

ISO/IEC 11770-2:2018 (E)

IT Security techniques — Key management — Part 2: Mechanisms using symmetric techniques

Contents

	Foreword
	Introduction
1	Scope
2	Normative references
3	Terms and definitions
4	Symbols and abbreviated terms
5	Requirements
6	Point-to-point key establishment
6.1	General
6.2	Key establishment mechanism 1
6.3	Key establishment mechanism 2
6.4	Key establishment mechanism 3
6.5	Key establishment mechanism 4
6.6	Key establishment mechanism 5
6.7	Key establishment mechanism 6
7	Mechanisms using a Key Distribution Centre
7.1	General
7.2	Key establishment mechanism 7
7.3	Key establishment mechanism 8
7.4	Key establishment mechanism 9
7.5	Key establishment mechanism 10
8	Mechanisms using a Key Translation Centre
8.1	General
8.2	Key establishment mechanism 11
8.3	Key establishment mechanism 12
8.4	Key establishment mechanism 13
Annex A	(normative) Object identifiers
A.1	Formal definition
A.2	Use of subsequent object identifiers
Annex B	(informative) Properties of key establishment mechanisms
Annex C	(informative) Auxiliary techniques
C.1	Data integrity
C.1.1	Integrity of individual messages
C.1.2	Integrity of two-part messages
C.2	Key calculation
C.3	Key confirmation
C.4	Combination of key establishment and entity authentication