

ISO/IEC 11770-3:2015-08 (E)

Information technology - Security techniques - Key management - Part 3: Mechanisms using asymmetric techniques

Contents		Page
Foreword		v
Introduction		vi
1	Scope	1
2	Normative references	1
3	Terms and definitions	2
4	Symbols and abbreviations	7
5	Requirements	9
6	Key derivation functions	9
7	Cofactor multiplication	9
8	Key commitment	10
9	Key confirmation	11
10	Framework for key management	12
10.1	General	12
10.2	Key agreement between two parties	12
10.3	Key agreement between three parties	12
10.4	Secret key transport	13
10.5	Public key transport	13
11	Key agreement	14
11.1	Key agreement mechanism 1	14
11.2	Key agreement mechanism 2	15
11.3	Key agreement mechanism 3	16
11.4	Key agreement mechanism 4	18
11.5	Key agreement mechanism 5	18
11.6	Key agreement mechanism 6	19
11.7	Key agreement mechanism 7	21
11.8	Key agreement mechanism 8	22
11.9	Key agreement mechanism 9	23
11.10	Key agreement mechanism 10	24
11.11	Key agreement mechanism 11	25
11.12	Key agreement mechanism 12	26
12	Secret key transport	27
12.1	Secret key transport mechanism 1	27
12.2	Secret key transport mechanism 2	28
12.3	Secret key transport mechanism 3	30
12.4	Secret key transport mechanism 4	32
12.5	Secret key transport mechanism 5	33
12.6	Secret key transport mechanism 6	35

13	Public key transport	36
13.1	Public key transport mechanism 1	36
13.2	Public key transport mechanism 2	37
13.3	Public key transport mechanism 3	38
Annex A (normative) Object identifiers		40
Annex B (informative) Properties of key establishment mechanisms		47
Annex C (informative) Examples of key derivation functions		49
Annex D (informative) Examples of key establishment mechanisms		56
Annex E (informative) Examples of elliptic curve based key establishment mechanisms		60
Annex F (informative) Example of bilinear pairing based key establishment mechanisms		68
Annex G (informative) Secret key transport		71
Annex H (informative) Patent information		76
Bibliography		80