ISO/IEC 11770-5:2020 (E)

Information security — Key management — Part 5: Group key management

Contents

Foreword

Introduction

1 Scope

2 Normative references

3 Terms and definitions

4 Symbols and abbreviated terms

5 Requirements

6 Tree-based key establishment mechanisms

6.1 General model
6.2 Joining process
6.3 Leaving process
6.4 Rekeying process
6.5 Logical key structure
6.5.1 General
6.5.2 Star-based structure
6.5.3 d-ary tree-based structure
6.5.4 General tree-based structure
6.6 Symmetric key-based key establishment mechanisms
6.6.1 General
6.6.2 Mechanism 1 — Key establishment mechanism with individual rekeying
6.6.3 Mechanism 2 — Key establishment mechanism with batch rekeying

7 Key chain-based group key management with limited forward key chain

7.1 General model
7.2 Calculations by the key distribution centre
7.2.1 Key chains
7.2.2 Group forward secrecy
7.2.3 Group backward secrecy
7.2.4 Forward and backward secrecy
7.3 Calculations by the client entity

Annex A (normative) Object identifiers

Annex B (informative) Load-balancing mechanism for a general tree-based structure

Page count: 18