ISO/IEC 11770-5:2011-12 (E)

Information technology - Security techniques - Key management - Part 5: Group key management

Contents

Page

Foreword iv

Introduction v

1 Scope 1

2 Normative references 1

3 Terms and definitions 1

4 Symbols and abbreviations 4

5 Requirements 5

6 Tree based key establishment mechanisms for multiple entities 5
6.1 General model 5
6.2 Joining process 6
6.3 Leaving process 6
6.4 Rekeying process 6
6.5 Logical key structure 7
6.6 Symmetric key based key establishment mechanisms 8

7 Key chain based group key management 12

8 Key chain based group key management with unlimited forward key chain 13
8.1 Calculations by the key distribution centre 13
8.2 Calculations by the client entity 15

9 Key chain based group key management with limited forward key chain 18
9.1 Calculations by the key distribution centre 18
9.2 Calculations by the client entity 19

Annex A (normative) Object identifiers 20

Annex B (informative) Load balancing mechanism for general tree based structure 21

Bibliography 22