

ISO/IEC 11770-3:2008-07 (E)

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

Contents		Page
Foreword		iv
Introduction		v
1	Scope	1
2	Normative references	2
3	Terms and definitions	2
4	Symbols and abbreviations	6
5	Requirements	8
6	Key derivation functions	8
7	Cofactor multiplication	9
8	Key commitment	10
9	Key confirmation	10
10	Secret key agreement	12
10.1	Key agreement mechanism 1	12
10.2	Key agreement mechanism 2	13
10.3	Key agreement mechanism 3	14
10.4	Key agreement mechanism 4	16
10.5	Key agreement mechanism 5	17
10.6	Key agreement mechanism 6	18
10.7	Key agreement mechanism 7	20
10.8	Key agreement mechanism 8	22
10.9	Key agreement mechanism 9	23
10.10	Key agreement mechanism 10	24
10.11	Key agreement mechanism 11	25
11	Secret key transport	27
11.1	Key transport mechanism 1	27
11.2	Key transport mechanism 2	28
11.3	Key transport mechanism 3	30
11.4	Key transport mechanism 4	31
11.5	Key transport mechanism 5	33
11.6	Key transport mechanism 6	35
12	Public key transport	37
12.1	Public key distribution without a trusted third party	37
12.2	Public key distribution using a trusted third party	39
Annex A (informative) Properties of key establishment mechanisms		41
Annex B (informative) Examples of key derivation functions		43
Annex C (informative) Examples of key establishment mechanisms		51

Annex D (informative) Examples of elliptic curve based key establishment mechanisms	57
Annex E (informative) Key transport	69
Annex F (normative) ASN.1 module	74
Bibliography	82