ISO/IEC 24767-2

Edition 1.0 2009-01

INTERNATIONAL STANDARD

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

INTERNATIONAL ELECTROTECHNICAL COMMISSION

PRICE CODE R

ICS 35.200

ISBN 978-2-88910-838-1

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

INFORMATION TECHNOLOGY – HOME NETWORK SECURITY –

Part 2: Internal security services – Secure communication protocol for middleware (SCPM)

FOREWORD

1) ISO (International Organization for Standardization) and IEC (International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards. Their preparation is entrusted to technical committees; any ISO and IEC member body interested in the subject dealt with may participate in this preparatory work. International governmental and non-governmental organizations liaising with ISO and IEC also participate in this preparation.

2) In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

3) The formal decisions or agreements of IEC and ISO on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC and ISO member bodies.

4) IEC, ISO and ISO/IEC publications have the form of recommendations for international use and are accepted by IEC and ISO member bodies in that sense. While all reasonable efforts are made to ensure that the technical content of IEC, ISO and ISO/IEC publications is accurate, IEC or ISO cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.

5) In order to promote international uniformity, IEC and ISO member bodies undertake to apply IEC, ISO and ISO/IEC publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any ISO/IEC publication and the corresponding national or regional publication should be clearly indicated in the latter.

6) ISO and IEC provide no marking procedure to indicate their approval and cannot be rendered responsible for any equipment declared to be in conformity with an ISO/IEC publication.

7) All users should ensure that they have the latest edition of this publication.

8) No liability shall attach to IEC or ISO or its directors, employees, servants or agents including individual experts and members of their technical committees and IEC or ISO member bodies for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication of, use of, or reliance upon, this ISO/IEC publication or any other IEC, ISO or ISO/IEC publications.

9) Attention is drawn to the normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.

10) Attention is drawn to the possibility that some of the elements of this International Standard may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

International Standard ISO/IEC 24767-2 was prepared by subcommittee 25: Interconnection of information technology equipment, of ISO/IEC joint technical committee 1: Information technology.

The list of all currently available parts of ISO/IEC 24767 series, under the general title *Information technology – Home network security*, can be found on the IEC web site.

This International Standard has been approved by vote of the member bodies, and the voting results may be obtained from the address given on the second title page.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

INFORMATION TECHNOLOGY – HOME NETWORK SECURITY –

Part 2: Internal security services – Secure communication protocol for middleware (SCPM)

1 Scope

This part of ISO/IEC 24767 specifies security in a home network for equipment with limited IT capability. The Secure Communication Protocol for Middleware (SCPM) is particularly designed to support network security (see 5.2) for equipment not capable of supporting Internet security protocols such as IPSec or SSL/TLS. Although this protocol is designed for unsafe transmissions, it may be used on other types of transmissions. Of course, the quality level of the security services of SCPM is not equal with that of the Internet security protocols but will ensure that such middleware can also be connected securely within a home. It is not the intention that SCPM replace existing security mechanisms of protocols that have already been published.

The SCPM provides the security services at the network layer and the protocol does not rely on any specific media transmission. This part of ISO/IEC 24767 contains detailed specifications of the security services supported, the necessary message formats, the information flows and the processing of these pieces of information necessary for the implementation of this protocol.

Therefore, this standard neither addresses media-dependent issues nor an overall security architecture covering every home-networking technology. The protocol specified in this standard is media-independent and covers the security services for the network layer for protocols that do not have a conflicting network-layer addressing scheme. Network layer security services are provided through the use of a combination of cryptographic and security mechanisms.

Each protocol should specify the details of this security implementation. An HES system supporting more than one protocol needs a gateway in between protocols.

Finally, this standard does not define any type of application except for key management which has become essential in any security service. Nonetheless, there are no restrictions on which types of applications may be deployed with SCPM.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 10116, *Information technology – Security techniques – Modes of operation for an n-bit block cipher*

ISO/IEC 11577, *Information technology – Open Systems Interconnection – Network layer security protocol*

ISO/IEC 11770-3, *Information technology – Security techniques – Key management – Part 3: Mechanisms using asymmetric techniques*

ISO/IEC 18033-3, *Information technology – Security techniques – Encryption algorithms – Part 3: Block ciphers*