

# ISO/IEC 24767-2:2009-01 (E)

## Information technology – Home network security – Part 2: Internal security services – Secure communication protocol for middleware (SCPM)

---

### CONTENTS

- FOREWORD..... 5
- 1 Scope..... 6
- 2 Normative references ..... 6
- 3 Terms, definitions and abbreviations ..... 7
  - 3.1 Terms and definitions ..... 7
  - 3.2 Abbreviations ..... 8
- 4 Conformance ..... 8
- 5 Design considerations of internal security services for home networks ..... 9
  - 5.1 General ..... 9
  - 5.2 Issues addressed by security measures ..... 10
    - 5.2.1 General ..... 10
    - 5.2.2 Unsafe transmission ..... 10
    - 5.2.3 Intentional misuse ..... 10
  - 5.3 Design principles of security measures..... 11
    - 5.3.1 General ..... 11
    - 5.3.2 Minimization of resources for cost-saving ..... 11
    - 5.3.3 Independence of communication media ..... 11
    - 5.3.4 Independence of cryptographic algorithms..... 11
    - 5.3.5 Extensibility of variant usages ..... 11
- 6 Secure communication protocol for middleware (SCPM)..... 11
  - 6.1 General ..... 11
  - 6.2 What is SCPM..... 12
  - 6.3 How does SCPM work ..... 12
  - 6.4 Where is SCPM going to be implemented ..... 14
  - 6.5 Usage levels of SCPM..... 14
  - 6.6 Usage keys of SCPM..... 15
- 7 Secure message frame format..... 15
  - 7.1 General communication frame ..... 15
    - 7.1.1 General ..... 15
    - 7.1.2 Header (HD) ..... 16
    - 7.1.3 Source address (SA) and destination address (DA) ..... 16
    - 7.1.4 Byte counter (BC)..... 16
    - 7.1.5 Application Data (ADATA) ..... 16
  - 7.2 Secure frame structure ..... 16
    - 7.2.1 General ..... 16
    - 7.2.2 Secure header (SHD) ..... 17
    - 7.2.3 Sequence number field (SNF)..... 18
    - 7.2.4 Plain text data part byte counter (PBC)..... 18
    - 7.2.5 Plain text application data (PADATA)..... 18
    - 7.2.6 Block check code (BCC) ..... 18
    - 7.2.7 Padding (PDG) ..... 18
    - 7.2.8 Message data authentication signature (MDAS)..... 19
- 8 SCPM processing..... 19
  - 8.1 Algorithms and processing ..... 19

8.1.1	General .....	19
8.1.2	Encryption algorithms and encryption calculation.....	19
8.1.3	Data authentication algorithms and data authentication calculation.....	19
8.1.4	Cipher block chaining (CBC) mode .....	20
8.1.5	SNF initialisation and verification.....	20
8.1.6	Initialisation vector (IV) value .....	21
8.2	Secure message frame processing.....	22
8.2.1	General .....	22
8.2.2	Message frame processing of data authentication only .....	22
8.2.3	Message frame processing of confidentiality only .....	23
8.2.4	Message frame processing of data authentication and confidentiality .....	25
9	Key management.....	27
9.1	General .....	27
9.2	Key initialisation .....	27
9.2.1	Initialisation of a user key .....	27
9.2.2	Initialisation of service provider keys .....	30
9.2.3	Initialisation of maker key .....	32
9.3	Master key update.....	32
9.3.1	Master key update between KSN and a device .....	32
9.3.2	Key synchronization .....	36
9.3.3	Master key update request from a device .....	38
Annex A (informative)	To authorize a key setting node.....	41
Bibliography.....		42
Figure 1	– Use of combined technologies against security risks .....	10
Figure 2	– General message frame versus secure message frame.....	13
Figure 3	– Round trip communications of SCPM .....	13
Figure 4	– Position of SCPM.....	14
Figure 6	– Secure message frame .....	17
Figure 7	– Data format of a secure header (SHD) .....	17
Figure 8	– Encryption employing AES-CBC with 128-bit key .....	19
Figure 9	– Data authentication calculation .....	20
Figure 10	– Sequences of SNF initialisation.....	21
Figure 11	– Calculation of IV value .....	21
Figure 13	– Secure message frames employing encryption service.....	25
Figure 14	– Secure message frames employing encryption and data authentication services.....	27
Figure 15	– Sequences of user key initialisation .....	29
Figure 16	– Secure message frames of “user key” initialisation.....	30
Figure 17	– Sequences of service provider key initialisation.....	31
Figure 19	– Sequences of master key updates controlled by KSN using the DH algorithm .....	34
Figure 21	– Secure message frames of master key update – Key exchange using DH shared secret key .....	36
Figure 22	– Sequences of master key update for synchronization .....	37
Figure 23	– A state transition diagram of a device during master key update controlled by KSN.....	38

Figure 24 – Sequences of master key update requested from a device .....	39
Figure 25 – A state transition diagram of a device when master key update is requested from the device.....	40
Figure A.1 – An example to authenticate the KSN.....	41