ISO/IEC 11770-2:2008-06 (E)

Information technology - Security techniques - Key management - Part 2: Mechanisms using symmetric techniques

Contents

Page

Foreword iv

1 Scope 1

2 Normative references 1

3 Terms and definitions 2

4 Symbols and abbreviated terms 3

5 Requirements 4

6 Point-to-point key establishment 5
6.1 Key Establishment Mechanism 1 5
6.2 Key Establishment Mechanism 2 5
6.3 Key Establishment Mechanism 3 6
6.4 Key Establishment Mechanism 4 7
6.5 Key Establishment Mechanism 5 7
6.6 Key Establishment Mechanism 6 8

7 Mechanisms using a Key Distribution Centre 9
7.1 Key Establishment Mechanism 7 10
7.2 Key Establishment Mechanism 8 11
7.3 Key Establishment Mechanism 9 12
7.4 Key Establishment Mechanism 10 14

8 Mechanisms using a Key Translation Centre 15
8.1 Key Establishment Mechanism 11 16
8.2 Key Establishment Mechanism 12 16
8.3 Key Establishment Mechanism 13 18

Annex A (normative) ASN.1 module 21

Annex B (informative) Properties of key establishment mechanisms 23

Annex C (informative) Auxiliary techniques 25

Bibliography 27