ISO/IEC 11770-4:2017-11 (E)

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

Contents

Page

Foreword iv

Introduction v

1 Scope 1

2 Normative reference 1

3 Termsanddefinitions 1

4 Symbols and abbreviated terms 6

5 Requirements 8

6 Password-authenticated key agreement 10
6.1 General 10
6.2 Balanced Key Agreement Mechanism 1 (BKAM1) 10
6.2.1 General 10
6.2.2 Prior shared parameters 11
6.2.3 Functions 11
6.2.4 Key agreement operation 14
6.3 Balanced Key Agreement Mechanism 2 (BKAM2) 15
6.3.1 General 15
6.3.2 Prior shared parameters 15
6.3.3 Functions 16
6.3.4 Key agreement operation 19
6.4 Augmented Key Agreement Mechanism 1 (AKAM1) 22
6.4.1 General 22
6.4.2 Prior shared parameters 22
6.4.3 Functions 23
6.4.4 Key agreement operation 24
6.5 Augmented Key Agreement Mechanism 2 (AKAM2) 25
6.5.1 General 25
6.5.2 Prior shared parameters 26
6.5.3 Functions 26
6.5.4 Key agreement operation 29
6.6 Augmented Key Agreement Mechanism 3 (AKAM3) 30
6.6.1 General 30
6.6.2 Prior shared parameters 30
6.6.3 Functions 31
6.6.4 Key agreement operation 33

7 Password-authenticated key retrieval 35
7.1 General 35
7.2 Key Retrieval Mechanism 1 (KRM1) 35
7.2.1 General 35
7.2.2 Prior shared parameters 36
7.2.3 Functions 36
7.2.4 Key retrieval operation 37

Annex A (normative) Functions for data type conversion 38

Annex B (normative)Objectidentifiers 42

Annex C (informative) Guidance on choice of parameters 45

Bibliography 47