

# ISO/IEC 9594-11:2025-08 (E)

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

---

<b>Contents</b>		<b>Page</b>
SECTION 1 – GENERAL.....		1
1	Scope .....	1
2	Normative references .....	1
2.1	Identical Recommendations   International Standards.....	1
2.2	Paired Recommendations   International Standards equivalent in technical content .....	1
2.3	International Standards .....	2
2.4	Other references.....	2
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 defined in this Recommendation   International Standard .....	3
4	Abbreviations .....	4
5	Conventions.....	5
6	Communication model .....	5
7	Common data types and special cryptographic algorithms .....	5
7.1	Introduction .....	5
7.2	ASN.1 information object class specification tool.....	5
7.3	Parameterized data types .....	7
7.4	Multiple cryptographic algorithm specifications .....	9
7.5	Parameterized data types for providing multiple-cryptographic algorithm-values.....	15
7.6	Formal specification of encipherment .....	16
8	Symmetric-key algorithms .....	17
8.1	Introduction to symmetric-key algorithms.....	17
8.2	Advance encryption standard (AES) – symmetric-key algorithms.....	18
8.3	Camellia symmetric-key algorithms .....	21
8.4	SEED – symmetric-key algorithms .....	24
8.5	SM4 – symmetric-key algorithms.....	26
9	Public-key and digital signature algorithms .....	28
10	Key establishment algorithms .....	28
10.1	General .....	28
10.2	Diffie-Hellman over prime field.....	28
10.3	Elliptic curve Diffie-Hellman .....	30
10.4	Key derivation .....	31
11	General concepts for securing protocols .....	32
11.1	Introduction .....	32
11.2	Protected protocol plug-in concept.....	32
11.3	Communication structure.....	32
11.4	Another view of the relationship between the wrapper protocol and the protected protocol.....	33
11.5	Structure of the application protocol data unit.....	33
11.6	Exception conditions .....	33
SECTION 2 – THE WRAPPER PROTOCOL.....		34
12	Wrapper protocol general concepts .....	34
12.1	Introduction .....	34
12.2	UTC time specification.....	34

12.3	Use of alternative cryptographic algorithms.....	34
12.4	Establishment of symmetric keys .....	34
12.5	Sequence numbers .....	35
12.6	Use of invocation identification in the wrapper protocol .....	35
12.7	Mapping to underlying services.....	35
12.8	Addressing of communicating entities.....	35
12.9	Definition of protected protocols.....	35
12.10	Overview of wrapper protocol data units.....	35
13	Association management.....	36
13.1	Introduction to association management .....	36
13.2	Association handshake request .....	36
13.3	Association handshake accept .....	37
13.4	Association reject due to security issues.....	38
13.5	Association reject by the protected protocol.....	39
13.6	Handshake security abort.....	40
13.7	Handshake abort by protected protocol .....	40
13.8	Data transfer security abort.....	41
13.9	Abort by protected protocol.....	41
13.10	Release request WrPDU .....	42
13.11	Release response WrPDU.....	42
13.12	Release collision .....	43
14	Data transfer phase .....	43
14.1	Symmetric keys renewal.....	43
14.2	Data transfer by the client.....	44
14.3	Data transfer by the server .....	45
15	Information flow.....	48
15.1	Purpose and general model.....	48
15.2	Protected protocol SAOC .....	49
15.3	Wrapper SAOC.....	49
16	Wrapper error handling .....	52
16.1	General .....	52
16.2	Checking of a wrapper handshake request.....	52
16.3	Checking of a wrapper handshake accept.....	53
16.4	Checking of data transfer WrPDUs .....	54
16.5	Wrapper diagnostic codes.....	56
17	End-to-end communications.....	57
SECTION 3 – PROTECTED PROTOCOLS .....		58
18	Authorization and validation list management .....	58
18.1	General on authorization and validation management.....	58
18.2	Defined protected protocol data unit types .....	58
18.3	Authorization and validation management protocol initialization request .....	59
18.4	Authorization and validation management protocol initialization accept.....	59
18.5	Authorization and validation management protocol initialization reject .....	59
18.6	Authorization and validation management protocol initialization abort.....	59
18.7	Add authorization and validation list request .....	60
18.8	Add authorization and validation list response.....	61
18.9	Replace authorization and validation list request .....	61
18.10	Replace authorization and validation list response .....	61
18.11	Delete authorization and validation list request.....	62
18.12	Delete authorization and validation list response .....	62
18.13	Authorization and validation list abort .....	63
18.14	Authorization and validation list error codes.....	63
19	Certification authority subscription protocol.....	64
19.1	Certification authority subscription introduction.....	64
19.2	Defined protected protocol data unit types .....	64
19.3	Certification authority subscription protocol initialization request.....	65
19.4	Certification authority subscription protocol initialization accept.....	65
19.5	Certification authority subscription protocol initialization reject .....	65

19.6	Certification authority subscription protocol initialization abort.....	65
19.7	Public-key certificate subscription request .....	66
19.8	Public-key certificate subscription response.....	66
19.9	Public-key certificate un-subscription request.....	67
19.10	Public-key certificate un-subscription response .....	68
19.11	Public-key certificate replacements request.....	69
19.12	Public-key certificate replacement response.....	69
19.13	End-entity public-key certificate updates request.....	70
19.14	End-entity public-key certificate updates response .....	71
19.15	Certification authority subscription abort .....	72
19.16	Certification authority subscription error codes.....	72
20	Trust broker protocol.....	72
20.1	Introduction .....	72
20.2	Defined protected protocol data unit types .....	73
20.3	Trust broker protocol initialization request.....	73
20.4	Trust broker protocol initialization accept.....	73
20.5	Trust broker protocol initialization reject .....	73
20.6	Trust broker protocol initialization abort.....	74
20.7	Trust broker request syntax .....	74
20.8	Trust broker response syntax .....	74
20.9	Trust broker error information .....	75
Annex A	Crypto Tools in ASN.1.....	76
Annex B	General cryptographic algorithms .....	81
Annex C	Wrapper protocol in ASN.1.....	92
Annex D	Protected protocol interface to the wrapper protocol .....	97
Annex E	Authorization and validation list management in ASN.1 .....	99
Annex F	Certification authority subscription in ASN.1.....	102
Annex G	Trust broker in ASN.1 .....	106
Annex H	Migration of cryptographic algorithms .....	108
H.1	Migration of cryptographic algorithms.....	108
H.2	Migration tools or migration approaches.....	109
H.3	Migration of public-key certificates and other data types using the extension mechanism .....	110
H.4	General migration approach for communication protocols .....	110
H.5	Use of multiple and choice cryptographic algorithms .....	111
Annex I	Auxiliary specifications .....	114
Annex J	Amendments and corrigenda.....	119
Bibliography	.....	120