ISO/IEC 11770-7:2021 (E)

Information security — Key management — Part 7: Cross-domain password-based authenticated key exchange

Contents

Foreword

Introduction

1 Scope

2 Normative references

3 Terms and definitions

4 Symbols and abbreviated terms

4.1 Abbreviated terms
4.2 Symbols

5 Requirements

6 Mechanisms

6.1 General
6.2 Sub-protocols and functions
6.2.1 General
6.2.2 Two-party password-based authenticated key exchange
6.2.3 Two-party asymmetric-key authenticated key exchange
6.2.4 Two-party symmetric-key authenticated key exchange
6.2.5 Two-party non-interactive key exchange
6.2.6 Session identity function
6.3 Mechanism 1
6.3.1 General
6.3.2 Prior shared parameters
6.3.3 Key exchange operation
6.3.3.1 General
6.3.3.2 Ephemeral public key construction (M1A)
6.3.3.3 Ephemeral public key construction (M1B)
6.3.3.4 Local password key exchange (M2A)
6.3.3.5 Local password key exchange (M2B)
6.3.3.6 Local client authentication (M3A)
6.3.3.7 Local client authentication (M3B)
6.3.3.8 Authentication token acquirement (M4A)
6.3.3.9 Authentication token acquirement (M4B)
6.3.3.10 Cross-domain key exchange (M5A)
6.3.3.11 Cross-domain key exchange (M5B)
6.4 Mechanism 2
6.4.1 General
6.4.2 Prior shared parameters
6.4.3 Key exchange operation
6.4.3.1 General
6.4.3.2 Client authentication key generation (M1A)
6.4.3.3 Client authentication key generation (M1B)
6.4.3.4 Local password-based key exchange (M2A)
6.4.3.5 Local password-based key exchange (M2B)
6.4.3.6 Local client authentication (M3A)
6.4.3.7 Local client authentication (M3B)
6.4.3.8 Client certificate acquirement (M4A)
6.4.3.9 Client certificate acquirement (M4B)

6.4.3.10 Client certificate validation (M5A)
6.4.3.11 Client certificate validation (M5B)
6.4.3.12 Cross-domain key exchange (M6A)
6.4.3.13 Cross-domain key exchange (M6B)
6.5 Mechanism 3
6.5.1 General
6.5.2 Prior shared parameters
6.5.3 Key exchange operation
6.5.3.1 General
6.5.3.2 Ephemeral public key construction (M1A)
6.5.3.3 Ephemeral public key construction (M1B)
6.5.3.4 Local password key exchange (M2A)
6.5.3.5 Local password key exchange (M2B)
6.5.3.6 Local client authentication (M3A)
6.5.3.7 Local client authentication (M3B)
6.5.3.8 Client key acquirement (M4A)
6.5.3.9 Client key acquirement (M4B)
6.5.3.10 Cross-domain key exchange (M5A)
6.5.3.11 Cross-domain key exchange (M5B)

Annex A (normative) Object identifiers

Annex B (normative) Conversion functions

B.1 BS2I
B.2 BS2OS
B.3 FE2I
B.4 FE2OS
B.5 GE2OSx
B.6 I2BS
B.7 I2OS

Page count: 26