
	9.3 Association accept	18
	9.4 Association reject due to security issues	19
	9.5 Association reject by the protected protocol	20
	9.6 Handshake security abort	21
	9.7 Handshake abort by protected protocol	21

9.8 Data transfer security abort 22
9.9 Abort by protected protocol 22
9.10 Release request WrPDU 23
9.11 Release response WrPDU 23
9.12 Release collision 24
10 Data transfer phase 24
10.1 Symmetric keys renewal 24
10.2 Data transfer by the client 24
10.3 Data transfer by the server 26
11 Information flow 28
11.1 Purpose and general model 28
11.2 Protected protocol SAOC 29
11.3 Wrapper SAOC 29
12 Wrapper error handling 32
12.1 General 32
12.2 Checking of a wrapper handshake request 32
12.3 Checking of a wrapper handshake accept 33
12.4 Checking of data transfer WrPDUs 34
12.5 Wrapper diagnostic codes 36
SECTION 3 – PROTECTED PROTOCOLS 37
13 Authorization and validation list management 37
13.1 General on authorization and validation management 37
13.2 Defined protected protocol data unit (PrPDU) types 37
13.3 Authorization and validation management protocol initialization request 38
13.4 Authorization and validation management protocol initialization accept9 38
13.5 Authorization and validation management protocol initialization reject 38
13.6 Authorization and validation management protocol initialization abort 38
13.7 Add authorization and validation list request 39
13.8 Add authorization and validation list response 40
13.9 Replace authorization and validation list request 40
13.10 Replace authorization and validation list response 40
13.11 Delete authorization and validation list request 41
13.12 Delete authorization and validation list response 41
13.13 Authorization and validation list abort 42
13.14 Authorization and validation list error codes 42
14 Certification authority subscription protocol 43
14.1 Certification authority subscription introduction 43
14.2 Defined protected protocol data unit (PrPDU) types 43
14.3 Certification authority subscription protocol initialization request 43
14.4 Certification authority subscription protocol initialization accept 44
14.5 Certification authority subscription protocol initialization reject 44
14.6 Certification authority subscription protocol initialization abort 44
14.7 Public-key certificate subscription request 44
14.8 Public-key certificate subscription response 45
14.9 Public-key certificate un-subscription request 46
14.10 Public-key certificate un-subscription response 46
14.11 Public-key certificate replacements request 47
14.12 Public-key certificate replacement response 48
14.13 End-entity public-key certificate updates request 49
14.14 End-entity public-key certificate updates response 49
14.15 Certification authority subscription abort 50
14.16 Certification authority subscription error codes 50
15 Trust broker protocol 51
15.1 Introduction 51
15.2 Defined protected protocol data unit (PrPDU) types 51
15.3 Trust broker protocol initialization request 51
15.4 Trust broker protocol initialization accept 52
15.5 Trust broker protocol initialization reject 52

15.6 Trust broker protocol initialization abort 52
15.7 Trust broker request syntax 52
15.8 Trust broker response syntax 53
15.9 Trust broker error information 53
Annex A − Crypto Tools in ASN.1 55
Annex B − Wrapper protocol in ASN.1 58
Annex C − Protected protocol interface to the wrapper protocol 63
Annex D − Cryptographic algorithms 65
Annex E − Authorization and validation list management in ASN.1 67
Annex F − Certification authority subscription in ASN.1 70
Annex G −Trust broker in ASN.1 74
Annex H − Migration of cryptographic algorithms 76
H.1 Introduction 76
H.2 Negotiation of cryptographic algorithms 76
H.3 Non-negotiable digital signature algorithms 77
Annex I − Auxiliary specifications 80
Bibliography 85