Edition 1.0 2009-01

INTERNATIONAL STANDARD

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

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 It also gives information on projects, withdrawn and replaced publications.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

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

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*

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

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

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

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.

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.

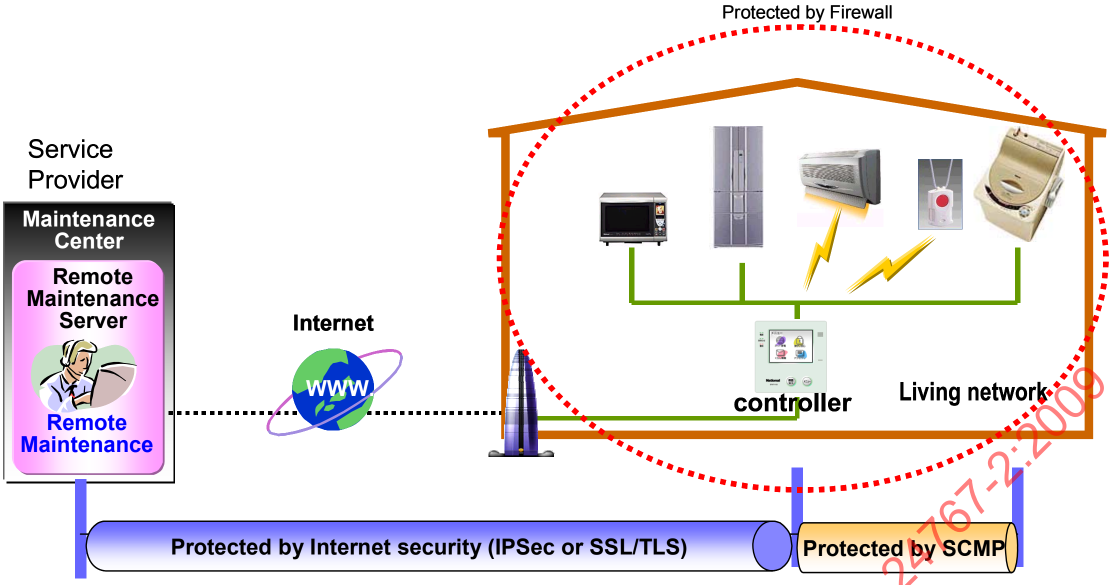


Figure 1 – Use of combined technologies against security risks

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.

5.2 Issues addressed by security measures

5.2.1 General

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

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.

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 into the communication between networked nodes. This clause also provides basic descriptions for the following clauses, which will describe each topic in more detail.

An SCPM implementation operating in a home appliance and an appliance controller offers protection for network traffic. The protection offered is based on requirements selected under various consideration and explained in 5.3.

6.2 What is SCPM

SCPM is designed to provide a mix of security services, comprising confidentiality, data origin authentication, data integrity and an anti-replay service (a form of partial sequence integrity). The set of services provided depends on whether the authentication/encryption mechanism is enabled or not.

Confidentiality may be selected independently of other services. However, the use of confidentiality without integrity/authentication may expose the communications to certain forms of active attacks that could undermine the confidentiality service.

Data origin authentication and data integrity are joint services (hereafter referred to as "authentication") and are offered as an option in conjunction with (optional) confidentiality. The anti-replay service may be selected only if data origin authentication is selected and its selection is solely at the discretion of the receiver. (Although the default calls for the sender to increment the sequence number used for anti-replay, the function is effective only if the receiver checks the sequence number.)

6.3 How does SCPM work

For the purpose of minimizing the message size, SCPM will not adopt the encapsulation mechanism used in a ISO network model. An ISO network model is shown in Figure 4. Instead, it utilizes the same message format, by inserting fields, such as security header, sequence number and data length between destination address (DA) and plain text data part byte counter (PBC) and encrypting/authenticating some fields. Figure 2 shows a comparison between a general message frame and a secure message frame. Exact field definitions will be described in Clause 7.

Figure 2 also shows that in home networking communications, messages carried in the frames can be roughly divided into two types: plaintext and ciphertext, depending on the corresponding indication in HD. Plaintext messages are directly carried in the payload, in the clear text, and secure messages are stored in the payload, either authenticated or encrypted. If the indication in HD shows that this is a secure frame, SCPM will be activated to interpret the encrypted/authenticated payload data. Otherwise, ordinary communications procedures are carried out as usual.

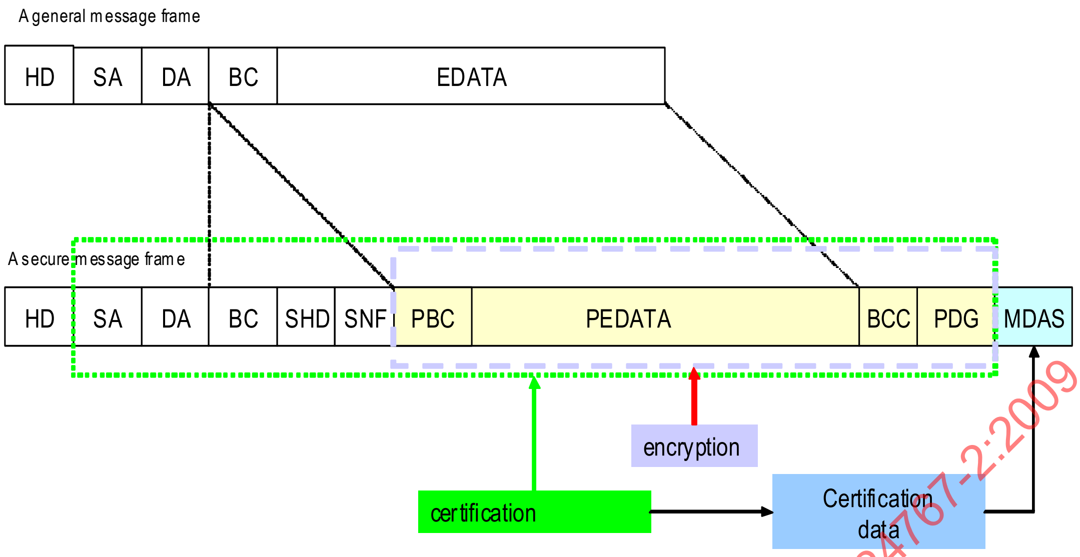


Figure 2 – General message frame versus secure message frame

Besides the specified message structure, SCPM also employs one round-trip communications mechanism to reduce the transmission data for media of lower and limited bandwidth (except for some cases where double confirmations are needed). A round-trip communication is a "request and response" protocol, where in a communication between two nodes, a service requester issues a request message and a requested service replies with a response message. The message flow is shown in Figure 3.

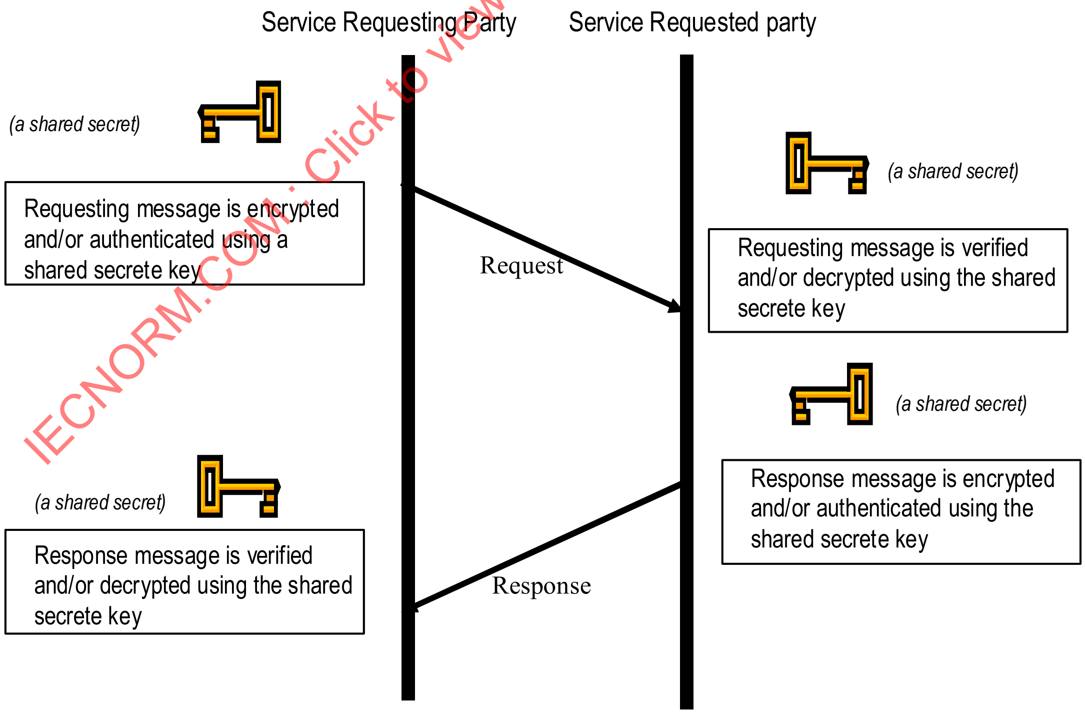

Service Requesting Party
Service Requested party
(a shared secret)
Requesting message is encrypted and/or authenticated using a shared secrete key
(a shared secret)
Requesting message is verified and/or decrypted using the shared secrete key
Request
(a shared secret)
Response message is encrypted and/or authenticated using the shared secrete key
(a shared secret)
Response message is verified and/or decrypted using the shared secrete key
Response

Figure 3 – Round trip communications of SCPM

6.4 Where is SCPM going to be implemented

The primary objective of SCPM is to have sufficient security mechanisms for a wide variety of applications with limited IT capability, and to provide secure communications at the network layer ISO/IEC 11577, as shown in Figure 4. SCPM is implemented in the layer of secure communication middleware and is equivalent to “Network Layer”, “Transport Layer” and “Session Layer” in Figure 4.

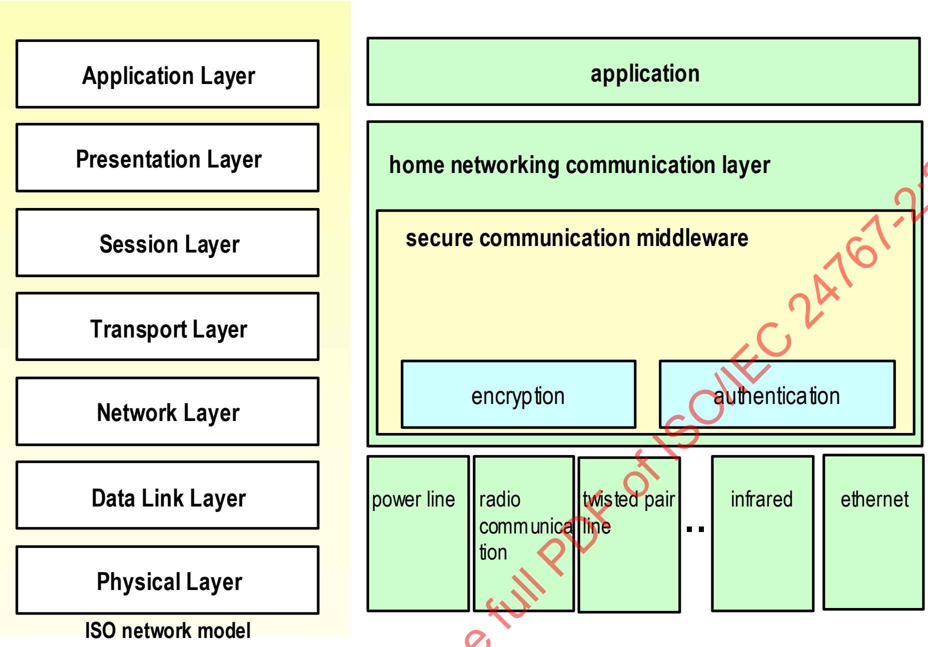


Figure 4 – Position of SCPM

Network-layer frames have no inherent security. It is relatively easy to forge the address, modify the contents, replay old frames and inspect the contents of frames in transit. Therefore, there is no guarantee that

a) the ackets received are from the claimed sender;

b) the packets contain the original data that the sender placed in them, and

c) that the original data has not been inspected by a third party while it travels.

Implementing security at the network layer has many advantages. Most of all, applications need few or no changes, for it can work seamlessly with any protocol transported above the network layer, which reduces the explosion in the implementations of other security protocols at higher layers.

Since it operates at the network layer, SCPM can be used to secure any protocol that can be encapsulated in a network packet, without any additional requirements.

6.5 Usage levels of SCPM

Applications relying on SCPM can be divided into four usage levels: supervisor, user, service provider and maker. Each usage can be illustrated as follows.

Supervisor level: A householder who supervises different access levels to devices falls under this level. For example, the procedures of initial setting of a user key are at “supervisor level”.

In supervisor level, confidentiality service and/or authentication is performed by “serial key” of the device. “Serial key” is set into the device in manufacture and displayed on the device’s outer case. A householder who supervises the access right to the device uses this “serial key” during the initial setting of the user key to the device.

User level: Inhabitants operating home-networking automation/manipulation belong to this level. “User key” is set into a device by the supervisor and one user key is set in one domain. When inhabitants don’t want to disclose home information to those other than their family members, communications message could be protected by “user key”.

Service provider level: When the householder is willing to transfer certain access right to a device to a service provider, communications between a control node and a device node is protected by the service provider key when security services are necessary, which prevents other unauthorized service providers from supervising the intended devices.

Maker level: When manufacturers perform operations and don’t want to be intercepted by malicious users, communications message can be protected by maker key. “Maker key” is supervised by the maker of the device.

6.6 Usage keys of SCPM

This standard defines the following five keys of SCPM.

Serial key: When confidentiality services and/or authentication are performed in supervisor level, “serial key” is used.

User key: When confidentiality services and/or authentication are performed in user level, “user key” is used.

Service provider key: When confidentiality services and/or authentication are performed in service provider level, “service provider key” is used.

Maker key: When confidentiality services and/or authentication are performed in maker level, “maker key” is used.

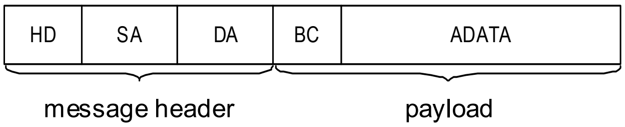
Master key: In this standard, “master key” is a generic name of shared secret key. When the common key is updated, the common key after update is called “new master key” and the common key before update is called “pre-master key”.

7 Secure message frame format

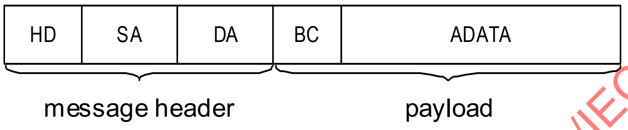
7.1 General communication frame

7.1.1 General

The overwhelming majority of packets that traverse the network today follow the rules and the formats defined by standards. A generic network frame, basically, includes message header and payload data. For instance, an IP datagram comprises IPv4/IPv6 header and payload. More specifically, the message header would comprise the frame header, the source address and the destination address. Payload data comprises the size of the following data and the communication information as described in Figure 5.



HD = Frame Header
SA = Source Address
DA = Destination Address
BC= Byte Counter of EDATA
ADATA= information carried in this message frame



HD = Frame Header
SA = Source Address
DA = Destination Address
BC= Byte Counter of EDATA
ADATA= information carried in this message frame

Figure 5 – General message frame

7.1.2 Header (HD)

The header contains type information that indicates whether the message frame is a secure frame or not. Besides, it may carry other possible information, for example the communication method. In networks, point to point communication is a typical model, but they also have several other types, for example broadcast communication and multicast communication.

7.1.3 Source address (SA) and destination address (DA)

SA represents the network address of the source that generated this message frame. DA represents the network address of the destination host. It could be IP address, MAC address or any form of addressing provided for specific communications.

7.1.4 Byte counter (BC)

The byte counter indicates the data size of the ADATA field in bytes.

7.1.5 Application Data (ADATA)

ADATA is a variable length field, which carries the service requesting information.

7.2 Secure frame structure

7.2.1 General

Payload data is further divided into seven fields: Secure header (SHD), sequence number field (SNF), plain text data part byte counter (PBC), payload data (PADATA), block check code (BCC), padding (PDG) and message data authentication signature (MDAS). The following subclauses define each field in the secure frame. Some fields could be “optional” (marked by * in Figure 6) which means that the field is omitted if the option is not selected. Whether or not an option is selected, is defined in secure header (SHD). The structure is shown in Figure 6.

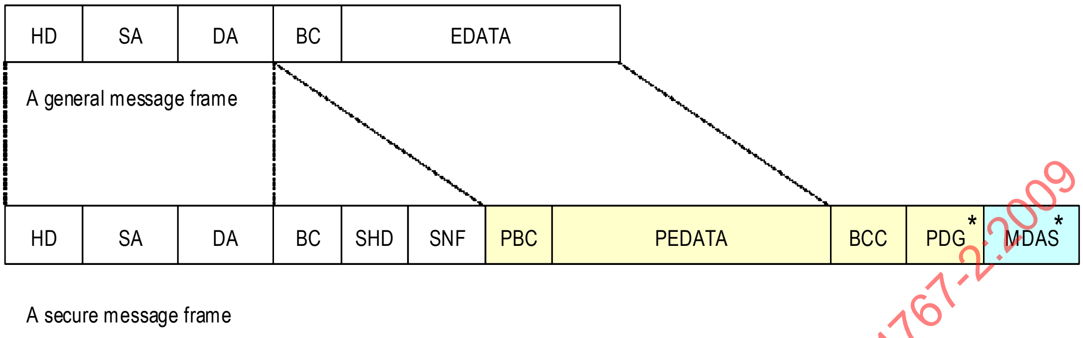


Figure 6 – Secure message frame

7.2.2 Secure header (SHD)

SHD is a 2-byte field. Figure 7 shows the data format in SHD.

b3:b2:b1:b0	**Key Index** b3:b2:b1:b0=0:0:0:0 Serial Key Index b3:b2:b1:b0=0:0:0:1 User Key Index b3:b2:b1:b0=0:0:1:0 Maker Key Index Others: 0:0:1:1 to 1:1:1:1 Service Provider Key Index
b4	1: used to indicate the message is encrypted and authenticated by a shared secret key computed by DH algorithm 0: b3:b2:b1:b0 key index is used
b5	For future reserved
b6	**Authenticate service indication** (Could not be b7:b6=1:1) 0 : Certification enabled 1 : Certification disabled
b7	**Encryption service indication**(Could not be b7:b6=1:1) 0 : Encryption enabled 1 : Encryption disabled
b8	**Message type** 0 : Request 1 : Response
b9~b11	For future reserved
b15:b14:b13:b12	**Secure services response** b15:b14:b13:b12 = 0:0:0:0: successful, b15:b14:b13:b12 = 0:0:0:1: verification of SNF fail b15:b14:b13:b12 = 0:0:1:0: verification of certification fail b15:b14:b13:b12 = 0:1:0:0 decrypts data fail

Figure 7 – Data format of a secure header (SHD)

Bit 0 to bit 3 are used to indicate the key index for various usages (supervisor, user, service provider and maker). Since there might be a couple of services for home appliances, the index of service provider key would range from (b3:b2:b1:b0) = 0:0:1:1 to 1:1:1:1.

In order to provide a master key update using ISO/IEC 11770-3 (DH algorithm), bit 4 is used to indicate this type of service. When value in bit 4 is set to 1, it means this secure message frame is protected by a shared secret value computed by ISO/IEC 11770-3 (DH algorithm).

Bit 6 and bit 7 are used to indicate the provided security service. When the value in bit 6 is set to 0, it means authentication service is enabled in this communication. When the value in bit 7 is set to 0, it means confidentiality service is enabled. Note that, bit 6 and bit 7 shall not be 1 simultaneously, because when the header in the message frame indicates this communication is secured, but neither authentication nor confidentiality service is specified, it would conflict with the indication in the HD field.

Since SCPM is a “request-response” protocol, bit 8 indicates the message property, value 0 indicates it’s a “request” message from a requesting party and value 1 indicates it’s a “response” message from a requested party.

Bit 12 to bit 15 are used to indicate the processing result of the request message and it is effective in a response message. Bit 12 indicates the correction of SNF verification, bit 13 indicates the correction of authentication verification and bit 14 indicates the correction of access right.

7.2.3 Sequence number field (SNF)

This is a 4-byte field which contains a monotonically increasing counter value (sequence number). It is mandatory and is always present even if the secure communication does not enable the anti-replay service for this message frame. Processing of SNF is the responsibility of the requested service. The initial value of SNF can be determined in two ways, randomly chosen (for a node cold or warm start) or reading and using the sequence number stored in non-volatile memory (for warm start only). The requested service increments the sequence number by 1 and transmits it to the service requester when authentication is successful.

The service requester uses the value of SNF in the next request message to the same requested service.

7.2.4 Plain text data part byte counter (PBC)

PBC is a 1-byte field indicating the number of bytes of plain text data (PADATA).

7.2.5 Plain text application data (PADATA)

PADATA is a variable-length field. The field is mandatory and is an integral number of bytes in length. The maximum length of PADATA is 255 bytes.

7.2.6 Block check code (BCC)

The purpose of employing block check code (BCC) mechanism is to detect errors. BCC is a 1-byte field, which stores a summation value generated by performing XOR operations on each field’s horizontal parity. Fields checked by BCC include: SA, DA, BC, SHD, SNF, PBC and PADATA. This check code is not a cryptographic check value.

7.2.7 Padding (PDG)

When an encryption algorithm is employed that requires the plaintext to be exact multiples of some number of bytes, for example the block size of a block cipher, PDG field is used to fill the plaintext (consisting of PBC, PADATA and BCC) to the size required by the algorithm. The service requester may add a couple of bytes padding. For Advanced Encryption Standard (AES), specified in ISO/IEC 18033-3, the service requester may add (0 to 15) bytes of padding. Inclusion of the PDG field is optional, but all implementations shall support generation and consumption of padding. If PDG bytes are needed but the encryption algorithm does not specify the padding contents, then the following default processing shall be used. The PDG field is filled with 0x00 value.

7.2.8 Message data authentication signature (MDAS)

MDAS is a variable-length field, whose length is specified by the authentication function selected. For example, if AES CBC-MAC with 128-bit key is employed (see ISO/IEC 10116), MDAS is a 16-byte data. MDAS is a value computed over SCPM message frame minus header (HD) and data authentication data (MDAS). MDAS field is optional and is included only if the authentication service has been selected and specified in SHD field.

8 SCPM processing

8.1 Algorithms and processing

8.1.1 General

Although both confidentiality and authentication are optional, at least one of these services shall be selected and hence both encryption and authentication algorithms shall not be simultaneously disabled.

8.1.2 Encryption algorithms and encryption calculation

The encryption algorithm employed is specified with key distribution. SCPM is designed for use with symmetric encryption algorithms. The mandatory SCPM encryption algorithm is the AES, specified in ISO/IEC 18033-3. Encrypted fields include PBC, PADATA, BCC and PDG. Figure 8 shows an example where the employed encryption algorithm is AES-CBC, 128-bit key length.

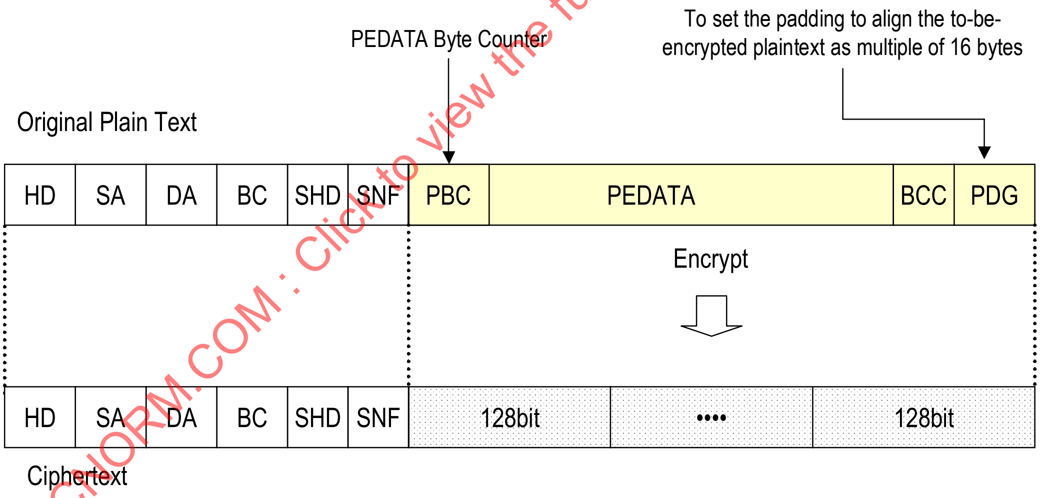


Figure 8 – Encryption employing AES-CBC with 128-bit key

8.1.3 Data authentication algorithms and data authentication calculation

Like for encryption algorithms mentioned above, data authentication algorithms employed for authentication data computation shall be specified with key distribution, which takes a message of any size and generates a fixed-length output. The mandatory SCPM data authentication algorithm is AES. It works the same way as the encryption algorithm and utilizes CBC-MAC to make a message authentication signature from a block cipher. Authentication data comes from the fields in the message frame and there are two cases to obtain the needed value: 1) Authentication only and 2). Authentication after encryption. Figure 9 shows how authentication data is computed. In case of authentication only, authentication data is computed from SA to BCC and put in the MDAS field. In case of authentication and encryption services enabled, encryption processing is performed first (from PBC to PDG), authentication is computed from SA to the encrypted data and put in the field of MDAS. The MDAS field is the last N bytes of the whole secure frame, where N is authentication algorithm-specific.

For some authentication algorithms, the byte string over which the authentication data value is computed shall be a multiple of the block size specified by the algorithms. If the length of this byte string does not match the block-size requirements of the algorithm, implicit padding shall be appended to the end of the authenticated message frame (after BCC when the service is authentication only, or after the encrypted data when the services are authentication and confidentiality) prior to the MDAS field. These padding bytes shall have a value of zero and the block size is specified by the algorithm specification. The padding is not transmitted with the message frame.

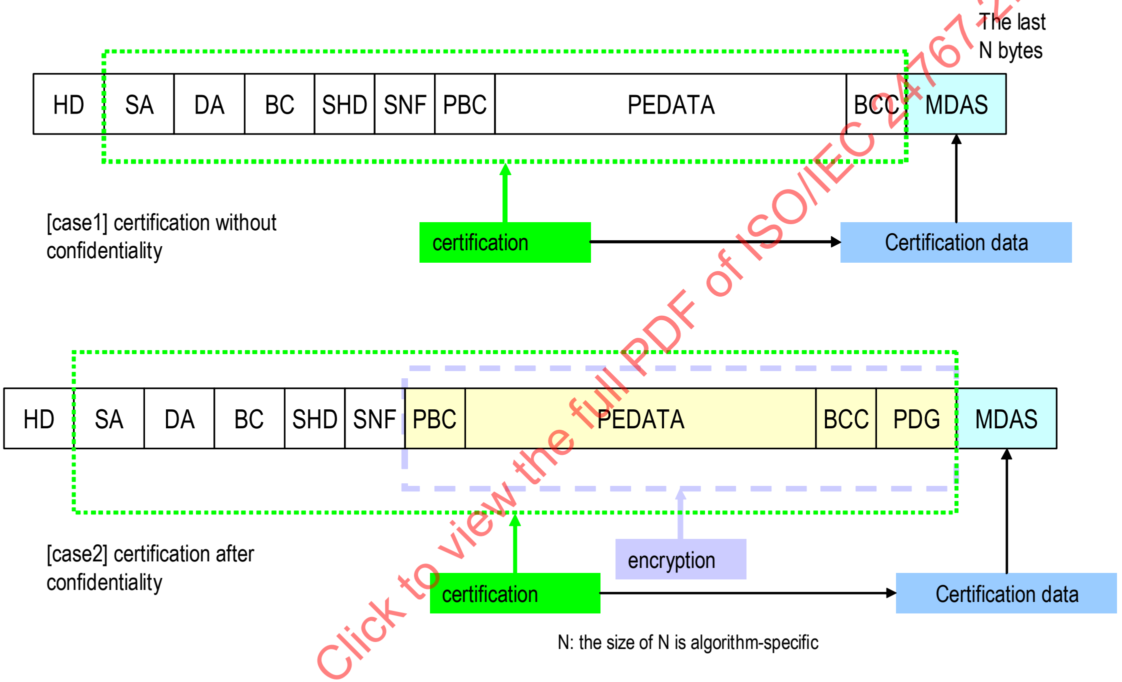


Figure 9 – Data authentication calculation

8.1.4 Cipher block chaining (CBC) mode

All encryption algorithms used in SCPM shall operate in cipher block chaining (CBC) mode (see ISO/IEC 10116). CBC requires that the amount of data to be encrypted be a multiple of the block size of the cipher. The requirement is met by adding padding to the end of data when necessary before encryption. The padding becomes part of the cipher text of the message frame and is stripped off by the requested service during inbound message processing. If data is already a multiple of the block size of the cipher, padding needs not to be added.

Ciphers in CBC mode also require an initialisation vector (IV) to avoid generating a new key for each encryption session. This IV is generated from SNF value and is described in 8.1.6.

8.1.5 SNF initialisation and verification

A service requester keeps the SNF value associated with a requested service in a previously successful response. A requested service controls/manages the SNF for each service requester. But for the first request, or the SNF value is lost for some reasons, for example, power off, the service requester doesn’t keep any sequence number, then SNF initialisation shall be performed with authentication service.

The requesting message comprises an arbitrary SNF and is sent to the opposite site as shown in Figure 10. When SNF fails to be verified, the requested service responds with a generated/maintained SNF value to indicate a “SNF verification failure”. The service requester gets the SNF value and sends an authentication message with the obtained SNF value. The requested service verifies the message and then sends successful authentication response to the service requester with the new SNF value (increased by 1).

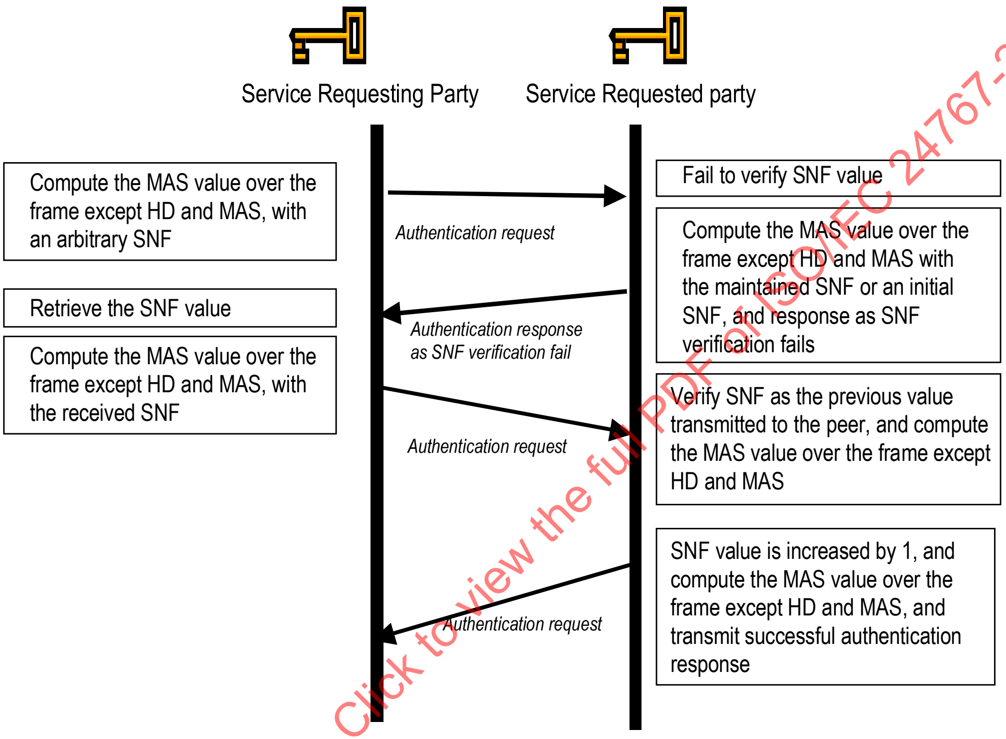

Service Requesting Party
Service Requested party
Compute the MAS value over the frame except HD and MAS, with an arbitrary SNF
Retrieve the SNF value
Compute the MAS value over the frame except HD and MAS, with the received SNF
Authentication request
Authentication response as SNF verification fail
Authentication request
Authentication request
Fail to verify SNF value
Compute the MAS value over the frame except HD and MAS with the maintained SNF or an initial SNF, and response as SNF verification fails
Verify SNF as the previous value transmitted to the peer, and compute the MAS value over the frame except HD and MAS
SNF value is increased by 1, and compute the MAS value over the frame except HD and MAS, and transmit successful authentication response

Figure 10 – Sequences of SNF initialisation

8.1.6 Initialisation vector (IV) value

Employing CBC requires an explicit initialisation vector (IV) of N bytes and N is algorithm-dependent. For example, 16-byte IV is used in AES-CBC, key length 128 bits. This IV immediately precedes the protected (encrypted) payload. Including the IV in each message frame ensures that decryption of each received message frame can be performed, even when some message frames are dropped in transit. The value of IV is derived from SNF. For instance, a 16-byte IV is used for AES-CBC. Figure 11 shows the setting of IV in the case of a 16-byte IV.

IV :	SNF	SNF	SNF	SNF

Figure 11 – Calculation of IV value

8.2 Secure message frame processing

8.2.1 General

Processing of a secure message frame depends on which services are being enabled.

The following subclauses illustrate how message frames are processed in the three combinations:

a) data authentication enabled only,

b) confidentiality enabled only, and

c) both data authentication and confidentiality are enabled.

Secure message exchange between the service requester and a requested service is peer-to-peer and if the specified destination network address is a broadcast address, the requested service shall abandon the message.

8.2.2 Message frame processing of data authentication only

Figure 12 shows the data authentication sequence between a service requester and a requested service.

The steps (numbers indicate the sequence) of data authentication message generation from service requester are depicted as follows.

a) Set indication values in SHD
   1) b0:b1:b2:b3 is used to indicate the key index used in this communication.
   2) b6:b7 = 0:1 is used to indicate the security service as: data authentication enable and confidentiality disabled.
   3) b8 = 0 is used to indicate the message is a “request” message.

b) Set sequence number
   1) If a sequence number from the previous communication is kept, it uses this sequence number.
   2) Otherwise (for the first communication, or if no sequence number is kept), an arbitrary sequence number randomly chosen is used as described in 7.2.3.

c) Compute BCC.

d) Compute MDAS over the whole message frame except HD and MDAS.

The steps of verifications of authentication message by the requested service are depicted as follows.

Step 1 Verify sequence number.

Step 2 Verify BCC.

Step 3 Verify the authentication data.

The response message is prepared as follows in order to transmit it to the service requester. The steps (numbers indicate the sequence) of response message generation from service requested party are depicted as follows.

e) Set indication values in SHD
   1) b0:b1:b2:b3 is used to indicate the key index used in this communication, which is the same as its corresponding request message.

2) b6:b7 = 0:1 is used to indicate the security service as: data authentication enable and confidentiality disabled, which is the same as its corresponding request message.

3) b8 = 1 is used to indicate the message is a “response” message.

4) record the response result in b12:b13:b14:b15 to indicate the verification is successful or not. If successful, set b12:b13:b14:b15 = 0:0:0:0.

f) Set sequence number

1) In the case of a successful response, put the next sequence number (increased by 1

2) In the case of a failed response

i) If a sequence number corresponding to this service requester does not exist, the requested service has to put the initial sequence number in a SNF field in response to the service requester.

ii) Otherwise, the previous sent sequence number is used.

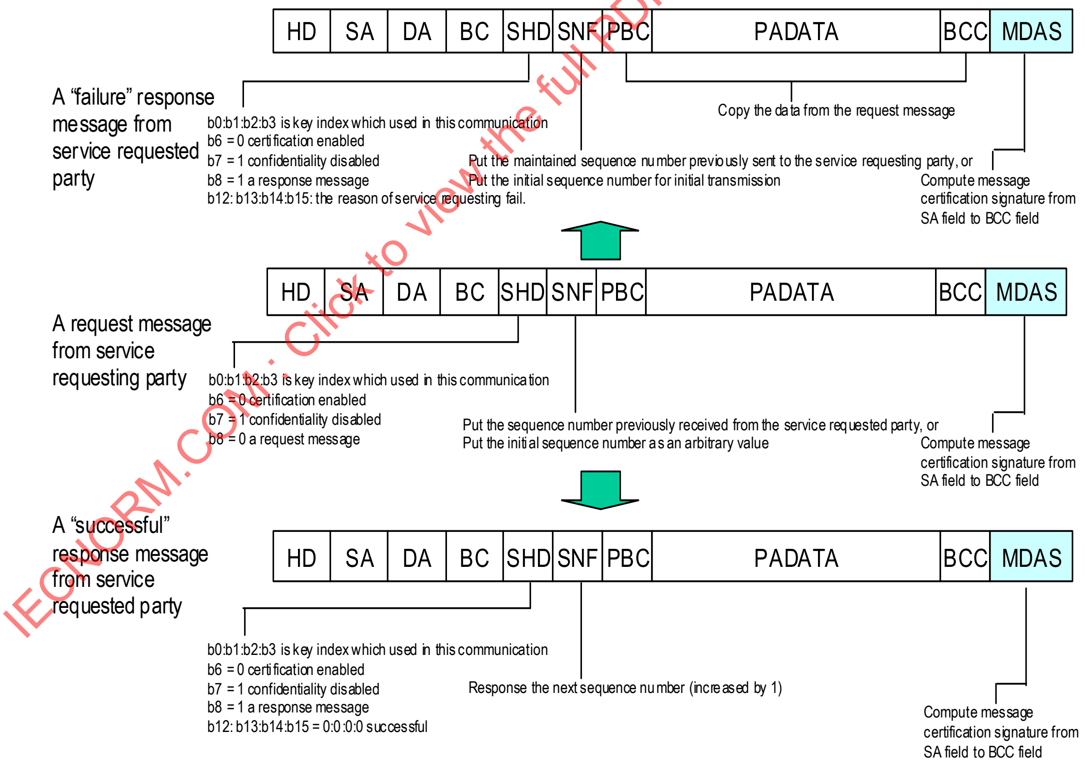
g) Set payload data

1) For failed data authentication, copy data from request and put them into PBC, PADATA and BCC from the corresponding fields of request message.

2) For successful data authentication, put response data and corresponding length into PADATA and PBC and calculate BCC.

h) Compute MDAS over the whole message frame except HD and MDAS.

Figure 12 shows an example of message frames employing an authentication service.



HD SA DA BC SHD SNF PBC PADATA BCC MDAS
A “failure” response message from service requested party
b0:b1:b2:b3 is key index which used in this communication
b6 = 0 certification enabled
b7 = 1 confidentiality disabled
b8 = 1 a response message
b12: b13:b14:b15: the reason of service requesting fail.
Put the maintained sequence number previously sent to the service requesting party, or
Put the initial sequence number for initial transmission
Copy the data from the request message
Compute message certification signature from SA field to BCC field
HD SA DA BC SHD SNF PBC PADATA BCC MDAS
A request message from service requesting party
b0:b1:b2:b3 is key index which used in this communication
b6 = 0 certification enabled
b7 = 1 confidentiality disabled
b8 = 0 a request message
Put the sequence number previously received from the service requested party, or
Put the initial sequence number as an arbitrary value
Compute message certification signature from SA field to BCC field
A “successful” response message from service requested party
HD SA DA BC SHD SNF PBC PADATA BCC MDAS
b0:b1:b2:b3 is key index which used in this communication
b6 = 0 certification enabled
b7 = 1 confidentiality disabled
b8 = 1 a response message
b12: b13:b14:b15 = 0:0:0:0 successful
Response the next sequence number (increased by 1)
Compute message certification signature from SA field to BCC field

Figure 12 – Secure message frames employing authentication service

8.2.3 Message frame processing of confidentiality only

Figure 13 shows the encryption sequence between service requester and requested service.

The steps of encryption message generation from service requester are depicted as follows (numbers indicate the sequence).

a) Set indication values in SHD

   1) b0:b1:b2:b3 is used to indicate the key index used in this communication.

   2) b6:b7 = 1:0 is used to indicate the security service as: data authentication disable and confidentiality enabled.

   3) b8 = 0 is used to indicate the message is a “request” message.

b) Set an arbitrary number in SNF field

c) Compute BCC

d) Encryption

   1) Add necessary padding data.

   2) If the employed algorithm is CBC mode, IV data acting as input to the encryption algorithm is calculated from the value of SNF field.

   3) Encrypt the result (PBC, PADATA, BCC and PDG).

The steps of verifications of encryption message by the requested service are depicted as follows (numbers indicate the sequence).

Step 1 Decrypt data.

Step 2 Verify BCC.

The response message is prepared as follows in order to transmit it to the service requester.

a) Set indication values in SHD

   1) b0:b1:b2:b3 is used to indicate the key index used in this communication, which is the same as its corresponding request message.

   2) b6:b7 = 1:0 is used to indicate the security service as: data authentication disabled and confidentiality enabled, which is the same as its corresponding request message.

   3) b8 = 1 is used to indicate the message is a “response” message.

   4) record the response result in b12:b13:b14:b15 to indicate the verification is successful or not. If successful, set b12:b13:b14:b15 = 0:0:0:0.

b) Set an arbitrary value in SNF field.

c) Set payload data

   1) For failed verification, copy encrypted data from the request message.

   2) For successful verification, put response data into PADATA and corresponding data length into PBC and compute BCC, then encrypts PBC, PADATA, BCC and padding data.

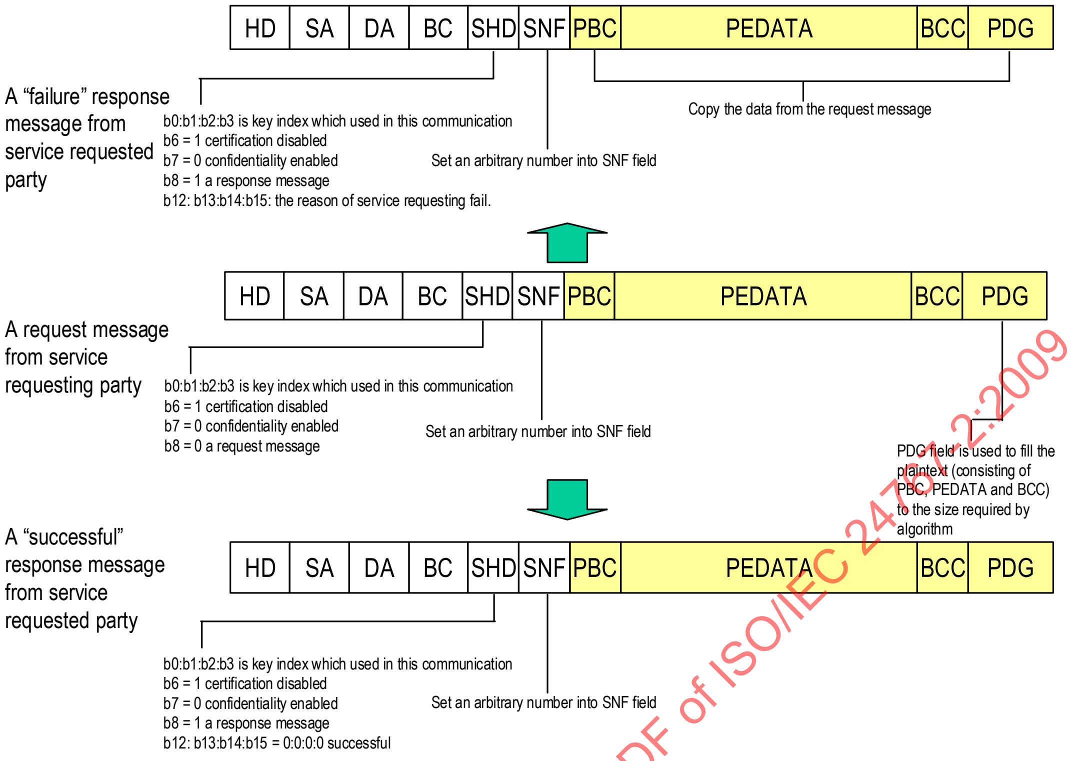

HD SA DA BC SHD SNF PBC PEDATA BCC PDG
A "failure" response message from service requested party
b0:b1:b2:b3 is key index which used in this communication
b6 = 1 certification disabled
b7 = 0 confidentiality enabled
b8 = 1 a response message
b12: b13:b14:b15: the reason of service requesting fail.
Set an arbitrary number into SNF field
Copy the data from the request message
HD SA DA BC SHD SNF PBC PEDATA BCC PDG
A request message from service requesting party
b0:b1:b2:b3 is key index which used in this communication
b6 = 1 certification disabled
b7 = 0 confidentiality enabled
b8 = 0 a request message
Set an arbitrary number into SNF field
PDG field is used to fill the plaintext (consisting of PBC, PEDATA and BCC) to the size required by algorithm
A "successful" response message from service requested party
HD SA DA BC SHD SNF PBC PEDATA BCC PDG
b0:b1:b2:b3 is key index which used in this communication
b6 = 1 certification disabled
b7 = 0 confidentiality enabled
b8 = 1 a response message
b12: b13:b14:b15 = 0:0:0:0 successful
Set an arbitrary number into SNF field

Figure 13 – Secure message frames employing encryption service

8.2.4 Message frame processing of data authentication and confidentiality

When both data authentication and confidentiality services are enabled, one fact to be aware of is, that the cipher text is data authenticated and the data authenticated plaintext is not encrypted. This means that, for outbound message frames encryption happens first and for inbound message frames data authentication happens first.

Figure 14 shows the processes both on service requester and requested service.

The steps of data authenticated and encrypted message generation from service requester are depicted as follows. The following order of processing facilitates rapid detection and rejection of replayed packets by the receiver, prior to decrypting the packet, hence potentially reducing the impact of DoS attack.

a) Set indication values in SHD
   1) b0:b1:b2:b3 is used to indicate the key index used in this communication.
   2) b6:b7 = 0:0 is used to indicate the security service as: data authentication and confidentiality enabled.
   3) b8 = 0 is used to indicate the message is a "request" message.
b) Set sequence number
c) Compute BCC.
d) Encryption
   1) Add a necessary padding data.
   2) If the employed algorithm is CBC mode, IV data acting as input to the encryption algorithm is calculated from SNF value.
   3) Encrypt the result (PBC, PADATA, BCC and PDG).

e) Authentication data calculation

1) Calculate the authentication value from SA to the encrypted data (comprises PBC, PADATA, BCC and PDG)

2) Save the calculation result in MDAS field.

The verification steps of an encrypted and authenticated message are described as follows.

Step 1 SNF value verification

Step 2 MDAS value verification

Step 3 Data decryption

Step 4 BCC value verification

The response message is prepared as follows in order to transmit it to the service requester. The steps (numbers indicate the sequence) of response message generation from service requested party are depicted as follows.

f) Set indication values in SHD

1) b0:b1:b2:b3 is used to indicate the key index used in this communication, which is the same as its corresponding request message.

2) b6:b7 = 0:0 is used to indicate the security service as: data authentication and confidentiality enabled, which is the same as its corresponding request message

3) b8 = 1 is used to indicate the message is a "response" message

4) recording the response result in b12:b13:b14:b15 to indicate the verification is successful or not. If successful, set b12:b13:b14:b15 = 0:0:0:0.

g) Set sequence number

1) In case of a successful response, put the next sequence number (increased by 1).

2) In case of a failed response,

i) If a sequence number corresponding to this service requester does not exist, the requested service has to put the initial sequence number in SNF field in response to the service requester.

ii) Otherwise, the previous sent sequence number is used.

h) Set payload data

1) For failed verification, copy encrypted data of PBC, PADATA, BCC and PDG from the request message.

2) For successful verification, put response data into PADATA and corresponding data length into PBC and compute BCC, then encrypts PBC, PADATA, BCC and padding data.

i) Compute MDAS over the whole message frame except HD and MDAS.

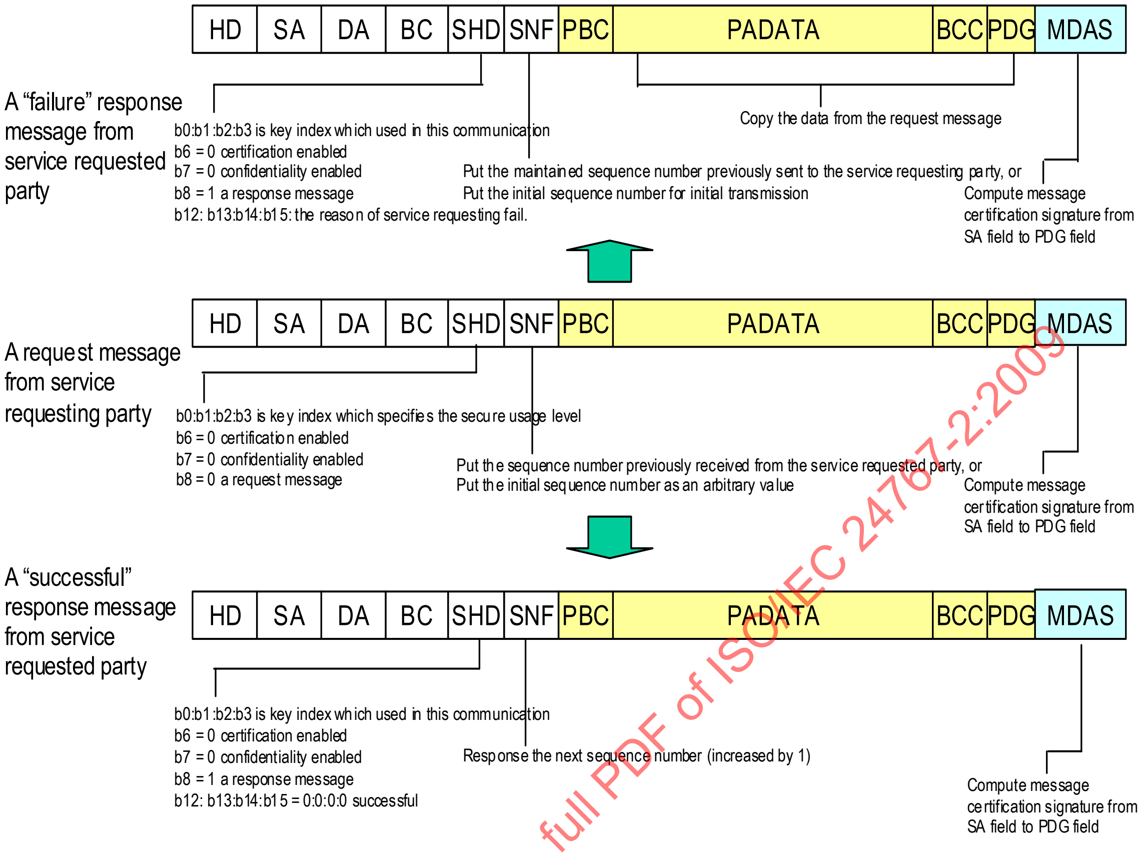

HD
SA
DA
BC
SHD
SNF
PBC
PADATA
BCC
PDG
MDAS
A "failure" response message from service requested party
b0:b1:b2:b3 is key index which used in this communication
b6 = 0 certification enabled
b7 = 0 confidentiality enabled
b8 = 1 a response message
b12: b13:b14:b15: the reason of service requesting fail.
Copy the data from the request message
Put the maintained sequence number previously sent to the service requesting party, or
Put the initial sequence number for initial transmission
Compute message certification signature from SA field to PDG field
A request message from service requesting party
b0:b1:b2:b3 is key index which specifies the secure usage level
b6 = 0 certification enabled
b7 = 0 confidentiality enabled
b8 = 0 a request message
Put the sequence number previously received from the service requested party, or
Put the initial sequence number as an arbitrary value
Compute message certification signature from SA field to PDG field
A "successful" response message from service requested party
b0:b1:b2:b3 is key index which used in this communication
b6 = 0 certification enabled
b7 = 0 confidentiality enabled
b8 = 1 a response message
b12: b13:b14:b15 = 0:0:0:0 successful
Response the next sequence number (increased by 1)
Compute message certification signature from SA field to PDG field

Figure 14 – Secure message frames employing encryption and data authentication services

9 Key management

9.1 General

One of the advantages of SCPM is that the mechanism of key management is also achieved by the same protocol, that is, keys used in SCPM are also distributed by SCPM.

Various keys for secure communications are initially set and operated differently depending on the key types. Key generation/distribution is controlled and managed by a "key setting node" (KSN). Home devices are responsible for keeping those distributed keys, which serve as the shared secrets between service requesters and requested service. This SCPM assumes that only one KSN is present in one domain and only one KSN distributes the key to home devices. Also, KSN manages the key between KSN and home devices. When KSN sends various keys to home devices, the keys shall be encrypted.

KSN plays an important role to deliver, update and store all keys. KSN shall be a very trusted device. A typical operation of how to authorize a KSN is described in Annex A.

9.2 Key initialisation

9.2.1 Initialisation of a user key

A "user key" is the shared secret between all devices within a domain. "Secure communications" is obtained through the practice of a "user key" when inhabitants operate home-networking automation/manipulation. When a device wishes to join the network (as a newly registered device), a "user key" initialisation is required on this device, which is accomplished by KSN's delivery of the protected "user key" to the newly registered device. Before this initialisation, a pre-shared secret shall be exchanged between both nodes by some out-of-band mechanisms. The processes are shown in Figure 15 and the steps are described as follows.

a) KSN authenticates a supervisor by proprietary mechanisms, for example using PIN.

b) Use "serial key" of the newly registered device (which is produced by its appliance maker) as a "pre-shared secret" and take the secret to KSN by some "out-of-band" mechanisms, for example the serial key of the newly registered device is inputted to KSN.

c) The preparation for the "user key" initialisation is done on the newly registered device.

   1) As this is the first communication between KSN and the newly registered device, there is no commonly agreed-upon (trusted) sequence number between the two, so the device has to randomly generate the initial value of the sequence number and delivers it to KSN, as described in 7.2.3.

   2) If the device is equipped with an "initial setting mode", it has to be switched to this mode.

d) KSN issues a request in plaintext to the newly registered device to inquire the encryption/authentication algorithm supported with the "serial key".

e) The newly registered device responds with its supported encryption/authentication algorithm to the KSN in plaintext.

f) KSN generates/retrieves the "user key", stores it with associated attributes (key length and algorithm) in PADATA, then encrypts/authenticates the "user key Initialisation request" message frame using the pre-shared "serial key" and pre-negotiated algorithm (noted above in items 4 and 5) and then transmits the secure message frame to the newly registered device.

g) The newly registered device receives and verifies the "user key Initialisation command" by the "serial key" and pre-negotiated algorithm (noted above in items 4 and 5).

h) If the verifications are successful, the newly registered device prepares the "user key Initialisation response" by increasing the sequence number by 1, copying encrypted data and authenticating the message by its "serial key" and then by transmitting it to KSN. As a result, KSN knows whether the newly registered device received the user key properly.

i) KSN receives and verifies the "user key Initialisation response", retrieves the new sequence number and confirms that the exchange is successful.

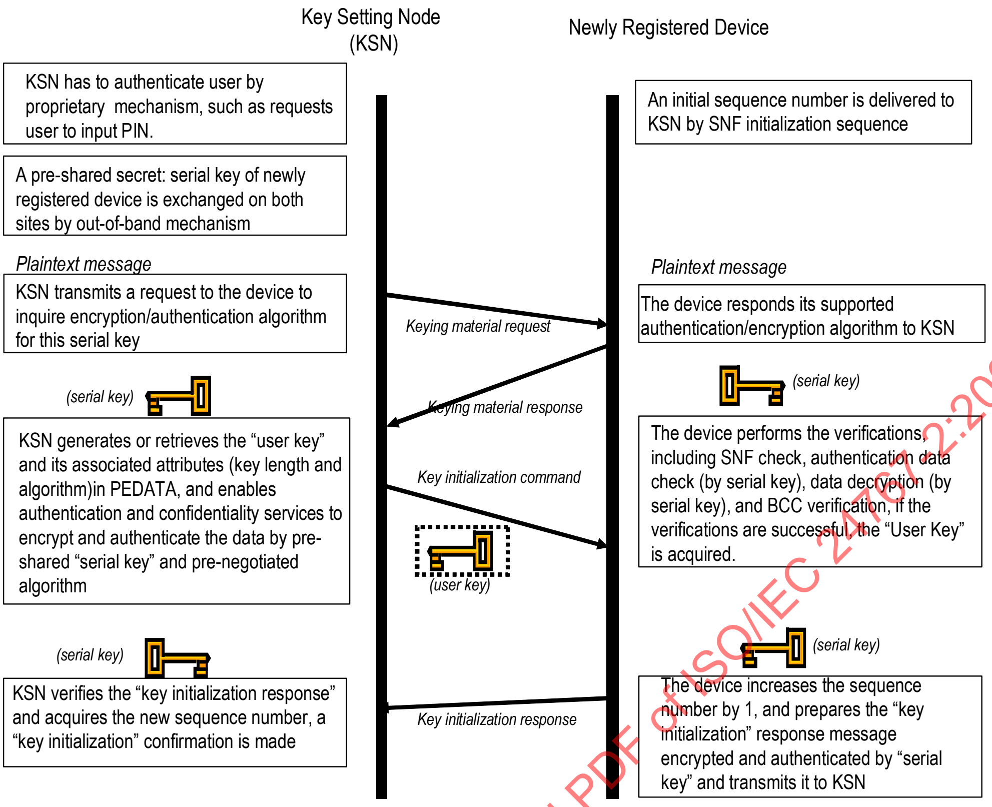

Key Setting Node
(KSN)
Newly Registered Device
KSN has to authenticate user by proprietary mechanism, such as requests user to input PIN.
An initial sequence number is delivered to KSN by SNF initialization sequence
A pre-shared secret: serial key of newly registered device is exchanged on both sites by out-of-band mechanism
Plaintext message
KSN transmits a request to the device to inquire encryption/authentication algorithm for this serial key
Plaintext message
The device responds its supported authentication/encryption algorithm to KSN
Keying material request
Keying material response
(serial key)
(serial key)
KSN generates or retrieves the “user key” and its associated attributes (key length and algorithm)in PEDATA, and enables authentication and confidentiality services to encrypt and authenticate the data by pre-shared “serial key” and pre-negotiated algorithm
Key initialization command
(user key)
The device performs the verifications, including SNF check, authentication data check (by serial key), data decryption (by serial key), and BCC verification, if the verifications are successful, the “User Key” is acquired.
(serial key)
(serial key)
KSN verifies the “key initialization response” and acquires the new sequence number, a “key initialization” confirmation is made
Key initialization response
The device increases the sequence number by 1, and prepares the “key initialization” response message encrypted and authenticated by “serial key” and transmits it to KSN

Figure 15 – Sequences of user key initialisation

If KSN doesn’t receive any response from the newly registered device, KSN will re-transmit the secure message again with the previously transmitted sequence number.

The secure message frames exchanged between KSN and the newly registered device are shown in Figure 16. The key initialisation request message comprises the secure header information (b0:b1:b2:b3 = 0:0:0:0 as serial key index, b6:b7 = 0:0 as data authentication and confidentiality enabled, b8=0 as a request message), the sequence number and the key materials containing “user key”, key length and the associated algorithm stored in PADATA. Successful and failed responses are also shown in Figure 15. Differences between successful and failed response are the following.

a) The response result will be indicated in b12:b13:b14:b15 of SHD.

b) If it is a successful response, the value of SNF is increased by 1, but if it fails, the value of SNF is the same as the previous response one.

c) For a failed response, encrypted data in response message is copied from a request message, but authentication data is computed from SA fields to the encrypted data (include PBC, PADATA, BCC and PDG). For a successful response, response information will be put in PADATA.

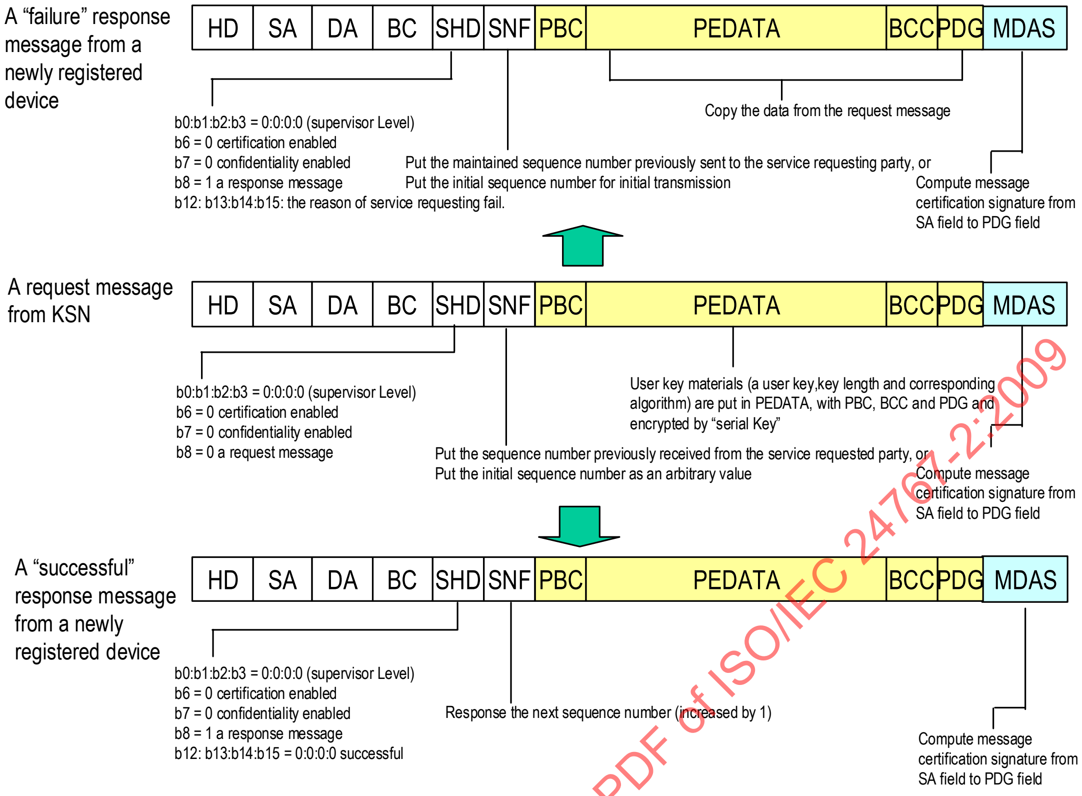

A "failure" response message from a newly registered device
HD
SA
DA
BC
SHD
SNF
PBC
PEDATA
BCC
PDG
MDAS
b0:b1:b2:b3 = 0:0:0:0 (supervisor Level)
b6 = 0 certification enabled
b7 = 0 confidentiality enabled
b8 = 1 a response message
b12: b13:b14:b15: the reason of service requesting fail.
Put the maintained sequence number previously sent to the service requesting party, or
Put the initial sequence number for initial transmission
Copy the data from the request message
Compute message certification signature from SA field to PDG field
A request message from KSN
b0:b1:b2:b3 = 0:0:0:0 (supervisor Level)
b6 = 0 certification enabled
b7 = 0 confidentiality enabled
b8 = 0 a request message
User key materials (a user key,key length and corresponding algorithm) are put in PEDATA, with PBC, BCC and PDG and encrypted by "serial Key"
Put the sequence number previously received from the service requested party, or
Put the initial sequence number as an arbitrary value
Compute message certification signature from SA field to PDG field
A "successful" response message from a newly registered device
b0:b1:b2:b3 = 0:0:0:0 (supervisor Level)
b6 = 0 certification enabled
b7 = 0 confidentiality enabled
b8 = 1 a response message
b12: b13:b14:b15 = 0:0:0:0 successful
Response the next sequence number (increased by 1)
Compute message certification signature from SA field to PDG field

Figure 16 – Secure message frames of "user key" initialisation

9.2.2 Initialisation of service provider keys

"Service provider keys" are the shared secrets between control nodes and device nodes. The "service provider key" delivery is also made by KSN to the newly registered device with the SCPM. A pre-shared secret, the "user key", is used to protect the delivery. The processes are shown in Figure 17 and the steps are described as follows.

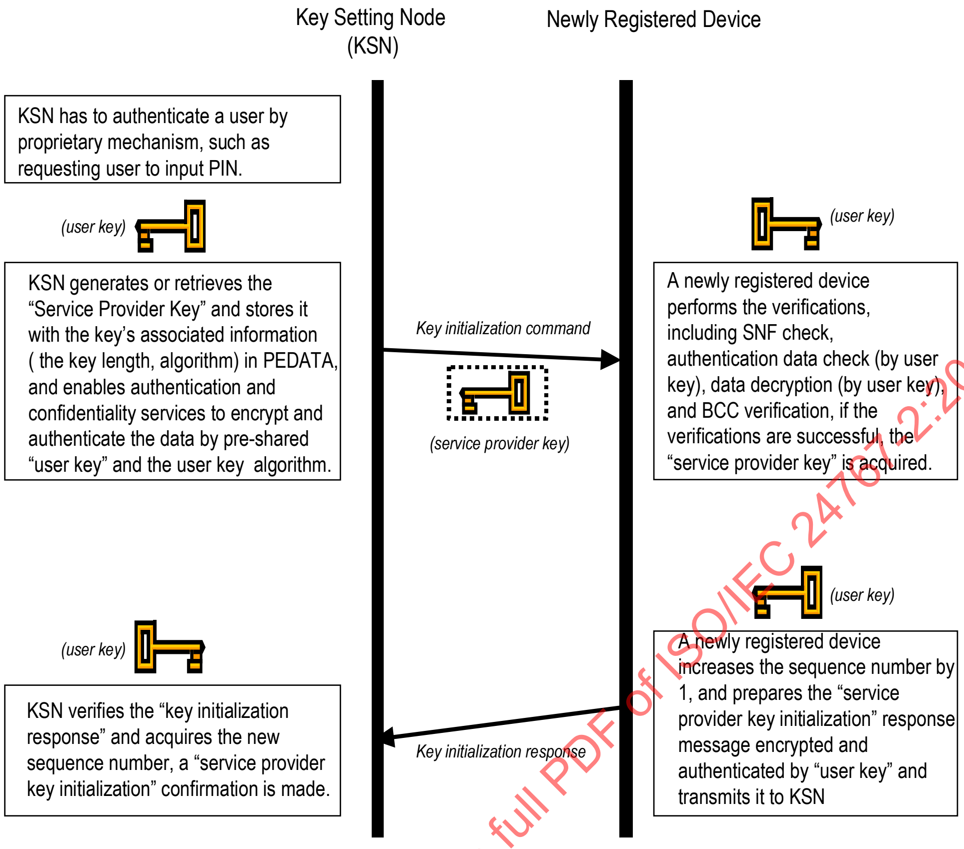
a) KSN authenticates the setting operation of "service provider key" by proprietary mechanisms, for example using PIN.

b) KSN generates/retrieves the "service provider key", stores it with associated attributes (key length and algorithm) in PADATA, enables data authentication and confidentiality services to encrypt and authenticate the "service provider key Initialisation request" data by the "user key" and the key's associated algorithm and then transmits it to the newly registered device.

c) The newly registered device receives and verifies the "service provider key Initialisation command" by the "user key" and its associated algorithm.

d) If the verifications are successful, the newly registered device prepares the "service provider key Initialisation response" by increasing the sequence number by 1, encrypting response data (PBC, PADATA, BCC and PDG) and adding authenticated data (MDAS) by the "user key" and then transmits it to KSN.

e) KSN receives and verifies the "service provider key initialisation response", retrieves the new sequence number and confirms the exchange is successful.



KSN has to authenticate a user by proprietary mechanism, such as requesting user to input PIN.

KSN generates or retrieves the "Service Provider Key" and stores it with the key's associated information (the key length, algorithm) in PEDATA, and enables authentication and confidentiality services to encrypt and authenticate the data by pre-shared "user key" and the user key algorithm.

A newly registered device performs the verifications, including SNF check, authentication data check (by user key), data decryption (by user key), and BCC verification, if the verifications are successful, the "service provider key" is acquired.

A newly registered device increases the sequence number by 1, and prepares the "service provider key initialization" response message encrypted and authenticated by "user key" and transmits it to KSN

KSN verifies the "key initialization response" and acquires the new sequence number, a "service provider key initialization" confirmation is made.

Figure 17 – Sequences of service provider key initialisation

If KSN doesn't receive any response from the newly registered device, KSN will re-transmit the secure message again with the previously transmitted sequence number.

The secure message frames exchanged between KSN and the newly registered device are shown in Figure 18, with an indication of key index in SHD set to b0:b1:b2:b3 = 0:0:0:1. The "service provider key", key length and the associated algorithm are encrypted and stored in PADATA. The composition of a request or a response message is almost the same as "user key initialisation", except the usage level and key materials are different.

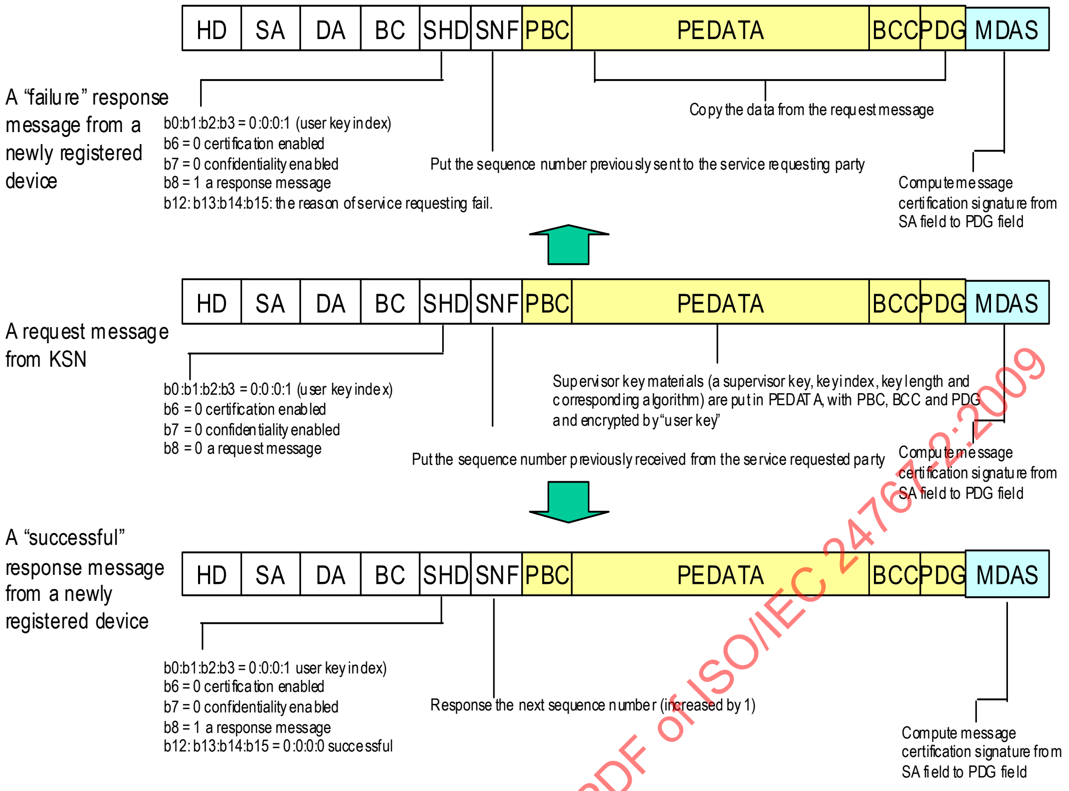

HD
SA
DA
BC
SHD
SNF
PBC
PEDATA
BCC
PDG
MDAS
A "failure" response message from a newly registered device
b0:b1:b2:b3 = 0:0:0:1 (user key index)
b6 = 0 certification enabled
b7 = 0 confidentiality enabled
b8 = 1 a response message
b12:b13:b14:b15: the reason of service requesting fail.
Put the sequence number previously sent to the service requesting party
Copy the data from the request message
Compute message certification signature from SA field to PDG field
A request message from KSN
b0:b1:b2:b3 = 0:0:0:1 (user key index)
b6 = 0 certification enabled
b7 = 0 confidentiality enabled
b8 = 0 a request message
Supervisor key materials (a supervisor key, key index, key length and corresponding algorithm) are put in PEDATA, with PBC, BCC and PDG and encrypted by "user key"
Put the sequence number previously received from the service requested party
Compute message certification signature from SA field to PDG field
A "successful" response message from a newly registered device
b0:b1:b2:b3 = 0:0:0:1 user key index)
b6 = 0 certification enabled
b7 = 0 confidentiality enabled
b8 = 1 a response message
b12:b13:b14:b15 = 0:0:0:0 successful
Response the next sequence number (increased by 1)
Compute message certification signature from SA field to PDG field

Figure 18 – Secure message frames of "service provider key" initialisation

9.2.3 Initialisation of maker key

It is recommended that a maker key is derived from the result of hash function of private information and property data of device.

No specific system is stipulated for setting the maker key for secure communications to the node.

9.3 Master key update

9.3.1 Master key update between KSN and a device

In SCPM, confidentiality and data authentication are assured by the use of a negotiated cryptographic algorithm, such as AES. AES is currently considered a strong cryptographic algorithm because the time estimated to crack AES is considerably longer than that to crack other algorithms, such as DES. DES keys are 56 bits long. AES can have key sizes of 128, 192 and 256 bits. On AES' 128-bit strength, the number of available keys is 10(**21) times more than that offered by DES and this means that if there exists a method capable of recovering a key in one second (though in fact "DES crackers" usually take a few hours to recover a DES key), it would still require 149 trillion years to crack a 128-bit AES key, which is rather insurmountable from the viewpoint of today's technologies. However, the security strength could not completely depend on the strength of the algorithm used, but may be subject to human frailties. In this case, it is recommended that master key update operations are performed periodically to avoid any possible security risk. However, it is opened for developers to find the balance between effective security practices and physical constraints.

Two optional master key update mechanisms are specified. One requires manual intervention by using "key initialisation" mechanism to distribute a new key as described in 8.1 and the other offers an automatic master key update operation by using computation sensitive Diffie-Hellman algorithm (DH) for a new key agreement. For those low-end devices, which could not afford DH operations but still want to exhibit a certain security level against possible attacks. Their periodical master key updates could be manually performed in the same way as “key initialisation”; for other devices processing more computation power, they can use a DH key agreement mechanism to enable automatic master key update operations within a specific time period. With respect to security consideration, shared secrets should be updated at predetermined intervals, which cover both “user key” and “service provider keys”. As for the “maker key”, whether it is to be updated or not is dependent on vendors.

Before describing the DH-based master key update mechanism, one would like to briefly introduce DH key agreement protocol itself. The protocol requires two system parameters p and g. They are both public and may be used by all the users in a system. Parameter p is a prime number and parameter g (usually called a generator) is an integer less than p, which is capable of generating every element from 1 to p−1 when multiplied by itself a certain number of times, modulo the prime p. In this way, the KSN and an intended device can use the DH key agreement protocol to agree on a shared secret key. In the following where a “new master key” will be used to represent either a new “user key” or “service provider key” and a “pre-master key” will be used to represent either a to-be-updated “user key” or “service provider key”, the steps of how a “new master key” distribution is activated by the KSN to a device using the SCPM and how a pre-shared secret, the “pre-master key”, is used to authenticate the two peers, are shown in Figure 19 and described as follows. A key of sufficient length and an unpredictable random private value are essential for the security of both key generation and the Diffie-Helmann protocol.

a) KSN generates a random private value and derives its public value using parameters p and g and the private value, then stores the computed DH public value in PADATA, enables data authentication service to authenticate the “DH public value exchange command” data by the “pre-master key” and then transmits it to a device.

b) The device receives and verifies the “DH public value exchange command” by the “pre-master key”. If the verifications are successful, the DH public value of KSN is acquired by the device.

c) The device increases the sequence number by 1 and prepares the “DH public value exchange response” message authenticated by “pre-master key” and transmits it to KSN.

d) KSN verifies the message “public value exchange response” and acquires the new sequence number, a public value exchange confirmation is made.

e) The device generates a random private value and derives its public value using parameters p and g and the private value, then store the computed DH public value in PADATA, enables data authentication service to authenticate the “DH public value exchange command” data by the “pre-master key” and then transmits it to KSN.

f) KSN receives and verifies the “DH public value exchange command” by the “pre-master key”. If the verifications are successful, the DH public value of the device is acquired by KSN.

g) KSN increases the sequence number by 1 and prepares the “DH public value exchange response” message authenticated by “pre-master key” and transmits it to the device.

h) The device verifies the message “public value exchange response” and acquires the new sequence number, a public value exchange confirmation is made.

i) KSN computes the shared secret key using its private value and the device’s public value. The device computes the shared secret key using its private value and KSN’s public value. And both of them derive a same value by DH algorithm, called a shared-secret key.

j) KSN generates/retrieves the “new master key”, stores it with associated key index, key length and algorithm in PADATA, enables data authentication and confidentiality services to encrypt and authenticate the “new master key update command” data by the shared-secret key computed by DH algorithm and then transmit it to the device.

k) The device receives and verifies the “new master key update command” by the shared secret key computed by ISO/IEC 11770-3 (DH algorithm).

l) If the verifications are successful, the device prepares the “new master key update response” by increasing the sequence number by 1, encrypting response data (PBC, PADATA, BCC and PDG) and adding authenticated data (MDAS) by the shared-secret key computed by ISO/IEC 11770-3 (DH algorithm) and then transmit it to KSN.

m) KSN receives and verifies the "new master key update response", retrieves the new sequence number and confirms the exchange is successful.

In a) – h), the two entities (KSN and the device) exchange DH public value using "pre-master key" to authenticate each other.

In i), the two entities individually compute the shared secret key by using ISO/IEC 11770-3 (DH algorithm).

In j) – m) the KSN distributes the "new masker key" protected by the computed shared secret key and the devices verifies it.

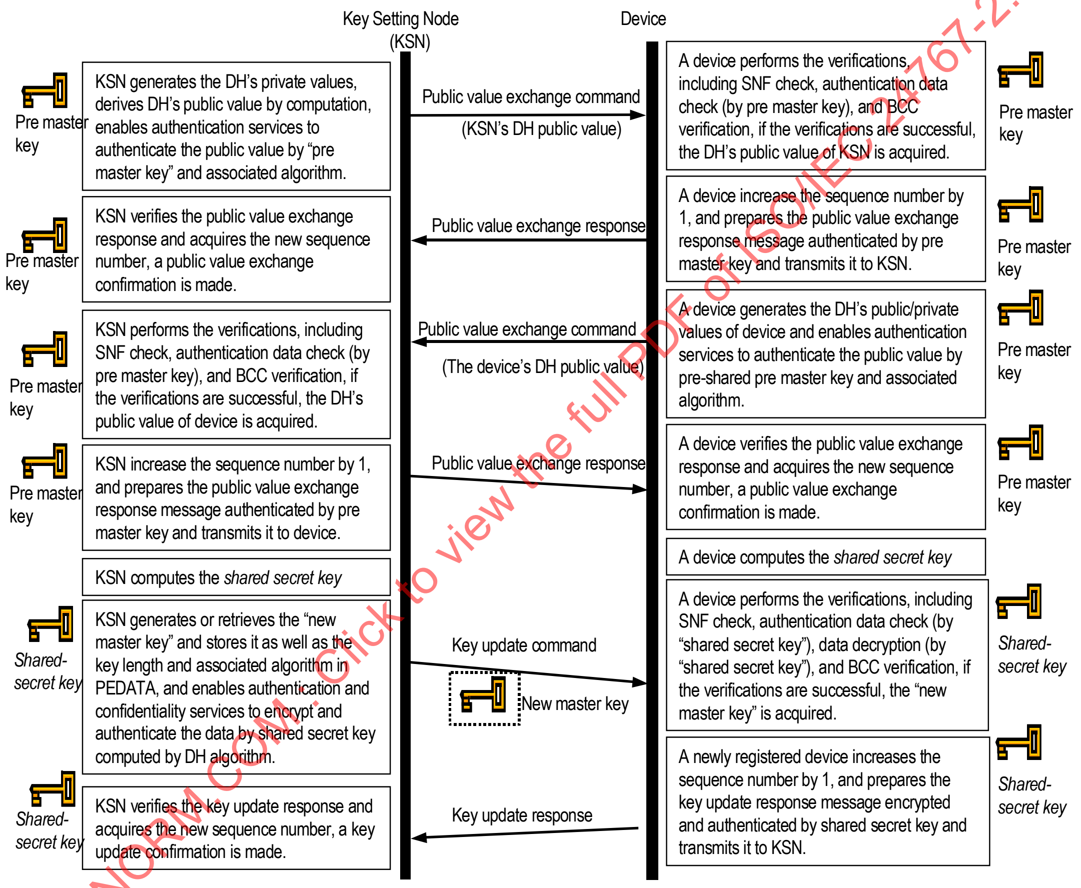

Key Setting Node (KSN)
Device
Pre master key
KSN generates the DH's private values, derives DH's public value by computation, enables authentication services to authenticate the public value by "pre master key" and associated algorithm.
Public value exchange command
(KSN's DH public value)
A device performs the verifications, including SNF check, authentication data check (by pre master key), and BCC verification, if the verifications are successful, the DH's public value of KSN is acquired.
Pre master key
Pre master key
KSN verifies the public value exchange response and acquires the new sequence number, a public value exchange confirmation is made.
Public value exchange response
A device increase the sequence number by 1, and prepares the public value exchange response message authenticated by pre master key and transmits it to KSN.
Pre master key
Pre master key
KSN performs the verifications, including SNF check, authentication data check (by pre master key), and BCC verification, if the verifications are successful, the DH's public value of device is acquired.
Public value exchange command
(The device's DH public value)
A device generates the DH's public/private values of device and enables authentication services to authenticate the public value by pre-shared pre master key and associated algorithm.
Pre master key
Pre master key
KSN increase the sequence number by 1, and prepares the public value exchange response message authenticated by pre master key and transmits it to device.
Public value exchange response
A device verifies the public value exchange response and acquires the new sequence number, a public value exchange confirmation is made.
Pre master key
KSN computes the shared secret key
A device computes the shared secret key
Shared-secret key
KSN generates or retrieves the "new master key" and stores it as well as the key length and associated algorithm in PEDATA, and enables authentication and confidentiality services to encrypt and authenticate the data by shared secret key computed by DH algorithm.
Key update command
New master key
A device performs the verifications, including SNF check, authentication data check (by "shared secret key"), data decryption (by "shared secret key"), and BCC verification, if the verifications are successful, the "new master key" is acquired.
Shared-secret key
Shared-secret key
KSN verifies the key update response and acquires the new sequence number, a key update confirmation is made.
Key update response
A newly registered device increases the sequence number by 1, and prepares the key update response message encrypted and authenticated by shared secret key and transmits it to KSN.
Shared-secret key

Figure 19 – Sequences of master key updates controlled by KSN using the DH algorithm