ISO/IEC 11770-3:2021-10 (E)

Information security - Key management - Part 3: Mechanisms using asymmetric techniques

Contents

Page

Foreword 5

Introduction 6

1 Scope 1

2 Normative references 2

3 Terms and definitions 2

4 Symbols and abbreviations 8

5 Requirements 10

6 Key derivation functions 11

7 Cofactor multiplication 11

8 Key commitment 12

9 Key confirmation 12

10 Framework for key management 13
10.1 General 13
10.2 Key agreement between two parties 14
10.3 Key agreement between three parties 14
10.4 Secret key transport 15
10.5 Public key transport 15

11 Key agreement 15
11.1 Key agreement mechanism 1 15
11.2 Key agreement mechanism 2 17
11.3 Key agreement mechanism 3 17
11.4 Key agreement mechanism 4 19
11.5 Key agreement mechanism 5 20
11.6 Key agreement mechanism 6 21
11.7 Key agreement mechanism 7 23
11.8 Key agreement mechanism 8 24
11.9 Key agreement mechanism 9 25
11.10 Key agreement mechanism 10 26
11.11 Key agreement mechanism 11 27
11.12 Key agreement mechanism 12 28
11.13 Key agreement mechanism 13 29
11.14 Key agreement mechanism 14 30
11.15 Key agreement mechanism 15 31

12 Secret key transport 32
12.1 Secret key transport mechanism 1 32
12.2 Secret key transport mechanism 2 34
12.3 Secret key transport mechanism 3 35
12.4 Secret key transport mechanism 4 37

12.5 Secret key transport mechanism 5 38
12.6 Secret key transport mechanism 6 41

13 Public key transport 42
13.1 Public key transport mechanism 1 42
13.2 Public key transport mechanism 2 43
13.3 Public key transport mechanism 3 44

Annex A (normative) Object identifiers 46

Annex B (informative) Properties of key establishment mechanisms 55

Annex C (informative) Examples of key derivation functions 58

Annex D (informative) Examples of key establishment mechanisms 66

Annex E (informative) Examples of elliptic curve based key establishment mechanisms 70

Annex F (informative) Example of bilinear pairing based key establishment mechanisms 80

Annex G (informative) Secret key transport 84

Bibliography 88