ISO/IEC 11770-4:2006-05 (E)

Information technology - Security techniques - Key management - Part 4: Mechanisms based on weak secrets

Contents

Page

Foreword iv

1 Scope 1

2 Normative references 2

3 Terms and definitions 2

4 Symbols and notation 6

5 Requirements 8

6 Password-authenticated key agreement 9 6.1 Key Agreement Mechanism 1 10
6.1.1 Prior shared parameters 10
6.1.2 Functions 10
6.1.3 Key agreement operation 12
6.2 Key Agreement Mechanism 2 13
6.2.1 Prior shared parameters 14
6.2.2 Functions 14
6.2.3 Key agreement operation 16
6.3 Key Agreement Mechanism 3 17
6.3.1 Prior shared parameters 17
6.3.2 Functions 17
6.3.3 Key agreement operation 20

7 Password-authenticated key retrieval 21
7.1 Key Retrieval Mechanism 1 22
7.1.1 Prior shared parameters 22
7.1.2 Functions 22
7.1.3 Key retrieval operation 23

Annex A (normative) Functions for Data Type Conversion 24

Annex B (normative) ASN.1 Module 28

Annex C (informative) Guidance on Choice of Parameters 30

Bibliography 32