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)

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 24767-2:2009
https://standards.iteh.ai/catalog/standards/sist/00bafc52-7474-4ff9-9855-519936d30fe4/iso-iec-24767-2-2009

ISO/IEC 24767-2:2009(E)

THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2009 ISO/IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester.

If you have any questions about ISO/IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland
Email: inmail@iec.ch
Web: www.iec.ch

About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

- Catalogue of IEC publications: www.iec.ch/searchpub

The IEC on-line Catalogue enables you to search by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, withdrawn and replaced publications.

- IEC Just Published: www.iec.ch/online_news/justpub

Stay up to date on all new IEC publications. Just Published details twice a month all new publications released. Available on-line and also by email.

- Electropedia: www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing more than 20 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary online.

- Customer Service Centre: www.iec.ch/webstore/custserv

If you wish to give us your feedback on this publication or need further assistance, please visit the Customer Service Centre FAQ or contact us:

Email: csc@iec.ch
Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 24767-2:2009
https://standards.iteh.ai/catalog/standards/sist/00bafc52-7474-4ff9-9855-519f56d50be4/iso-iec-24767-2-2009

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)

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 24767-2:2009
https://standards.iteh.ai/catalog/standards/sist/00bafc52-7474-4ff9-9855-519936d30fe4/iso-iec-24767-2-2009

INTERNATIONAL ELECTROTECHNICAL COMMISSION

PRICE CODE R

ICS 35.200

ISBN 2-8318-1020-6

CONTENTS

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 24767-2:2009
https://standards.iteh.ai/catalog/standards/sist/00bafc52-7474-4ff9-9855-519936d30fe4/iso-iec-24767-2-2009

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 24767-2:2009
https://standards.iteh.ai/catalog/standards/sist/00baefc-52-7474-4ff9-9855-519936d30fe4/iso-iec-24767-2-2009

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 24767-2:2009
https://standards.iteh.ai/catalog/standards/sist/00bafc52-7474-4ff9-9855-519936d30fe4/iso-iec-24767-2-2009

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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.

ISO/IEC 24767-2:2009
https://standards.iteh.ai/catalog/standards/sist/00bcf652-7474-4ff0-9855-[illegible]/iso-iec-24767-2-2009

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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.

ISO/IEC 24767-2:2009
https://standards.iteh.ai/catalog/standards/sist/00bab252-7474-4ff9-9855-519936d30fe4/iso-iec-24767-2-2009

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*

3 Terms, definitions and abbreviations

3.1 Terms and definitions

For the purpose of this document the following definitions apply.

3.1.1
confidentiality
property that information is not made available or disclosed to unauthorized individuals, entities or processes

3.1.2
data authentication
service used to ensure that the source of the data claimed by a party to a communication is correctly verified

3.1.3
data integrity
property that data has not been altered or destroyed in an unauthorized manner

3.1.4
key setting node
entity responsible for key generation/distribution and management

iTeh STANDARD PREVIEW
(standards.iteh.ai)

3.1.5
MAC address
media access control sub-layer of the data-link layer of the communications protocol used

ISO/IEC 24767-2:2009
https://standards.iteh.ai/catalog/standards/sist/00bafc52-7474-4ff9-9855-519936d30fc4/iso-iec-24767-2-2009

3.1.6
message frame
minimum data unit transmitted between a home appliance node and a home appliance control

3.1.7
out of band
use of other mechanisms than the ones required on a communications channel to transmit information

3.1.8
requested service
networked node that responds to service requests

3.1.9
service requester
networked node that issues service requests

3.1.10
user authentication
service used to ensure that the identity claimed by a party to a communication is correctly verified, whereas an authorization service ensures that the identified and authenticated party is entitled to access a particular device or application on the home network

3.1.11
white goods
appliances that are used daily life, for example, air conditioner, refrigerator and so on

3.2 Abbreviations

For the purpose of this document the following abbreviations apply.

ADATA	Application DATA (7.1.5)
BC	Byte Counter [data length in bytes of the following data payload (size of ADATA)]
BCC	Block Check Code (7.2.6)
CBC	Cipher Block Chaining
CPU	Central Processing Unit
DA	Destination Address (of a message frame)
DCL	Data-Link Layer
DES	Data Encryption Standard
DH	Diffie-Hellman (was the first published public-key algorithm and it can be used for key distribution)
DoS	Denial of Services
HD	HeaDer (of the message frame)
HES	Home Electronic System
IP	Internet Protocol
IPSec	IP Security protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IV	Initialisation Vector
KSN	Key Setting Node
MAC	Message Authentication Code
MDAS	Message Data Authentication Signature
PBC	Plain text data part Byte Counter (data length in bytes of the following data payload (size of PADATA))
PDG	PaDdinG
PADATA	Plain text Application DATA
PIN	Personal Identification Number
SA	Source Address (of a message frame)
SCPM	Secure Communication Protocol for Middleware
SHD	Secure Header
SNF	Sequence Number Field
SSL	Secure Sockets Layer
TLS	Transport Layer Security
XOR	eXclusive OR

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 24767-2:2009
https://standards.iteh.ai/catalog/standards/sist/00bafc52-7474-4ff9-9855-519936d30fe4/iso-iec-24767-2-2009

4 Conformance

For conformance to this International Standard the following applies.

a) The structure shall conform to the requirements outlined in Clause 6.

b) The message frame format shall conform to the specifications outlined in Clause 7.

c) The implementation and processing shall conform to the specifications outlined in Clause 8.

d) The key management shall conform to the specifications outlined in Clause 9. This shall be achieved in that the key initialization conforms to the specifications in 9.2.1.

5 Design considerations of internal security services for home networks

5.1 General

With more and more home appliances being connected to the home networks, residential users are increasingly concerned about the safety of their possessions. In this way, security considerations have become one of the most challenging research issues that need to be addressed to fulfil users' needs. Among these issues, defence against outside threats has been quite successful using existing solutions such as IPSec or SSL/TLS (see Bibliography for SSL/TLS specifications), but defence against inside threats still remains uncertain due to several changing criteria. This standard specifies the internal security services for home electronic systems and for home networks.

The internal network of a home needs to be protected. However, not all equipment that is controlled in a home needs the same kind of protection. At least three levels of protection can be foreseen. Some equipment can support the full IP stack with various security protocols while other pieces of equipment are insensitive and thus may not need to be secured at all. And, in between these two categories, there are pieces of equipment that should be protected but do not have the capacity to support the full set of Internet Protocols. The purpose of this standard is to provide security for such middleware equipment that does not have the IP capacity. SCPM provides various security services at the network layer and is intended to be media-independent, thus protecting communications from internal home network intruders.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 24767-2:2009
https://standards.iteh.ai/catalog/standards/sist/00baf152-7474-4ff9-9855-519936d306f4/iso-iec-24767-2-2009

In order to deal with the protection measures over the Internet, existing solutions such as IPSec or SSL/TLS can be tailored for home appliances. A combination of SCPM and existing solutions, correctly configured, combined with firewall technology, will meet the criteria of low cost, low complexity and moderate inconvenience while doing a good job on defending the home against threats.

Figure 1 gives an example of combined safeguard technologies. A maintenance centre tries to upgrade software in white goods, for example, a washing machine. However, a washing machine without IPSec or SSL capability could not provide end-to-end security with a server in the maintenance centre. The demarcation line could be set between two segments, from the server of the maintenance centre to a controller (with IP capability) at home and the controller to the washing machine. IPSec or SSL/TLS is used to protect the segment (from the server of the maintenance centre to a controller) and SCPM is used to protect the other segment (from the controller to the washing machine). The controller is responsible for decrypting the transmitted codes from the server protected by IPSec or SSL/TLS and encrypting the messages again by SCPM. The washing machine with SCPM protocol is able to decrypt the data and finally retrieve the transmitted code from the server. Because the home network is protected by a firewall, a malicious user cannot easily intrude on the network and retrieve the transmitted code while the controller is busy in decrypting or encrypting the transmitted codes.

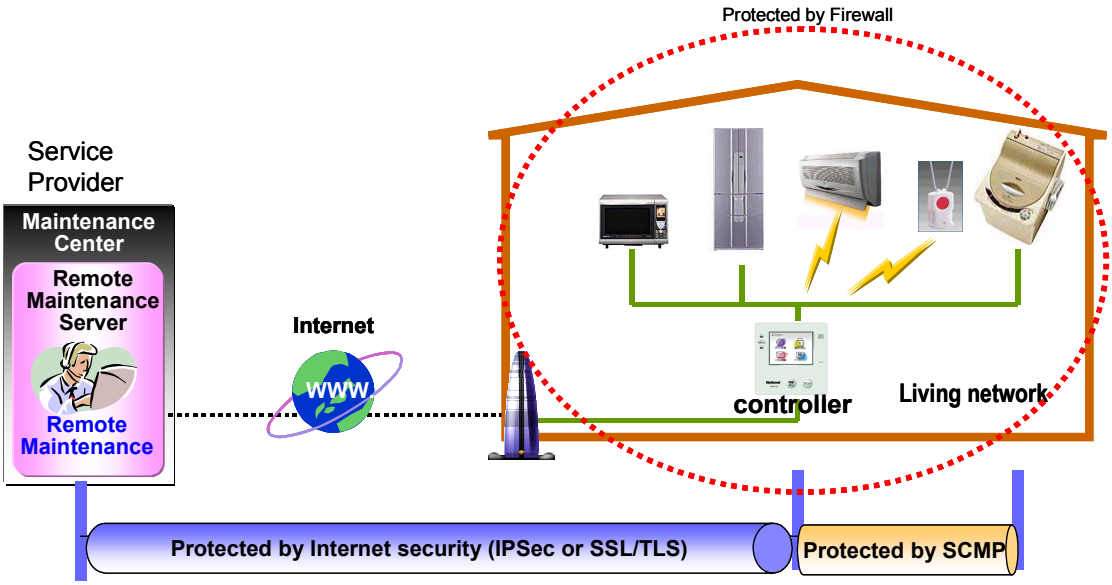

Figure 1 – Use of combined technologies against security risks

This standard provides a solution for sub-parts which contain non-IP devices within HES. IPsec and TLS provide a solution for IP based devices within HES.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

5.2 Issues addressed by security measures

5.2.1 General

ISO/IEC 24767-2:2009
https://standards.iteh.ai/catalog/standards/sist/00baf152-7d71-4f80-9855-519036430fa4/iso-iec-24767-2-2009

In home networks, there are many security risks. The goal of security services is to defend against malevolent/threat agents that seek to compromise the home information security. Aiming at the networking communications inside home, the following factors stimulate the discussion of in-home security requirements.

5.2.2 Unsafe transmission

Power line: Most houses have power-line installations, and houses in the same neighbourhood usually share a “power-line subnet” which connects to the same distribution transformer. Thus, power-line commands from one house can potentially reach devices in another near-by house and interfere with the controlling of those devices. This factor also makes interception possible.

Wireless link: Wireless networking is perhaps the most attractive approach to set up a network in the home since it avoids the cost and arduousness of wiring. However, it comes with a security drawback. Malicious users no longer need to gain physical access to the network medium, instead they can simply intercept another user’s transmissions within the working range of a sending node.

The nature of unsafe transmission media makes home networks vulnerable to various forms of attacks such as passive eavesdropping, active interfering, leakage of secret information, data tampering, impersonation and denial of service.

5.2.3 Intentional misuse

Although the security services of this standard focus on the inside of a home, when unsafe transmission media are used, the domain under consideration is no longer restricted to the inside of the home. The security services shall also protect against outsiders getting access to information transmitted within the home and against the ability to influence or manipulate such pieces of information.

In order to deal with these most demanding requirements for the security of home-networking communications, the main emphasis lies in the following four areas:

- Confidentiality – information should only be available to authorized persons. This function protects data from unauthorized disclosure.
- Data origin authentication and data integrity – data origin authentication is to allow the sources of data received to be verified as claimed. However, this function cannot provide protection against the duplication or modification of data. In this case, data integrity shall be used in conjunction with data origin authentication.
- Anti-replay – ensures message frame security by making it impossible for a hacker to intercept message frames and insert changed frames into the data stream between a source node and a destination node.
- Access control –provides the protection of system resources against unauthorized use.

5.3 Design principles of security measures

5.3.1 General

Taking into account the fact that the SCPM mechanism is going to be implemented in household appliances with limited resources, such as household appliances with 8-bit CPU, and that residential security shall be flexible, special consideration has been given to the following points, allowing the owner to trade off convenience, risk and cost.

5.3.2 Minimization of resources for cost-saving

iTeh STANDARD PREVIEW
(standards.iteh.ai)

The SCPM mechanism is expected to be implemented as lightly as possible when considering the limited hardware resources (CPU performance and memory capacity). These constraints make it difficult to implement fully and for many years the well-known security measures available in information technologies that are usually computation-intensive.

ISO/IEC 24767-2:2009
https://standards.iteh.ai/catalog/standards/sist/00bafc52-7474-4ff9-9855-51995bd50fe4/iso-iec-24767-2-2009

5.3.3 Independence of communication media

There are many types of transmission media used in homes to connect different devices to the network. The mechanisms specified in Clause 6 are independent of any transmission media. These mechanisms allow flexible use of services and at the same time keep them secure.

5.3.4 Independence of cryptographic algorithms

The SCPM mechanism is expected to permit the selection of different cryptographic algorithms without affecting other parts of its implementation and the incorporation of newly developed cryptographic methods into the implementation for future security improvements.

5.3.5 Extensibility of variant usages

While broadband connections are mostly used for Internet access today, they also create new service opportunities, such as maintenance of home appliances, monitoring of home security or metering-related services. To provide for future use in conjunction with variant services that will be applied in home networks, the SCPM mechanism is expected to be equipped with the capability to establish two or more service-specific shared keys for a household appliance, allowing two or more secure domains to be created within home networks.

6 Secure communication protocol for middleware (SCPM)

6.1 General

This clause provides a high-level description about how SCPM works in order to give an overall picture of its process and behaviour from a system's perspective and to see how it fits